



# Department of Homeland Security Office of Inspector General

## Review of the Department of Homeland Security's Capability to Share Cyber Threat Information

(Redacted)





September 29, 2011

### Preface

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

This report addresses the strengths and weaknesses of the Department's capability to share cyber threat information among its federal, state, local, and tribal governments and private sector partners. It is based on direct observations and analyses of applicable documents. We obtained additional supporting documentation through interviewing personnel from selected federal agencies and companies in the private sector.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, which appears to read "Charles K. Edwards". The signature is written in a cursive style.

Charles K. Edwards  
Acting Inspector General

# Table of Contents/Abbreviations

---

Executive Summary .....	1
Background .....	2
Results of Audit .....	4
Actions Taken To Share Cyber Threat Information .....	4
Description of How Cyber Threat Information Is Shared Among Federal Agencies and the Private Sector .....	5
Mechanisms Used To Disseminate Classified Cyber Threat Information.....	12
Effectiveness of DHS’ Sharing and Distributing Cyber Threat Information Among Key Stakeholders .....	13
Recommendations.....	23
Management Comments and OIG Analysis .....	23
DHS’ Enforcement Authority.....	25
Recommendation .....	26
Management Comments and OIG Analysis .....	26

## Appendices

Appendix A: Purpose, Scope, and Methodology.....	27
Appendix B: Management Comments to the Draft Report .....	28
Appendix C: NCCIC’s Operational Partners .....	36
Appendix D: Major Contributors to this Report.....	37
Appendix E: Report Distribution .....	38

## Abbreviations

CYBERCOM	United States Cyber Command
DCAR	Department/Agency Cybersecurity Activity Reports
DoD	Department of Defense
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
GFIRST	Government Forum of Incident Response and Security Team
HSDN	Homeland Secure Data Network
I&A	Office of Intelligence and Analysis
ISAC	Information Sharing and Analysis Center
IT	information technology
JACKE	Joint Agency Cyber Knowledge Exchange
JWICS	Joint Worldwide Intelligence Communications System
MOA	Memorandum of Agreement

---

NASDAQ	National Association of Securities Dealers Automated Quotations
NCCIC	National Cybersecurity and Communications Integration Center
NCSD	National Cyber Security Division
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
NTOC	NSA/Central Security Service National Threat Operation Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
RSA	Rivest, Shamir, and Adleman
SIPRNet	Secret Internet Protocol Router Network
US-CERT	United States Computer Emergency Readiness Team

# OIG

---

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

## **Executive Summary**

We audited the Department of Homeland Security's (DHS) capability to share cyber threat information, as required by the *Intelligence Authorization Act for Fiscal Year 2010*. This act requires the Inspectors General of DHS and the Intelligence Community to report to Congress on (1) how cyber threat information is being shared among federal agencies and the private sector, (2) the mechanisms used to share classified cyber threat information, (3) an assessment of the effectiveness of sharing and distributing cyber threat information, and (4) any other matters that may inform the Congress or the President regarding the effectiveness of cybersecurity programs. Our audit focused on DHS' collaboration efforts to share and distribute cyber threat information with federal civilian agencies and its private sector partners. The Office of the Director of National Intelligence Office of Inspector General (OIG) focused its efforts on the Intelligence Community and the military branches. The results of its review will be provided in a separate classified report.

DHS has taken actions to create an environment to promote cyber threat information sharing in support of its mission. However, DHS can further improve its cyber threat information sharing by strengthening its public-private partnership to ensure better communication with government and sector coordinating councils and the private sector's Information Sharing and Analysis Centers. Also, DHS must delineate the roles and responsibilities between the National Cybersecurity and Communications Integration Center and the United States Computer Emergency Readiness Team to avoid confusion among federal agencies and the private sector.

We are making three recommendations to the Department. The Office of Intelligence and Analysis and the National Protection and Programs Directorate concurred with our recommendations and have already begun to take actions to implement them. The Department's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

---

## Background

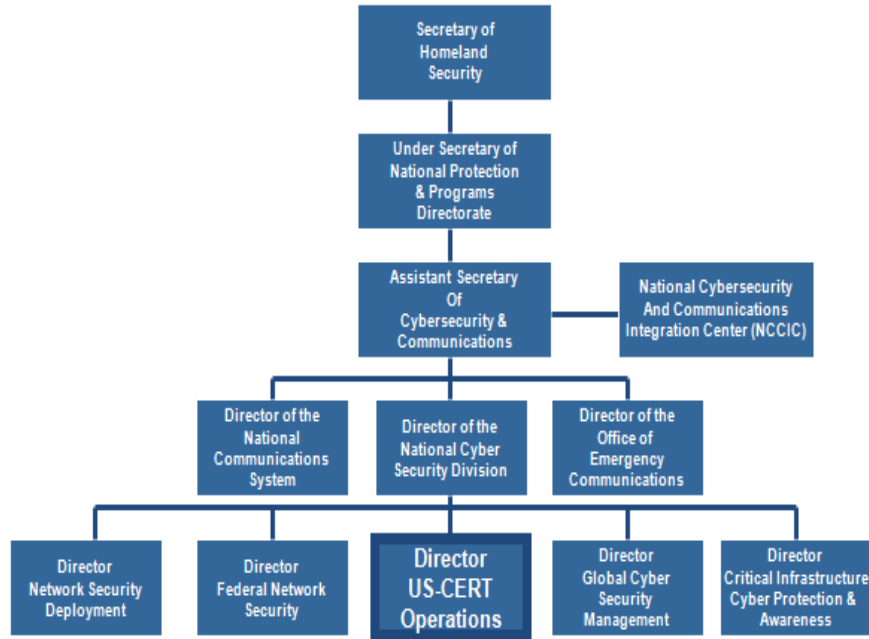
The *Intelligence Authorization Act for Fiscal Year 2010* requires the Inspectors General of DHS and the Intelligence Community to report to Congress regarding the status of sharing cyber threat information. The report should include the following:

- A description of how cyber threat intelligence information, including classified information, is being shared among the agencies and departments of the United States and with the private sector;
- A description of the mechanisms by which classified cyber threat information is distributed;
- An assessment of the effectiveness of cyber threat information sharing and distribution; and
- Any other matters identified by the Inspector General that would help to fully inform Congress or the President regarding the effectiveness of cybersecurity programs.

DHS is responsible for securing cyberspace and critical infrastructure under *Homeland Security Presidential Directive 7*. Specifically, DHS is responsible for (1) developing a comprehensive national plan for critical infrastructure protection; (2) developing and enhancing national cyber analysis and warning capabilities; (3) providing and coordinating incident response and recovery planning, including conducting incident response exercises; (4) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems; and (5) strengthening international cyberspace security. As such, DHS is the cybersecurity lead for federal civilian agencies, and it partners with the private sector to develop security capabilities. Its goals are to create a safe, secure, and resilient cyber environment and to promote awareness of cybersecurity.

To fulfill its mission, DHS partners with other federal agencies, the Intelligence Community, and the private sector to collaborate and share cyber threat intelligence information. Within DHS, the U.S. Computer Emergency Readiness Team (US-CERT) serves as the principal cyber watch, warning, and analysis center for federal civilian agencies and an operational point of coordination with the

private sector for cyber incident response.<sup>1</sup> Specifically, US-CERT is responsible for protecting the nation’s critical information systems infrastructure by coordinating the defense against and response to cyber attacks. See figure 1 for the Cybersecurity and Communications organizational chart.



**Figure 1: Cybersecurity and Communications Organizational Chart**  
 Source: US-CERT

In October 2009, DHS established the National Cybersecurity and Communications Integration Center (NCCIC), as the Department’s integrated cybersecurity and communications operations center. NCCIC is the focal point of coordination for national response efforts to significant cyber incidents. Specifically, NCCIC combines two of DHS’ operational units: US-CERT, the operational arm of the NCSD, leads a public-private partnership to protect and defend the nation’s cyber infrastructure; and the National Coordinating Center for Telecommunications which is the operational arm of the National Communications Systems. US-CERT uses NCCIC as the mechanism to brief the Department’s senior leadership on significant cybersecurity events. Additionally, NCCIC includes two other components: the Industrial Control Systems Cyber Emergency Response Team, which focuses on control systems security, and the Office of

<sup>1</sup> US-CERT is a branch of the National Cyber Security Division (NCSD) within the National Protection and Programs Directorate’s (NPPD) Office of Cybersecurity and Communications.

---

Intelligence and Analysis (I&A) Cyber Threat Branch. Although each organizational component fulfills separate operating missions, NCCIC's mission includes coordinating the operations of these components and developing a common operating picture. See figure 2 for DHS organizations that have a major presence on the NCCIC floor.

