



# Department of Homeland Security Office of Inspector General

## **U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain**



*Office of Inspector General*

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



**Homeland  
Security**

June 7, 2010

### 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 audits, inspections, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the U.S. Computer Emergency Readiness Team's (US-CERT) efforts to coordinate national cyber analyses and warnings against and response to attacks within the nation's critical infrastructure. It is based on direct observations and analyses of applicable documents. We obtained additional supporting documentation through interviews with selected personnel located in the National Cyber Security Division, US-CERT Program Office, Carnegie Mellon University – Software Engineering Institute, and selected federal agencies.

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 cursive script that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General

# Table of Contents/Abbreviations

---

Executive Summary .....	1
Background .....	2
Results of Audit .....	3
Actions Have Been Taken to Address Cybersecurity .....	3
Improvements Are Needed to Strengthen the Cybersecurity Program .....	5
Recommendations .....	11
Management Comments and OIG Analysis .....	11
Better Information Sharing and Communication Can Enhance Coordination Efforts With the Public .....	12
Recommendations .....	14
Management Comments and OIG Analysis .....	15
Improved Situational Awareness and Identification of Network Anomalies Can Better Protect the Cyberspace .....	17
Recommendation .....	21
Management Comments and OIG Analysis .....	21

## Appendices

Appendix A: Purpose, Scope, and Methodology .....	22
Appendix B: Management Comments to the Draft Report .....	24
Appendix C: Major Contributors to this Report .....	28
Appendix D: Report Distribution .....	29

# Table of Contents/Abbreviations

---

## Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GFIRST	Government Forum of Incident Response Security Team
NCCIC	National Cybersecurity and Communications Integration Center
NCSD	National Cyber Security Division
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
OMB	Office of Management and Budget
SOP	Standard Operating Procedure
US-CERT	U.S. Computer Emergency Readiness Team

# OIG

*Department of Homeland Security  
Office of Inspector General*

---

## **Executive Summary**

We reviewed the U.S. Computer Emergency Readiness Team's (US-CERT) efforts in coordinating national cybersecurity analyses and warning against and response to attacks against the nation's cyberspace. US-CERT leads a public-private partnership to protect and defend the nation's cyber infrastructure. It coordinates and facilitates information sharing among federal agencies, state and local governments, private sectors, academia, international partners, and the public on cybersecurity threats and attacks.

US-CERT has made progress in implementing a cybersecurity program to assist federal agencies in protecting their information technology systems against cyber threats. Specifically, it has facilitated cybersecurity information sharing with the public and private sectors through various working groups, issuing notices, bulletins, and reports, and web postings. Further, the Office of Cybersecurity and Communications has established a unified operations center that includes US-CERT to address threats and incidents affecting the nation's critical information technology and cyber infrastructure. To increase the skills and expertise of its staff, US-CERT has developed a technical mentoring program to offer cybersecurity and specialized training.

Still, US-CERT can further improve its analysis and warning program. For example, US-CERT must improve its management oversight by developing a strategic plan, establishing performance measures, and approving policies and procedures to ensure that its analysis and warning program is effective. It must also ensure that it has sufficient staff to perform its mission. Additionally, it should improve its information sharing and communications coordination efforts with the public. Finally, US-CERT needs to improve its situational awareness and identification capability by monitoring the federal cyber infrastructure for network anomalies in real-time.

We are making seven recommendations to the Under Secretary of the National Protection and Programs Directorate (NPPD). NPPD concurred with six of the seven recommendations and has

---

already begun taken actions to implement them. NPPD's response is included, in its entirety, as Appendix B.

## **Background**

The National Strategy to Secure Cyberspace provides the framework and guidance for national cybersecurity efforts, including responding to threats and incidents, reducing vulnerabilities, promoting outreach and awareness, training, and establishing partnerships through increased coordination among state and local governments, academia, international organizations, and the public and private sectors. Additionally, DHS is responsible for developing the national cyberspace security response system, which includes providing crisis management support and coordinating with other agencies to provide warning information.

The National Cyber Security Division (NCSA) created US-CERT in 2003 to protect the federal government network infrastructure by coordinating efforts to defend against and respond to cyber attacks. Specifically, US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating cyber incident response activities.

Additionally, US-CERT collaborates with federal agencies, the private sector, the research community, academia, state, local, and tribal governments, and international partners. Through coordination with various national security incident response centers in responding to potential security events and threats on both classified and unclassified networks, US-CERT disseminates cybersecurity information to the public.

US-CERT is comprised of the following four sections:

- Analysis – provides analytical insight into cyber activity; conducts technical analysis of data; and characterizes the threat, vulnerability, and incident.
- Business, Performance, and Planning – improves mission through integrated planning; provides oversight in management of the budget and program performance; and manages staffing efforts.

- 
- Detection – develops actionable intelligence from multiple sources; tracks and reports metrics from the sensor suite; and coordinates with Network Security Deployment and Federal Network Security.
  - Mission Management – maintains operations center; produces and reports threat information; and collaborates and coordinates with cybersecurity stakeholders.