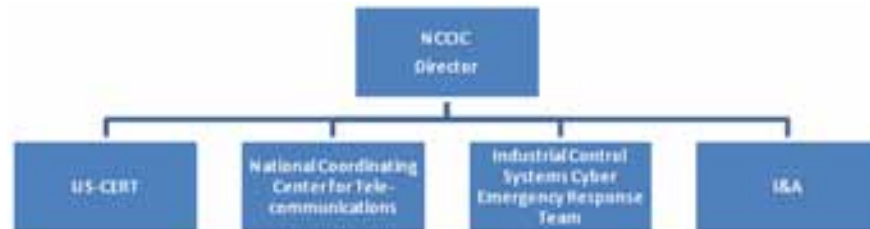


Figure 2: NCCIC's Organizational Components

Source: OIG

I&A is tasked with strengthening the Department's and other federal agencies' abilities to perform their homeland security functions by accessing, integrating, analyzing, and sharing timely and relevant intelligence and information, while protecting the privacy and civil liberties of citizens. One of I&A's missions is to deliver analytical intelligence products to its customers that address threats posed by all threat actors to the nation's critical infrastructure. I&A also develops policies that address and mitigate cybersecurity threats.

## Results of Audit

### Actions Taken To Share Cyber Threat Information

DHS has taken actions to create an environment to promote the effective sharing of cyber threat information in support of its mission. For example, DHS has taken the following actions to foster and improve cyber threat information sharing among the federal and private sectors:

- US-CERT developed an internal-external communication plan that depicts strategies to strengthen collaborative partnerships to improve shared cyber situation awareness.<sup>2</sup>
- DHS developed the *National Cyber Incident Response Plan* in coordination with federal, state, local, territorial, and private sector

---

<sup>2</sup> External partners include federal agencies, private sector, state and local governments, and international partners.



---

partners to establish the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and coordinate the recovery from a cyber incident. The plan serves as a mechanism across the cyber risk management spectrum, including incident management, data flow enhancement, analytical collaboration, and other integrated cybersecurity coordination efforts among the federal operations centers, Information Sharing and Analysis Centers (ISACs), and industry participants involved in cyber coordination and incident response activities.<sup>3</sup>

- DHS established a memorandum of agreement (MOA) with the Department of Defense (DoD) to set forth the terms by which both agencies will exchange personnel, equipment, and facilities to improve inter-agency collaboration in strategic planning for the nation's cybersecurity and to synchronize current operational missions.
- US-CERT established partnerships with ISACs, including Financial Services, Multi-State, and Information Technology (IT), to facilitate government and industry collaboration to mitigate unauthorized cyber activity in private networks and to improve the protection of privately owned critical infrastructure.

Although DHS has taken actions to facilitate the exchange of cyber threat information between federal agencies and the private sector, the Department still faces numerous challenges in carrying out its mission as the principal lead for securing the cyberspace. DHS must continue to improve its coordination efforts with other federal agencies and the private sector regarding cybersecurity mitigation strategies, information sharing initiatives, and sharing of best practices and processes to protect critical infrastructure and key resources across the sectors. Additionally, DHS must encourage both federal agencies and private sector partners to share their cyber threat information with the Department, in order to develop effective responses to potential attacks.

## **Description of How Cyber Threat Information Is Shared Among Federal Agencies and the Private Sector**

DHS shares cyber threat information among federal agencies and the private sector through various information portals; published reports;

---

<sup>3</sup> ISACs consist of the owners and operators of critical infrastructure and key resources to facilitate consistent interaction between and among public-private members and the government. They are considered collaborative partners with the shared goal of securing the nation's critical infrastructure.

---

telephone, email, and secure video teleconferences; and person-to-person contact, including working groups. The mechanism for sharing the information largely depends on the classification of the information and on the tools available for the intended recipient to receive the information.

### **Collaboration Among DHS Components and the Intelligence Community**

US-CERT shares cybersecurity information with the Intelligence Community through I&A's Cyber Threat Branch analysts, who are detailed both at NPPD and NCCIC. I&A and NPPD detailees work with US-CERT personnel at the NCCIC to coordinate on threat assessments and analysis activities. This coordination enables direct, person-to-person collaboration to fulfill the intelligence requirements of the NCCIC, US-CERT, and the Industrial Control Systems Cyber Emergency Response Team.

As a component of the NCCIC, the I&A's Cyber Threat Branch determines when threat intelligence and information is disseminated to its homeland security customers in DHS and the Intelligence Community to ensure that information from all sources is combined to provide a complete assessment of potential threats to the nation. US-CERT analysts identify cyber threat anomalies from intrusion detection systems that may signal potential unauthorized, unusual, or risky network activity on federal networks. Then, I&A uses US-CERT analyses to produce intelligence products, such as Homeland Security Intelligence Reports and Intelligence Information Reports.<sup>4</sup> Both reports are distributed via the Automated Messaging Handling System and the Homeland Secure Data Network (HSDN)<sup>5</sup> to DHS components and to other members of the Intelligence Community. I&A and US-CERT also coordinate on preparing the Secretary's daily cybersecurity briefings.

### **Collaboration with Federal Agencies**

To support the operations and improve situational awareness of the nation's cyber infrastructure, DHS engages in bi-directional communication exchange with federal agencies through meetings

---

<sup>4</sup> Homeland Security Intelligence Reports contain processed intelligence information and serve as a mechanism for a wider distribution to the broader Intelligence Community. Intelligence Information Reports consist of raw, unevaluated intelligence, which serves as a bridge between the Intelligence Community and the Department's non-intelligence components.

<sup>5</sup> HSDN is a classified wide area network for DHS and its components with specific and controlled interconnections to the Intelligence Community and federal law enforcement resources.

---

and continued dissemination of products and services. DHS' goals are to articulate key cybersecurity messages and to disseminate timely and accurate technical information to its federal agency partners. Additionally, DHS encourages partnerships with national and international entities to encourage situational awareness and share critical cyber threat information. DHS cyber security officials believe that on-going bi-directional communication is paramount to the success of these partnerships. For example, US-CERT exchanges liaison officers with the Federal Bureau of Investigation's (FBI) National Cyber Investigative Joint Task Force, National Security Agency's (NSA) Central Security Service National Threat Operation Center (NTOC), DoD's United States Cyber Command (CYBERCOM) and Cyber Crime Center, and the DHS National Operations Center. In addition, the United States Secret Service stations a liaison at US-CERT to improve communication and exchange cyber threat information.

When potential cyber crimes and threats are detected, FBI's Cyber Division notifies outside agencies of information and intelligence gleaned from all facets of FBI cyber investigations and intelligence gathering efforts. The FBI shares with DHS through its cyber liaison assigned to DHS and by disseminating timely and actionable intelligence and threat information directly to US-CERT during ongoing investigations. US-CERT in turn uses the intelligence and information to notify its partner agencies and institute any mitigation strategies provided by the FBI notification.

Further, DHS participates in information sharing initiatives including weekly meetings attended by the DoD's CYBERCOM, the NSA NTOC, and the Departments of Energy and State. DHS also participates in the National Cyber Investigative Joint Task Force meetings, which have majority participation from law enforcement agencies. Also, DHS operates the Government Forum of Incident Response and Security Team (GFIRST) portal and coordinates its annual conference.<sup>6</sup>

US-CERT's information sharing and incident response process includes distributing recipient-specific Department/Agency Cybersecurity Activity Reports (DCARs) to federal agencies.<sup>7</sup> As

---

<sup>6</sup> GFIRST promotes cooperation among the full range of departments and agencies as well as the defense, civilian, intelligence, and law enforcement communities. Members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices.

<sup>7</sup> US-CERT publishes the weekly DCARs to provide senior cybersecurity officials awareness of cybersecurity incidents occurring across the civilian federal government. This report details the trends observed in the .gov domain and open source reporting.

---

of January 2011, US-CERT distributed DCARs to 10 federal agencies as well as a general government-wide DCAR. Additionally, US-CERT participates in a number of monthly sharing activities with different agencies, as well as operates and organizes the Joint Agency Cyber Knowledge Exchange (JACKE) program meetings.

To further exchange cyber threat data between both agencies, DoD and DHS launched initiatives to share analysts and coordinate their cyber operations which include the NSA NTOC, and DoD's Cyber Crime Center. The MOA between DoD and DHS works toward ensuring that both agencies' priorities and requests for support are clearly communicated and met. Among other responsibilities, DHS officials maintain cognizance of both agencies' activities to avoid duplication of efforts and potential conflict. Both agencies have personnel co-located at their sites to support their operational and planning efforts. Further, DHS has entered into other initiatives or MOAs, such as with the FBI's National Cyber Investigative Joint Task Force. These agreements provide DHS with additional resources to improve inter-agency collaboration in strategic planning for the nation's cybersecurity, mutual support for capabilities development, and synchronization of current operation mission activities.

### **Collaboration with State, Local, Tribal, and Territorial Governments**

State, local, tribal, and territorial governments receive their cyber threat information from I&A's Cyber Threat Branch, National Operations Center, NCCIC, fusion centers, and through the Department of Justice FBI/National Cyber Investigative Joint Task Force outreach for law enforcement agencies. Additionally, state governments have designated a senior official for the Cyber Unified Coordination Group to improve situational awareness, which is a key element in responding to cyber security incidents. Further, the state and local government partners participate in the Homeland Security State and Local Intelligence Community of Interest working group to share sensitive information regarding current and emerging threats to the nation. Cyber threat information is disseminated to state and local governments via secured video teleconferences and Homeland Security State and

---

Local Intelligence Community of Interest and HSDN portals.<sup>8</sup> Under the *Cybersecurity Partner Local Access Plan* pilot program, I&A arranges for US-CERT to provide cybersecurity awareness briefings to fusion centers on a region-by-region basis.

Further, DHS collaborates with state, local, tribal and territorial governments through its working relationship with the Multi-State ISAC. The Multi-State ISAC serves as the primary contact between US-CERT and state and local governments. US-CERT provides funding to the Multi-State ISAC and communicates with them on a daily basis.

### **Collaboration with the Private Sector**

US-CERT is developing information sharing relationships with critical infrastructure and key resources sector partners, such as the Financial Services ISAC, IT-ISAC, and Multi-State ISAC. Currently, there are liaisons from the IT-ISAC, Multi-State ISAC, and the communication sector at the NCCIC. Further, the Financial Services ISAC participates in a pilot program with DoD's Cyber Crime Center and US-CERT to regularly share cybersecurity products and information. Additionally, US-CERT coordinates with the Industrial Control Systems Cyber Emergency Response Team to communicate with other private companies to secure their control systems. US-CERT works in close collaboration with other federal cyber centers to share threat information with the private sector.

For example, in August 2010, US-CERT briefed the IT-ISAC on security issues related to mobile devices, worked with the NSA to monitor developments of Zeus malware and provided informational briefings at GFIRST conference.<sup>9</sup> In September 2010, US-CERT representatives met with the Secretary of Defense to discuss incident information sharing.

Based on their awareness of cybersecurity, private sector recipients can receive cyber threat information in several ways. For example, some recipients (e.g., Financial Sector ISAC, Energy Sector ISAC, and Water Sector ISAC) are considered NCCIC's operational

---

<sup>8</sup> The Homeland Security State and Local Intelligence Community of Interest consists of state and local government partners. It allows intelligence analysts in the states and federal agencies to share sensitive homeland security intelligence information and analysis on a daily basis.

<sup>9</sup> Zeus malware is a generic back door that allows full control by an unauthorized remote user. Its primary function is financial gain by stealing online credentials, such as file transfer protocol, email, online banking and other passwords.

---

partners, and they receive information directly from their analysts and other liaisons at the NCCIC.

The NCCIC also provides regular briefings to the Sector Coordinating Councils, which have established mechanisms to share cyber threat information with individual critical infrastructure owners and operators. Additionally, specific private sector entities, (e.g., telecommunication providers, software vendors, and internet service providers) have established relationships with the NCCIC and requested information to ensure their resiliency.

Further, the private sector receives cyber threat information by accessing DHS' portals and websites (e.g., GFIRST portal and the US-CERT.gov website, which includes the National Cyber Alert System). The private sector also uses the Homeland Security Information Network/US-CERT to collaborate with the public sector about cyber security incidents, vulnerabilities and exploits in a trusted environment.<sup>10</sup> US-CERT also provides information on current cyber security issues, activities, and resources to the private sector on its public website.

---

<sup>10</sup> The Homeland Security Information Network is a national web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. Users can share within their communities or reach out to other communities as needed.

Figure 3 depicts the information sharing environment used by US-CERT. See appendix C for a list of NCCIC’s operational partners.

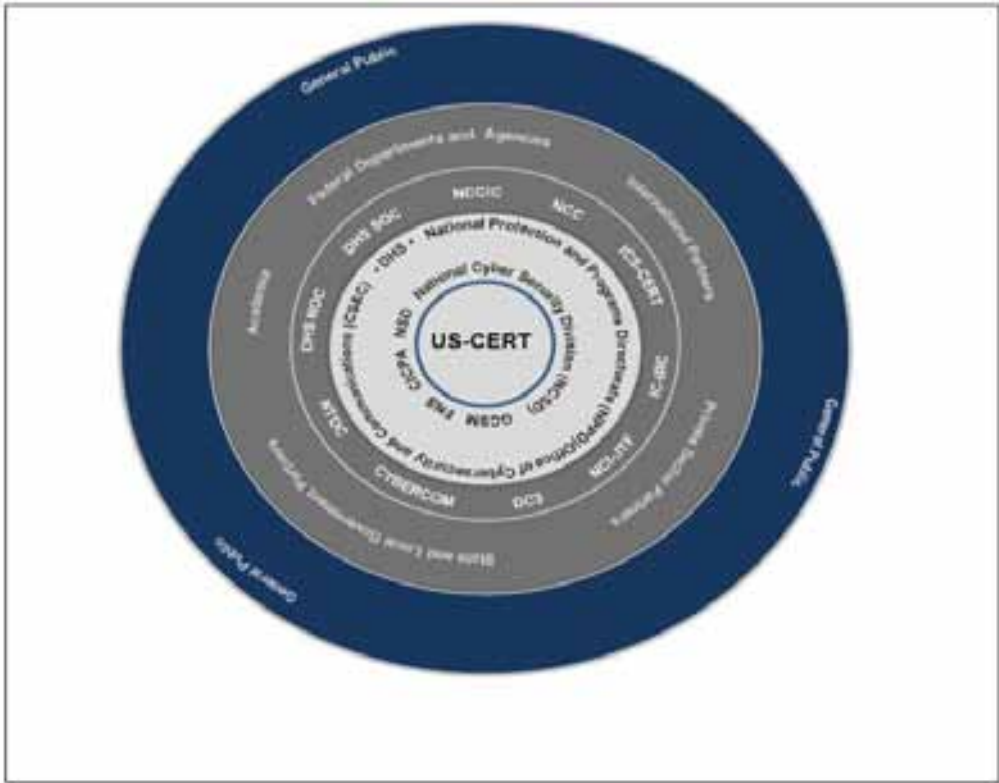


Figure 3 Acronyms		
CICPA	Cyber Infrastructure Cyber Protection and Awareness	ICS-CERT Industrial Control Systems Cyber Emergency Response Team
DC3	Department of Defense Cyber Crime Center	NCC National Coordinating Center for Telecommunications
FNS	Federal Network Security	NCI-JTF National Cyber Investigative Joint Task Force
GCSM	Global Cyber Security Management	NOC National Operations Center
IC-IRC	Intelligence Community Incident Response Center	NSD Network Security Deployment
		SOC Security Operations Center

**Figure 3: US-CERT Information Sharing Environment** Source: US-CERT

Finally, DHS is undertaking many initiatives to enhance the exchange of cyber threat information with the private sector. These initiatives include the following:

- Expanding its private sector information sharing processes by building an information sharing model that incorporates private sector stakeholders across multiple sectors. Under this model, US-CERT coordinates with its partners to provide their stakeholders with timely risk information and remediation

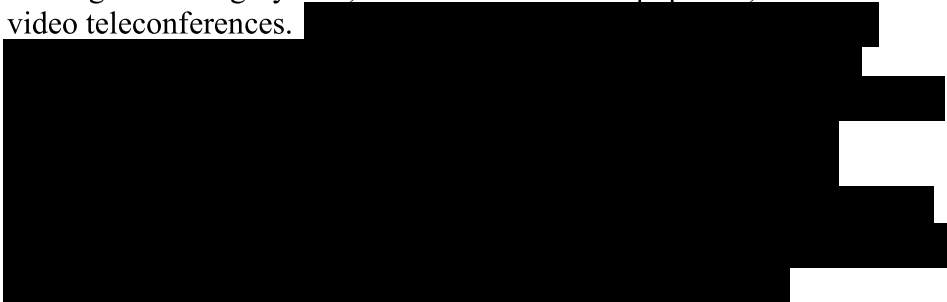
---

strategies to protect their networks and those of their critical infrastructure.

- Contracting with Carnegie Mellon University’s Software Engineering Institute to develop and coordinate cybersecurity data flow efforts between the federal government and the private sector. The projected outcome is to include capabilities that map and align actionable cybersecurity risk management activities, potential attacks, and vulnerability mitigation.
- Participating in conferences and engagements that support its coordination with federal, state and local governments, as well as the international, public and private sector communities to share up-to-date information on cyber threats and mitigation strategies and to promote information sharing.