NCSD developed Einstein to provide US-CERT with a situational awareness snapshot of the health of the federal government’s cyberspace. US-CERT manages Einstein and maintains its public website and secure portal to fulfill the mission. Technologies, such as Einstein, enable US-CERT to detect unusual and previously identified network traffic patterns and trends that signal unauthorized, threatening, or risky networks activities, and to categorize anomalous activity that could pose a risk to US-CERT constituents. US-CERT uses other systems in addition to Einstein. Through fusion of information received from all of these sources, US-CERT is able to prioritize and escalate cyber activity appropriately, coordinate incident response activities, and share alerts, warnings, and mitigation strategies around threats and vulnerabilities.

## **Results of Audit**

### **Actions Have Been Taken to Address Cybersecurity**

US-CERT has made progress in developing and implementing the capabilities to detect and mitigate cyber incidents across federal agencies’ networks. Similarly, US-CERT leads and coordinates efforts to improve the nation’s cybersecurity posture, promote cyber information sharing, and mitigate cyber risks.

For example, the Office of Cybersecurity and Communications developed the National Cybersecurity and Communications Integration Center (NCCIC), which is a unified operations center to address security threats and incidents that may affect the

---

nation's critical information systems and network infrastructure.<sup>1</sup> Specifically, the NCCIC helps DHS to fulfill its mission to secure cyberspace by supporting the decision making process for the federal government, and enabling incident response through shared situational awareness. As a result, the NCCIC serves as the "central repository" for the cyber protection efforts of the federal government and its private sector partners. Figure 1 shows the NCCIC's Watch Floor layout.



Figure 1. NCCIC Watch Floor.<sup>2</sup>

Source: US-CERT

Other actions designed to improve the expertise of US-CERT staff and information sharing include the following:

- Conducting in-person and online training to increase individual's knowledge, skills, and abilities regarding specific information topics that are relevant to US-CERT

---

<sup>1</sup> The NCCIC consists of the following organizations: National Communications System, National Coordinating Center; NCSD, US-CERT; NCSD, Industrial Control System Cyber Emergency Response Team; Office of Intelligence and Analysis; National Cybersecurity Center; Department and Agency, Security Operations Centers; Law Enforcement and Intelligence Community; and the private sector.

<sup>2</sup> The NCCIC is located in Arlington, VA and is equipped with wall-mounted screens to display maps and threat data. The NCCIC has a seating capacity of 60 personnel.



---

operations. Training relates to packet capture analysis and signature development; malware; and web browser security.<sup>3</sup>

- Participating in public and private sector working groups to promote information sharing and collaboration. The working groups assist in the coordination and mitigation of computer and cyber security incidents as well as the development of best security practices.
- Distributing US-CERT products regarding specific vulnerabilities and situational awareness, as well as quarterly trend and analysis reports, to public and private sectors.

While progress has been made, US-CERT still faces numerous challenges in reducing cyber security risks and protecting the nation's critical infrastructure. US-CERT must continue to improve its ability to analyze and reduce cyber threats and vulnerabilities and to disseminate information through a cohesive effort between public and private sectors.

## **Improvements Are Needed to Strengthen the Cybersecurity Program**

US-CERT is hindered in its ability to provide an effective analysis and warning program for the federal government in a number of ways. Specifically, US-CERT does not have the appropriate enforcement authority to help mitigate security incidents. Additionally, it is not sufficiently staffed to perform its mission. Further, US-CERT has not finalized performance measures and policies and procedures related to cybersecurity efforts.

### **Enforcement Authority Could Help Mitigate Security Incidents**

US-CERT does not have the appropriate enforcement authority to ensure that agencies comply with mitigation guidance concerning threats and vulnerabilities. It needs the authority to enforce its

---

<sup>3</sup> Packet capture involves reviewing the content of the data stream in the network traffic. Signature development consists of creating a mathematical algorithm to identify information in a message. Malware is malicious codes (e.g., viruses and worms) used to disrupt service.

---

recommendations so that federal agencies' systems and networks are protected from potential cyber threats. Without this authority, US-CERT is limited in its ability to mitigate effectively ever evolving security threats and vulnerabilities.

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 (NIPP) stipulates that US-CERT, a partnership between DHS and the public and private sectors, is tasked to secure the nation's critical infrastructure and coordinate the defense against and response to cyber attacks across the nation. Further, the NIPP requires agencies to cooperate with DHS in implementing protection efforts.

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 management officials stated that the proposed *Federal Information Security Management Act* (FISMA) 2008 legislation would have given it some leverage to implement incident response and cybersecurity recommendations.<sup>4</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 be 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 approved, US-CERT remains without enforcement authority.

US-CERT's notices contain recommendations that address the threats and vulnerabilities in federal agencies' infrastructures. Additionally, US-CERT products help to update federal information security policy and guidance. Without the enforcement authority to implement recommendations, US-CERT continues to be hindered in coordinating the protection of federal cyberspace.