## **Mechanisms Used To Disseminate Classified Cyber Threat Information**

DHS uses several mechanisms to share classified cyber threat information with federal agencies, the Intelligence Community, and the private sector. Specifically, DHS communicates and distributes “Secret” cyber threat information through the use of classified information systems and person-to-person interactions. Cyber threat information that is classified as “Secret” is disseminated through HSDN and the Secret Internet Protocol Router Network (SIPRNet),<sup>11</sup> as well as through the Automated Message Handling System,<sup>12</sup> Secure Terminal Equipment,<sup>13</sup> and secured video teleconferences.



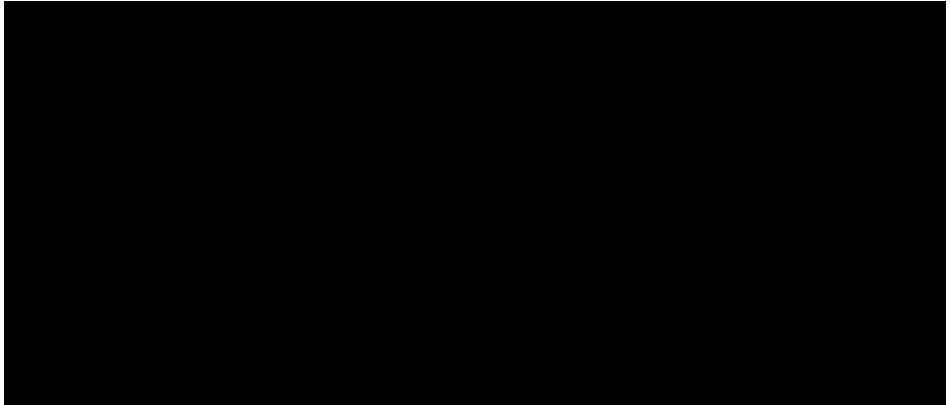
---

<sup>11</sup> SIPRNet is a DoD system used to transmit information that is classified as “Secret”.

<sup>12</sup> The Automated Message Handling System provides a user-friendly means to send and receive messages and to provide connectivity to and interoperability with other federal agencies, allies, tactical users, and defense contractors. It also provides guaranteed delivery to the intended recipients and maintains writer to reader accountability.

<sup>13</sup> Secure Terminal Equipment consists of encrypted telephone communications system for wired or landline communications.





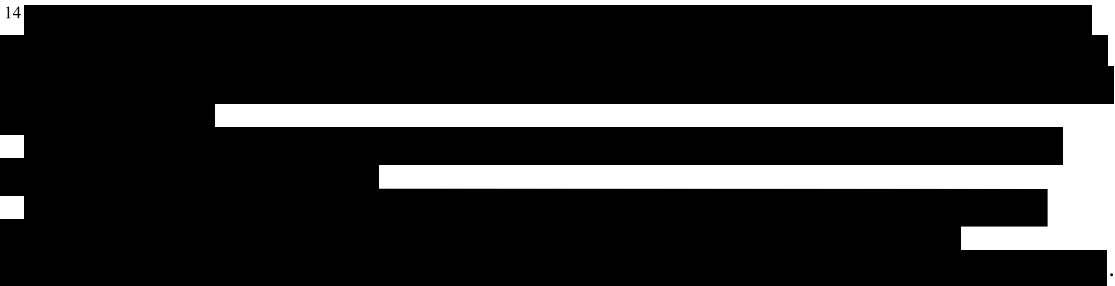
Person-to-person interactions occur between liaisons who are detailed at the NCCIC, or stakeholders and public sector partners participating in monthly or quarterly working groups, GFIRST, and JACKE meetings. Further, DHS participates in the Operations and Intelligence Round-Up, which is a weekly analyst-to-analyst exchange coordinated by CYBERCOM. Also, DHS organizes the JACKE monthly meetings with analysts and representatives from various Security Operations Centers. The CYBERCOM, JACKE, and NTOC meetings mostly address operational issues.

### **Effectiveness of DHS’ Sharing and Distributing Cyber Threat Information Among Key Stakeholders**

Although considerable amount of information is being shared between DHS, other federal agencies, and the Intelligence Community, more sharing and coordination efforts are needed to address cyber threats in a

---

14



---

timely and synchronized manner. Specifically, some federal agencies have limited access to classified cyber threat information. Additionally, DHS has limited control over the classified cyber threat and tear line information it receives.<sup>17</sup> As a result, some stakeholders do not perceive the information provided as valuable because it may not be timely or provide recommended actions to address potential cyber threats.

### **Most Federal Partners Are Not Equipped to Receive Classified Cyber Threat Information**

DHS' ability to share classified cyber threat information with other federal agencies is contingent upon these agencies having the required facilities, equipment, and employees to receive and process classified material. Specifically, many federal agencies do not have access to HSDN and JWICS, systems used for transmitting "Secret" and "Top Secret" classified information, respectively. Further, the lack of proper security clearances for senior IT personnel at these agencies is a major hindrance for DHS to share classified cyber threat information timely and effectively.

We interviewed senior officials from eight federal agencies to evaluate the effectiveness of DHS' sharing and distributing of cyber threat information. Overall, these officials indicated that cyber threat information was shared effectively. However, they expressed concerns regarding their access to classified cyber threat information.

For example, officials at one department informed us that the agency has only one or two JWICS terminals for multiple users as well as limited HSDN access. Only 6 of 220 personnel at its national security operations center have "Top Secret" clearances. Although the agency does not generally handle classified information, its personnel have found classified cyber threat forums and products valuable and would like to share more information learned from these forums within the organization. However, currently it cannot do so as the material is classified and only a few of its staff possess the required security clearance.

Additionally, since there is no JWICS access at another agency's Office of the Chief Information Officer (OCIO), its personnel have to reach out to other agency staff outside the OCIO with JWICS

---

<sup>17</sup> A tear line report contains a physical line on an intelligence message or document which separates categories of information that have been approved for disclosure and release. Normally, the intelligence below the tear line has been previously cleared for disclosure or release.

---

access to obtain the information needed to respond to a potential threat. This usually requires this department's OCIO personnel to travel to another location. Similarly, cyber security staff at two other agencies must travel to another location to access classified systems. Then, agency personnel must print out and transport classified material back to their respective offices.

Agency officials cited the lack of sufficient funding as the main obstacle to their agencies acquiring access to classified cyber threat information. At four agencies we visited, management officials decided not to obtain access to classified material because they believed the cost outweighs its benefits. Specifically, one department's official told us that it is extremely difficult to make a case to its leadership for classified system access when US-CERT does not provide classified cyber threat products tailored to the agency's specific needs, which would have greatly increased their value. In the case of another agency's OCIO, agency officials informed us that its JWICS access request was pending approval from the Office of the Director of National Intelligence. According to these officials, a service level agreement was established to allow US-CERT to monitor agency's network traffic. This agreement requires JWICS access, and US-CERT has not made a request to the Office of the Director of National Intelligence on its behalf. US-CERT officials responded that DHS does not have sufficient resources to help other federal agencies obtain the required system access and security clearances.

According to *Homeland Security Presidential Directive 7*, the DHS Secretary is required to establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other federal agencies, state and local governments, and the private sector in a timely manner. Additionally, the *National Infrastructure Protection Plan 2009* established the goal that requires critical infrastructure and key resources partners to strive toward access to robust information sharing networks that include relevant intelligence and threat analysis, and incident reporting. Further, effective communication which includes multidirectional information sharing between government and industry to streamline and reduce redundant reporting is highly encouraged.

Unless other agencies acquire the required facilities and equipment, and ensure that their personnel possess the proper security clearance to receive or process classified cyber threat

---

information, DHS will continue to be restricted in what kind of cyber threat information it can share. As a result, these federal agencies will be hindered in their respective efforts to address effectively cyber threats to their systems.

### **DHS Has Limited Control Over the Classified and Tear Line Information It Receives**

Federal agency and private sector officials expressed concerns regarding DHS' inability to provide unclassified cyber threat information to a wider customer base. Cultural and mission differences among Intelligence Community members and federal agencies affect how cyber threat analyses are produced and result in products of varied quality and timeliness for DHS' partners and customers. However, since the Department is not the originator of the classified materials, DHS is often restricted in distributing cyber threat information that is classified "Secret" or "Top Secret". Specifically, DHS is prohibited by originating authorities from creating tear line reports or providing specific details to other agencies. As a result, many DHS partners and customers are not receiving the cyber threat information needed to take proper action.

Based on their respective cyber functions, elements of the Intelligence Community focus on the priority to support their own missions. As a result, intelligence/cyber threat information they share with DHS may not allow time-sensitive threat mitigation actions to be taken. DoD officials told us that classified cyber-related information becomes too restrictive and generalized when it is collected from multiple sources. That is, originators often consider only their respective missions and needs for the information but not the prospective needs of their cyber threat partners.

Additionally, DHS does not have the authority to declassify any information that the Department did not generate. Specifically, DHS cannot generate tear line reports or release any information that may hinder another agency's on-going investigation, work in progress, or violate applicable classification policies.

As part of *Intelligence Community Policy Memorandum Number 2007-500-1, Unevaluated Domestic Threat Tear Line Reports (November 2007)*, the Office of the Director of National Intelligence requires the Intelligence Community to produce unclassified versions of all classified reports involving threats to the United States that identify a specific target, geographic

---

location, or method of attack.<sup>18</sup> However, some Intelligence Community elements are not including their tear line reports with the classified material. Finally, there is no similar requirement for non-Intelligence Community elements to create tear line reports.

According to US-CERT officials, since it can be very time-consuming to develop tear line reports, other agencies are not willing to create these reports for their classified products. In some instances, when DHS receives tear line reports, the Department may still be restricted as to when and with whom the information can be shared. In addition, the originating agencies may restrict the distribution of the tear line report. Some federal agencies and private sector officials said that they would, at a minimum, prefer to receive information regarding what is being attacked and the method (i.e., excluding the attacker or the specific agency/company being attacked) in an unclassified format.

### **Private Sector Stakeholder Views**

We met with representatives from 17 private sector companies and 2 ISACs to obtain their views on the effectiveness of DHS' sharing and coordination efforts between the Department and the private sector. Most of these officials indicated that DHS has improved its information sharing efforts over the last few years. Specifically, US-CERT has increased its outreach efforts by participating in more private sector meetings and conferences and is providing more actionable information in its alerts and bulletins.

Representatives from the Finance, Healthcare and Public Health, and Communication sectors noted improvements in their collaboration with US-CERT. However, some officials expressed concerns regarding the effectiveness of DHS' collaboration efforts and with the quality and timeliness of US-CERT products. As a result, private sector companies often use their own tools to share, analyze, and exchange cyber threat information within their sectors, rather than collaborating with DHS.

The private sector officials we interviewed identified a number of improvements that DHS could implement to further enhance its

---

<sup>18</sup> The Intelligence Community Policy Memorandum states "all available context information relating to the information collected shall be included in the tear line report. This may include information on the source/sub-source's access to the information, reporting history, possible motivation, or other pertinent details". These reports shall be consistent with statutory requirements to protect intelligence sources and methods.

---

cyber threat information sharing initiatives.<sup>19</sup> Specifically, DHS needs to:

- Improve the accuracy and timeliness of its alerts and bulletins. Specifically, some of the larger companies told us that DHS provided the same cyber threat information they had already received from other sources, such as ISACs, and private vendors. Additionally, these companies noted that DHS does not always provide cyber threat information timely to allow for prompt response and mitigation.
- Customize products with cyber threat information for specific sectors. Without these customized products, according to some representatives, they have to conduct extensive analyses to determine whether the threat or vulnerability cited in US-CERT's products pertains to their sector.
- Identify recommended actions companies should take to mitigate the threats or security incidents cited in US-CERT's alerts and bulletins. Some representatives told us that US-CERT products do not always include actionable recommendations. According to these companies, without these recommendations they could not take prompt corrective actions to mitigate the threat identified.
- Provide guidance on how classified and "for official use only" cyber threat information could be distributed within global companies. For example, some global companies told us that they were not sure if they could disseminate cyber threat information provided by US-CERT to key cybersecurity personnel at their overseas offices. They said that they employ foreign nationals in cyber security positions at their overseas offices, and these employees may not possess the security clearances needed to gain access to critical cyber threat information.

Further, cybersecurity personnel at some companies expressed concerns that DHS did not engage them fully when drafting new

---

<sup>19</sup> The private companies represented nine critical infrastructure and key resource sectors including finance, chemical, communications, energy, IT, nuclear, postal and shipping, healthcare and public health, and transportation systems.

---

policies and initiatives that may affect them. For example, when planning the *National Cyber Incident Response Plan Annex*, DHS announced that the private sector would have an opportunity to comment on the strategy. However, some company officials told us that they were given the opportunity to comment on the document only after it was developed by a government-only working group. Additionally, some IT-ISAC members voiced concerns that when DHS reached out to the private sector with other draft policies for comments, they were given a relatively short time to comment on the nearly finalized policies, such as the *Homeland Security Strategy for Enterprise*. Since some private companies believe that DHS' strategies are lacking in the areas of cross-sector and cross-company information sharing, they have piloted their own cybersecurity efforts to address their concerns.

US-CERT officials acknowledged the concerns expressed by some in the private sector with their services and products. Since US-CERT's mission is to serve the broader spectrum of cybersecurity for the nation, these officials do not believe they can provide the sector- or industry-specific information that these partners desire. US-CERT officials added that it does not have sufficient resources to provide each partner with customized cyber threat activity and information. To augment the information provided through published products, US-CERT communicates with the private sector through the coordination with various organizations, such as Sector Specific Agencies and the ISACs. According to US-CERT officials some products are "alert" products by design and are intended only to draw attention to a possible threat in as timely a fashion as possible – not to provide in-depth analysis.

US-CERT officials disagreed with the perception that the Department did not reach out to the private sector for its input in developing joint initiatives and information sharing efforts. They cited its development and exercise of the *National Cyber Incident Response Plan* and the establishment of MOAs between DHS, DoD, and the Financial Services ISAC as examples of soliciting input and participation from private sector partners.

*Homeland Security Presidential Directive 7* requires DHS and federal agencies to collaborate with the private sector to facilitate information sharing concerning physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. Additionally, the *Comprehensive National Cybersecurity Initiative* encourages the enhancement of on-going

---

partnerships between the federal government and the public and private sector owners and operators of the critical infrastructure and key resources.

To improve communication with the private sector, DHS is drafting a cyber information flow policy to outline the information sharing processes among the Department, ISACs, and private sector partners. The goal of the policy is to establish on-going sharing of cyber threat information, such as trends, tactics, and techniques among key stakeholders. According to I&A officials, the Office of the Director of National Intelligence National Intelligence Manager for Cyber and DHS have begun a project to develop information requirements and convert them into timely, actionable intelligence for government and private sector critical infrastructure network defenders.

### **The Roles and Responsibilities of NCCIC and US-CERT Have Not Been Delineated**

DHS has not defined and communicated the roles of the newly created NCCIC to its partners or developed a portal to disseminate NCCIC products. NCCIC was established as a member of DHS' information sharing environment to serve as a cyber threat aggregate authority at DHS. However, some private sector partners expressed concerns experienced by their liaisons stationed on the NCCIC floor. For example, some private sector liaisons have experienced connectivity and other technical problems that keep them from accessing actionable and timely threat information. Additionally, some US-CERT's customers have become less satisfied with the support they have received since the creation of NCCIC.

Because of the problems they experience at NCCIC, some federal agencies and private companies, including ISACs, do not see the value in stationing liaisons on the floor. For example, the IT sector and IT-ISAC representatives informed us that their liaisons cannot access their companies' networks from the NCCIC floor to coordinate incident responses. Instead, the liaisons have to access their companies' networks via their laptop computers away from the NCCIC floor.

Further, some officials in the private sector expressed concern with NCCIC's dissemination of information during specific cyber events, such as the National Association of Securities Dealers



---

Automated Quotations (NASDAQ) attack,<sup>20</sup> the Rivest, Shamir, and Adleman (RSA) hack,<sup>21</sup> and the Stuxnet attack.<sup>22</sup> According to some of the private sector officials we interviewed, DHS did not provide information concerning these attacks to the private sector timely. In some instances, the private sector first learned of the attacks through the media and then received information from the Department. For the NASDAQ Attack, Securities and Exchange Commission officials told us that they were directly involved in the incident as part of the financial sector and requested initial information about the attack from US-CERT. However, US-CERT declined the agency's request and instead released a bulletin regarding the incident. For the RSA hack, a banking official told us that DHS did not share specific details with the banking sector until it was reported in the media. In addition, the information that DHS released was general and limited because of the ongoing investigation by law enforcement agencies and some it was classified. However, some private sector officials told us that DHS should have worked more closely with them and consulted them, since their companies were being identified by the news media. Also, they felt that DHS did not sufficiently solicit industry's perspective on the best response procedure.

As a result, some companies and ISACs are evaluating whether to maintain the NCCIC liaison positions since they perceive the information flow as one-directional, with information flowing only to the NCCIC. Some private sector officials believe that they are not receiving the expected information and services or overall return on investment for the money they are spending in having a liaison at the NCCIC.

Further, some private sector officials view NCCIC as an added layer of complexity when working with DHS. For example, there is no longer a clear process for communicating incidents since NCCIC has been established. Some federal agency and company

---

<sup>20</sup> The NASDAQ attack was reported by the media on February 4, 2011. A NASDAQ stock market operator found suspicious files on its United States computer servers and determined that hackers could have affected one of its Internet-based client applications. However, at the time of the media report, there was no evidence that customer information was accessed or acquired or that any trading platforms were compromised.

<sup>21</sup> The RSA hack, reported by the media in March 2011, occurred when sensitive information related to the popular SecurID two-factor authentication products was stolen. Although the stolen information alone would not enable a successful attack on SecureID customers, it could reduce the effectiveness of the security.

<sup>22</sup> In 2010, researchers found that the Stuxnet malware was designed to infect industrial control systems.

---

officials are not even sure whether to report incidents to US-CERT, NCCIC, or both.

We discussed with NCCIC staff regarding the concerns raised in our meetings with private sector companies. In response, the NCCIC Director clarified the respective roles and responsibilities of NCCIC and US-CERT. First, he stated that US-CERT is a component of NCCIC. As such, US-CERT plans to work in coordination with other federal components of NCCIC, (e.g., Industrial Control Systems Cyber Emergency Response Team, National Coordinating Center for Telecommunications, and I&A) and to provide the input gathered from the US-CERT partners to the NCCIC. Then, NCCIC integrates the information gathered from its components and partners. US-CERT's partners are expected to continue using US-CERT; however, the NCCIC maintains direct contact with the Cyber Alliance Project partners and ISACs.

According to DHS officials, US-CERT is in a position to share its own information. Third-party information can be shared only with the permission of that third-party. This information may be the proprietary information of a private sector partners. Alternatively, it may be law enforcement information provided to US-CERT by the United States Secret Service or the FBI. US-CERT works with those private and public sector partners to package and disseminate their information in a manner that does not jeopardize their interests; however, US-CERT must still obtain permission from the owner.

DHS officials acknowledged that addressing the concerns from federal agency and private sector officials is a difficult challenge. Specifically, the effectiveness of sharing cyber threat information is contingent upon federal agency and private sector partners' willingness to collaborate and share all available information with DHS. DHS officials told us that the Department will continue to work with its public and private partners to encourage increased bi- and multi-directional information sharing.

It is essential that DHS, federal agencies, and the private sector share pertinent cyber threat information and improve collaboration to ensure that appropriate steps can be taken to mitigate the potential effect of a cyber incident. DHS cannot effectively defend against and respond to cyber incidents without the support and collaboration of other agencies and the private sector.

---

## Recommendations

We recommend that the Under Secretary of I&A:

**Recommendation #1:** Coordinate with the Office of Director of National Intelligence to develop policy on the right to release and share cyber threat and related information through tear line reports with the Intelligence Community, other federal agencies, and the private sector.

We recommend that the Under Secretary of NPPD:

**Recommendation #2:** Improve communication with NCCIC and US-CERT's partners and customers to address their concerns and needs regarding cyber threat information, products, and mitigation strategies.

## Management Comments and OIG Analysis

I&A concurred with recommendation 1. I&A is coordinating with the Office of Director of National Intelligence on an initiative to develop updated intelligence community policy on releasing and sharing information through unclassified tear line reports with I&A's customers, including federal agencies, state, local and tribal partners, and the private sector. The new guidance is intended to recognize the evolving threat paradigm and codify the responsibilities and standards for the intelligence community to provide tear line reports, including improved tailored threat information, to these partners. I&A plans to ensure that the new policy guidance facilitates the provision of unclassified cyber threat information to a wider customer base in a time-sensitive manner to enable responsive mitigation actions. Additionally, I&A has worked with the Office of Director of National Intelligence National Counterterrorism Center to finalize a process for expediting tear lines in exigent circumstances.

### OIG Analysis

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

---

NPPD concurred with recommendation 2. A series of corrective actions are planned to improve information sharing, products, and mitigation strategies. In fiscal year 2011, the Department finalized a new *Government Performance and Results Act* performance measure in which a customer feedback survey will be attached to US-CERT and Industrial Control Systems Cyber Emergency Response Team products. It will assess how timely and actionable each product is while providing customers an opportunity to provide feedback directly to the Department.

NCSD will enhance the framework under which information sharing occurs. First, NCSD will prepare a white paper on current information sharing programs. Additionally, NCSD will complete the transition of the agreement underlying the Government Information Sharing Framework to a DHS/Financial Services ISAC agreement. NSCD also will create a comprehensive framework for DHS critical infrastructure information sharing agreements involving ISACs, IT providers, and other entities that manage or provide services to manage cyber networks and systems.

US-CERT is developing and deploying resources and process improvements that increase information sharing, such as implementing an Indicator Repository database and completing one Cyber Operational Resiliency Review assessment in partnership with a financial sector institution. Finally, the NCCIC and US-CERT will implement a comprehensive outreach initiative to ensure that DHS information sharing stakeholders understand their roles, responsibilities, and communication access points.

#### OIG Analysis

We agree that the steps NPPD plans to take satisfy the intent of this recommendation. This recommendation will remain open until NPPD provides documentation to support that all planned corrective actions are completed.

---

## DHS' Enforcement Authority

DHS does not have appropriate enforcement authority to help mitigate security incidents. Without this authority, DHS will continue to be hindered in its efforts to create a safe, secure, and resilient cyber environment.

We reported in June 2010 that US-CERT did not have the appropriate enforcement authority to ensure that agencies comply with mitigation guidance concerning threats and vulnerabilities.<sup>23</sup> Further, we reported that US-CERT needs the authority to enforce its recommendations so that federal agencies' systems and networks are protected from potential cyber threats.

According to *The National Strategy to Secure Cyberspace*, DHS is required to establish a public-private partnership to respond to and reduce the potential damage from cyber incidents. Additionally, the *National Infrastructure Protection Plan* stipulates that US-CERT, a partnership between DHS and the public and private sectors, is tasked to secure the nation's critical information systems infrastructure and coordinate the defense against and response to cyber attacks across the nation.

However, US-CERT was not given the authority to compel agencies to implement its recommendations to ensure that system vulnerabilities and incidents are remediated timely. US-CERT officials stated that the proposed *Federal Information Security Management Act of 2008* legislation would have given it some leverage to implement incident response and cybersecurity recommendations.<sup>24</sup> For example, the proposed legislation would have required agencies to address incidents that impair their security. Further, the agencies would have had to collaborate with others if necessary to address the incidents. Additionally, agencies would have been required to respond to incidents no later than 24 hours after discovery or provide notice to US-CERT as to why no action was taken. Finally, agencies would have had to ensure that information security vulnerabilities were mitigated timely. Since the proposed legislation was not enacted, US-CERT remains without enforcement authority.

US-CERT's products contain recommendations that address the threats and vulnerabilities in federal agencies' infrastructures. Additionally,

---

<sup>23</sup> U.S. Computer Emergency Readiness Team Makes Progress in Securing Federal Cyberspace, but Challenges Remain (OIG-10-94, June 2010).

<sup>24</sup> *Federal Information Security Management Act 2008* (Proposed Legislation), S. 3474, Calendar Number 1105, 110th Congress, Second Session.

---

US-CERT products help to update federal information security policy and guidance. Without the enforcement authority to implement recommendations, US-CERT will continue to be hindered in coordinating the protection of federal cyberspace.

## **Recommendation**

We recommend that the Under Secretary of NPPD:

**Recommendation #3:** Work with the administration to develop a legislative proposal for congressional consideration that will grant DHS appropriate enforcement authority to mitigate security incidents.

## **Management Comments and OIG Analysis**

NPPD concurred with recommendation 3. In May 2011, the administration transmitted a cybersecurity legislative proposal to Congress in response to Congress' call for assistance on how best to address the nation's cybersecurity needs. DHS worked closely with the White House and interagency partners to provide input and recommended language for this proposal.

### OIG Analysis

We agree that the steps NPPD has taken to satisfy the intent of this recommendation. This recommendation is closed.

## Appendix A

### Purpose, Scope, and Methodology

---

The objective of our audit was to determine DHS' capability to share cyber threat information as required by the *Intelligence Authorization Act for Fiscal Year 2010*. Specifically, we determined (1) how cyber threat information is shared among the agencies and departments of the United States and with persons responsible for the critical infrastructure; (2) the mechanisms by which classified cyber threat information is distributed; (3) the effectiveness of cyber threat information sharing and distribution; and (4) any other matters identified by the Inspector General that would help to fully inform Congress or the President regarding the effectiveness of cybersecurity programs.

Our review focused on DHS' cyber threat information sharing activities based on the requirements outlined in the *Homeland Security Act (2002)*, *The National Strategy to Secure Cyberspace (2003)*, *National Strategy for Information Sharing (2007)*, *Comprehensive National Cybersecurity Initiative (2009)* and *National Infrastructure Protection Plan (2009)*. We interviewed selected DHS officials. Additionally, we interviewed officials from the departments of Agriculture, Energy, Justice, State, Treasury, Veterans Affairs, and the Securities and Exchange Commission. Further we interviewed selected security personnel representing the finance, chemical, communication, energy, IT, postal and shipping, healthcare and public health, and transportation systems sectors regarding DHS' communication methods, systems, technologies, and tools used to share cyber threat information.

We conducted this performance audit between December 2010 and June 2011 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 D.

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

## Appendix B

### Management Comments to the Draft Report

---

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



**Homeland  
Security**

Mr. Charles K. Edwards  
Acting Inspector General  
DHS Office of Inspector General  
1120 Vermont Ave., NW  
Washington, D.C. 20005

RE: Draft Report OIG-11-078-ITA-I&A, *Review of DHS' Capability to Share Cyber-Threat Information*

Dear Mr. Edwards:

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the Office of Inspector General draft report for OIG-11-078-ITA-I&A, *Review of DHS' Capability to Share Cyber-Threat Information*. The Department, particularly the Office of Intelligence and Analysis (I&A), is actively resolving the issues identified in the report.

I&A appreciates the finding of the program evaluators that "DHS has taken actions to create an environment to promote cyber threat information sharing in support of its mission." DHS recognizes the importance of its mission to create a safe, secure and resilient cyber environment and promote awareness of cybersecurity in accordance with *Homeland Security Presidential Directive 7*. I&A understands the critical necessity of partnerships with Federal agencies, state and local governments, and the private sector to secure cyberspace, and appreciates the efforts your staff has undertaken to highlight the progress we have made to date, as well as areas of future improvement.

I&A's response to its assigned recommendation in the draft report can be found below:

**We recommend that the Under Secretary of I&A:**

**Recommendation #1:** Coordinate with the Office of Director of National Intelligence to develop policy on the right to release and share cyber threat and related information through tear line reports with the Intelligence Community, other federal agencies, and the private sector.

**DHS Response: Concur.** I&A is currently coordinating with the Office of the Director of National Intelligence (ODNI) on an initiative to develop updated Intelligence Community (IC) policy on releasing and sharing information through unclassified tearline reports with our customers, including those at other Federal agencies, state, local and tribal partners, and the private sector. This new IC-wide guidance is intended to recognize the evolving threat paradigm



## Appendix B

### Management Comments to the Draft Report

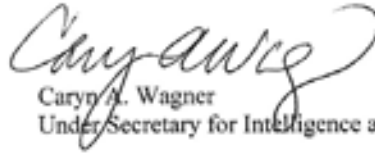
---

- 2 -

and codify the responsibilities and standards for the IC to provide tearline reports, including improved tailored threat information, to these partners. I&A has provided input to ODNI to begin to shape such a revised policy. I&A will ensure that the new IC policy guidance facilitates the provision of unclassified threat information (such as on cyber) to a wider customer base in a time-sensitive manner to enable responsive mitigation actions. In addition, we have worked with the ODNI National Counterterrorism Center to finalize a process for expediting tearlines in exigent circumstances.

I&A believes that this effort answers the intent of the recommendation and requests that it be closed. Again, we appreciate this opportunity to review and comment on the draft report. In addition to this response, technical comments and a sensitivity review were provided under separate cover. The Department looks forward to working with you on future Homeland Security engagements.

Sincerely,



Caryn A. Wagner  
Under Secretary for Intelligence and Analysis

## 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**

SEP 16 2011

Charles K. Edwards  
Acting Inspector General for Audits  
U.S. Department of Homeland Security  
Washington, DC 20528

Dear Mr. Edwards:

Re: *OIG Report 11-078-ITA-I&A, Review of Department of Homeland Security's Capability to Share Cyber Threat Information*

The Department of Homeland Security (DHS)/National Protection and Programs Directorate (NPPD) appreciates the opportunity to review and respond to the Office of Inspector General (OIG) report 11-078-ITA-I&A, *Review of Department of Homeland Security's Capability to Share Cyber Threat Information*. This audit was conducted as required by the Intelligence Authorization Act for Fiscal Year 2010.

DHS/NPPD is working to resolve the issues identified by the OIG. While the report notes progress made in creating and building the National Cybersecurity and Communications Integration Center (NCCIC), the OIG's findings do not accurately reflect the realities of creating a new organization. To illustrate this point, the NCCIC absorbed many of the government-wide responsibilities of the National Cyber Security Center (NCSC) and serves as the integration point for all cyber centers in the Comprehensive National Cybersecurity Initiative, as well as the various cyber components of DHS, Federal, State and local governments, and the private sector. The NCCIC continues to build personnel, capacity, and procedures to execute this complex task with a variety of interested stakeholders. This integration mission is facilitated by these parties' physical collocation in the NCCIC, but onboarding personnel (including representatives from the private sector) into a Top-Secret environment is a considerable challenge that takes time to implement.

It is also worth mentioning that the NCCIC's mission is clearly delineated from that of the United States Computer Emergency Readiness Team (US-CERT) in that NCCIC integrates and coordinates the information and efforts of its many partners—including US-CERT—to create and maintain a common operational picture for cyberspace. Despite the findings in the report, private sector companies and ISACs see the value and are interested in maintaining their daily presence on the NCCIC floor. Through these and other relationships, NCCIC continues to build its people, processes, and capabilities to deliver a cyber and communications common operational picture of national scope. DHS/NPPD has made significant progress in information sharing, but of course we recognize that improvements can be made. For example, US-CERT is executing an internal/external communications plan to improve shared cyber situational awareness. At the same time, the Department developed the National Cyber Incident Response Plan,

## Appendix B

### Management Comments to the Draft Report

---

which coordinates incident management, enhances data flow, and supports analytical collaboration among Federal, State and local government entities, and private sector partners.

The Department is focused on building relationships with critical infrastructure sector Information Sharing and Analysis Centers (ISACs), including the Multi-State ISAC (MS-ISAC) and those from the Banking and Finance, Information Technology, and Communications sectors. A final example of improved cybersecurity information sharing is the weekly Department/Agency Cybersecurity Activity Report (DCAR) that US-CERT distributes to 17 Federal agencies. Each agency-specific DCAR provides information to recipients based on malicious activity that US-CERT observes using the EINSTEIN system and other resources. DCARs also include suggested mitigation strategies. US-CERT also produces a weekly Federal enterprise DCAR. The agency-specific and enterprise-wide DCARs provide agencies with situational awareness of the malicious activity directed at them in the context of the larger Federal enterprise.

While the OIG report recognizes these and other successes, it does not identify two realities which serve as information-sharing constraints. First, while US-CERT is in a position to share its own information, it may not share third-party information without the permission of that third-party. Such information may be the proprietary information of a private sector partner or it may be law enforcement information provided to US-CERT by the U.S. Secret Service, the Federal Bureau of Investigation, or another law enforcement partner. US-CERT works diligently with private and public sector partners to package and disseminate their information in a manner that does not jeopardize their interests, but US-CERT must still obtain permission from the owner.

A second broader but associated reality is that effective bi-directional information sharing is based on trust and partnerships—whether they are public-private, public-public or private-private. US-CERT places a premium on such trust and guards each trust relationship it builds. The failure to do so by sharing proprietary information without permission would imperil existing relationships and hinder or even prevent the establishment of new relationships. During any incident for which US-CERT provides support, there is generally a sequence of events that occurs before US-CERT can broadly disseminate information. These events include obtaining necessary third-party permissions. Depending on the specifics surrounding the OIG's interviews with public and private sector partners, this sequencing can explain partners' perceptions of untimely information sharing during the incidents identified in the report. This important point is not addressed in the report.

Although these constraints can apply to any particular incident, the Department continues to build relationships and mechanisms to improve information sharing. To date, DHS has sponsored 1,272 SECRET and 49 TS/SCI (with an additional three pending read-in) clearances for critical infrastructure representatives. These clearances enable the exchange of sensitive information to more effectively protect national critical infrastructure. Many of these clearances were processed during the course of the audit.

## Appendix B

### Management Comments to the Draft Report

---

In addition, over the last several months, we have witnessed a few of our information sharing initiatives mature:

- The Department participates in the Government Information Sharing Framework (GISF) program, which is a partnership with the Department of Defense and the Financial Services ISAC (FS-ISAC) to share actionable cybersecurity threat and attack information with cleared members of the FS-ISAC. This information-sharing effort will allow the FS-ISAC and member firms of the Banking and Financial Services sector who participate in the FS-ISAC's Threat Intelligence Committee to improve network security, defense, and remediation efforts in our nation's financial services infrastructure.
- The Department participates in the Cross-Sector Information Sharing Framework (CSISF), which is an industry-formed operational integration of several ISACs and private sector entities. The CSISF established an operational private sector cybersecurity information-sharing capability, including a common repository for post-analytical industry-submitted cybersecurity data.
- Under the NCIRP, the Cyber Unified Coordination Group (UCG) replaced the National Cyber Response Coordination Group, and is an interagency and inter-organizational coordination body that incorporates public and private sector officials. The Cyber UCG is intended to operate both during steady state operations and incident response, and coordinates primarily through the NCCIC. Each member of the Cyber UCG has been pre-selected by the leadership of his or her agency or private sector organization to serve as a liaison responsible for harmonizing and synchronizing cyber operations, policies, and procedures related to cyber incident response activities.
- The Department supports the MS-ISAC so that it can provide managed security services to State, local, tribal and territorial (SLTT) partners. US-CERT coordinated a technology transfer of the EINSTEIN 1 Netflow Configuration model with the MS-ISAC, which the MS-ISAC is offering to SLTT entities as an alternative to full managed security services. As a result of this program, the MS-ISAC acts as a consolidated interface for US-CERT to support SLTT entities, expanding the Department's capability to reach SLTT governments while also providing protection to SLTT critical networks.
- The Critical Infrastructure Information Sharing and Collaboration Program (CISCP) is in the early stages of development, but the vision is to create a secure online portal for collaboration, where registered critical infrastructure sector entities can provide accurate, timely, and thorough information about current, emerging, and evolving technical threats to their networks. The portal will have the capability to process both non-attributional and Protected Critical Infrastructure Information attributional information. The Department's analysts will extract non-attributional data from submissions into the portal and produce tailored analysis and mitigation products based on those submissions.

## Appendix B

### Management Comments to the Draft Report

---

In early August, the Department's National Cyber Security Division (NCSD) held a workshop with representatives from each of these initiatives to discuss the current and future plans for the information sharing programs. The overall objectives of the workshop were to ensure that each program is working to its fullest potential, has a roadmap for any necessary expansion to additional stakeholders, and fits into an overall vision of information sharing activity between the Department and critical infrastructure participants.

***OIG Recommendation 1:*** *Coordinate with the Office of Director of National Intelligence to develop policy on the right to release and share information through tear line reports with the Intelligence Community, other Federal agencies, and the private sector.*

DHS Office of Intelligence and Analysis will provide this response.

***OIG Recommendation 2:*** *Improve communication with NCCIC and US-CERT partners and customers to address their concerns and needs regarding cyber threat information, products, and mitigation strategies.*

The Department concurs with this recommendation. A series of actions are planned to improve information sharing, products and mitigation strategies. In FY 2011, the Department finalized a new *Government Performance and Results Act* (GPRA) performance measure in which a customer feedback survey will be attached to US-CERT and Industrial Control Systems Cyber Emergency Response Team products. It will assess how timely and actionable each product is while providing customers an opportunity to provide feedback directly to the Department.

NCSD will enhance the framework under which information sharing occurs. First, NCSD will prepare a white paper on current information sharing programs, detailing how each program serves a distinct need, has a roadmap for any necessary expansion to additional stakeholders, and fits into an overall vision of information sharing activity between DHS and critical infrastructure representatives. Additionally, NCSD will complete the transition of the agreement underlying GISF to a DHS/FS-ISAC agreement. NCSD also will create a comprehensive framework for DHS critical infrastructure information sharing agreements involving ISACs, Information and Communications Technology providers, and other entities that manage or provide services to manage cyber networks and systems.

US-CERT is developing and deploying resources and process improvements that facilitate information sharing. First, US-CERT is implementing an Indicators Repository database, which is a malicious indicators collaborative resource available to all US-CERT constituencies. Second, it will complete one Cyber Operational Resiliency Review (CORR) assessment in partnership with a financial sector institution. This assessment will provide the financial services company, and the sector, insights to the threats facing these institutions. In addition, US-CERT will convert its watchlist to an XML-formatted,

## Appendix B Management Comments to the Draft Report

---

machine readable format, which will integrate the Indicators Repository and self-service data feeds. This will increase the ability to detect threats on the recipients' networks. US-CERT is also adding a Traffic Light Protocol—an International standard for information sharing—which informs partners at what levels information can be shared to secondary organizations. This not only helps US-CERT reinforce trusted information sharing relationships but also allows partners to disseminate that information appropriately to even wider communities.

Finally, the NCCIC and US-CERT will implement a comprehensive outreach initiative to ensure that DHS information-sharing stakeholders understand roles, responsibilities, and communication access points.

DHS/NPPD has established the following milestones to address this recommendation:

Key Milestones:		Original Target	Actual Completion
A	Implement new GPRA measure.	Q1FY2012	
B	Prepare a white paper on current Information Sharing programs.	Q3FY2012	
C	Transition GISF agreement.	Q1FY2012	
D	Create a comprehensive framework for DHS-critical infrastructure information sharing agreements.	Q4FY2012	
E	Implement an Indicators Repository database.	Q2FY2012	
F	Complete one CORR.	Q2FY2012	
G	Convert watchlist.	Q4FY2012	
H	Add Traffic Light Protocol to US-CERT products.	Q4FY2012	
I	Implement stakeholder outreach initiative.	Q2FY2012	

**Recommendation 3:** *Work with the Administration to develop a legislative proposal for congressional consideration that will grant DHS appropriate enforcement authority to mitigate security incidents.*

The Department concurs with this recommendation and has implemented it sufficiently. On May 12, 2011, the Administration transmitted a cybersecurity legislative proposal to Congress in response to Congress' call for assistance on how best to address the Nation's cybersecurity needs. DHS worked closely with the White House and interagency partners to provide input and recommended language for this proposal. For more information, please see <http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal>.

## Appendix B

### Management Comments to the Draft Report

---

Again, we thank you for the opportunity to review and provide comment on this draft report, and we look forward to working with you on future homeland security engagements.

Sincerely,



Rand Beers  
Under Secretary

#### Attachments

- 1) Technical comments
- 2) Sensitivity review

**Appendix C**  
**NCCIC's Operational Partners**

---

Communications ISAC  
Cyber Security Management Center  
Department of Defense  
Department of Transportation Federal Aviation Administration  
Department of the Treasury  
Departments and Agencies Security Operations Center  
Electricity Sector ISAC  
Energy ISAC  
Federal Bureau of Investigation  
Financial Services ISAC  
Immigration and Customs Enforcement Cyber Crimes Center  
Information Technology ISAC  
Intelligence Community-Incident Response Center  
Multi-State ISAC  
National Cyber Investigative Joint Task Force  
National Cybersecurity Center  
National Infrastructure Coordination Center  
National Operations Center  
National Response Coordination Center  
National Security Agency/Central Security Service National Threat  
Operation Center  
Surface Transportation ISAC  
United States Secret Service  
Water ISAC



**Appendix D**  
**Major Contributors to this Report**

---

Chiu-Tong Tsang, Director  
Tarsha Cary, Audit Manager  
Mike Horton, IT Officer  
Shannon Frenyea, Team Lead  
Amanda Strickler, Team Lead  
Megan Ryno, Program Analyst  
David Bunning, IT Specialist  
Bridget Glazier, IT Auditor  
Philip Greene, Referencer

## **Appendix E**

### **Report Distribution**

---

#### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretariat  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
Under Secretary, I&A  
Assistant Secretary, Cyber Security and Communications  
Chief Information Officer  
Deputy Chief Information Officer  
Chief Information Security Officer  
Director, NCCIC  
Director, NCSD  
Director, US-CERT  
Director, Compliance and Oversight Program  
Director, GAO/OIG Liaison Office  
Audit Liaison, I&A  
Audit Liaison, DHS/CISO  
Audit Liaison, DHS/CIO  
Audit Liaison, NPPD

#### **Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

#### **Congress**

Congressional Oversight and Appropriations Committees, as appropriate



#### ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at [www.dhs.gov/oig](http://www.dhs.gov/oig).

#### OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov); or
- Write to us at:  
DHS Office of Inspector General/MAIL STOP 2600,  
Attention: Office of Investigations - Hotline,  
245 Murray Drive, SW, Building 410,  
Washington, DC 20528.

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