---

<sup>4</sup> FISMA 2008 (Proposed Legislation), S. 3474, Calendar Number 1105, 110th Congress, Second Session.

---

### **Additional Staffing Could Help Meet Mission**

US-CERT does not have sufficient staff to perform its 24x7 operations as well as to analyze security information timely. US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch and information sharing and collaboration with state and local government, industry, and international partners. Without sufficient staffing, US-CERT cannot completely fulfill its responsibilities to analyze data and reports to reduce cyber threats and vulnerabilities as well as support the public and private sectors.

Although US-CERT's authorized positions were increased from 38 in 2008 to 98 in 2010, as of January 2010, only 45 positions are filled. In October 2009, the DHS Secretary announced that cybersecurity is an urgent priority for the nation and the department would hire additional cyber analysts, developers, and engineers to ensure that crucial computer networks are not vulnerable to possible cyber attacks. Currently, US-CERT augments its staffing shortages by contractor support.

Leadership turnover has hindered US-CERT's ability to hire and retain qualified staff. In the past 5 years, US-CERT has had four directors, and the director position has been unfilled until as recently as of April 2010. Further, due to the department's rigorous suitability clearance process, it takes US-CERT a significant amount of time to fill its critical positions. According to a former director, it takes 9 to 12 months for new applicants to begin working at US-CERT even if they already have a top secret clearance. As a result, staffing shortages force current analysts to perform additional duties, instead of fulfilling the technical analyst role for which they were hired.

### **Strategic Plan is Needed**

US-CERT has not developed a strategic plan to formalize goals, objectives, and milestones. Specifically, US-CERT has not identified or prioritized key activities for the division to monitor its progress in accomplishing its mission and goals. Without a strategic plan, US-CERT may have difficulty in achieving its goal to provide response support and defense against potential cyber attacks for the federal government.

---

The Comprehensive National Cybersecurity Initiative requires that the future cybersecurity environment be strengthened by defining and developing strategies to deter hostile and malicious activity in cyberspace. Additionally, the *Government Performance Results Act* requires agencies to develop strategic plans for program activities.

According to program officials, US-CERT is developing a strategic plan. This strategic plan should describe how US-CERT will perform its critical role by identifying and aligning goals, objectives, and milestones through a variety of means and strategies. Also, the strategic plan should contain performance measures related to specific programs, initiatives, products, and outcomes.

As the sophistication and effectiveness of cyber attacks have been steadily advancing in recent years, a strategic plan can help US-CERT to ensure that critical milestones and goals are accomplished in a timely manner. Further, a strategic plan can improve program operations by promoting the appropriate application of information resources.

### **Performance Measures are Needed to Assess the Effectiveness of US-CERT**

US-CERT has not formalized performance measures to direct and monitor its efforts to accomplish its mission and goals. Without sufficient outcome measures, US-CERT cannot effectively assess its program activity against its intended results.

Performance measures indicate whether a program is meeting its goals and achieving expected results. Further, performance measures address the direct products and services delivered by a program (outputs) and the results of those products and services (outcomes). Outcomes are important as they often describe the intended results or consequences that will occur from carrying out a program or activity.

The NIPP requires that a performance measure based system be used to provide feedback on efforts to attain the goals and supporting objectives of the programs implemented. Measures provide a basis for establishing accountability, documenting actual performance, promoting effective management, and providing a feedback mechanism to decision makers. Additionally,

---

performance measures offer a quantitative assessment to affirm that specific objectives are being met and gaps are identified in the national effort or individual agencies' efforts.

During our audit, US-CERT was in the process of developing performance measures. To date, US-CERT has provided the following performance measures to monitor its cybersecurity efforts for two of its four sections:

- Percent of funds obligated.
- Staffing level (filled or pending versus available).
- The percent of reduction in false positive rates in the Einstein.
- US-CERT operation's average time from the point a logged incident is assigned a severity level in the system to the point where a product to mitigate that incident is delivered.
- Percent of unique high alert level events detected by the Einstein validated as legitimate incidents.
- Creation of monthly metrics reports for each Einstein 2 agency.

After fieldwork, US-CERT officials informed us that they are currently revising the performance measures they developed to align with the goals, objectives, and key outcomes outlined in the strategic plan. They are currently not tracking the performance measures listed above.

Without outcome-based performance measures, US-CERT cannot track its or other public and private sectors' progress in managing cybersecurity risks and threats efficiently and effectively. Additionally, the performance measures and strategic plan will aid US-CERT in evaluating its progress in building an effective organization capable of mitigating long-term cyber threats and vulnerabilities.

---

## **Policies and Procedures Have Not Been Approved**

US-CERT has not approved its policies and procedures to ensure that management and operational controls are implemented to defend against, analyze, and respond to cyber attacks. Without the approved policies and procedures, US-CERT may be hindered in its ability to respond to security incidents effectively and promote continuity of operations and consistency.

Leadership and staff turnover and a continually evolving mission have hindered US-CERT's past efforts to update its standard operating procedures. Under the prior director, US-CERT outsourced to contractors off-site the function to maintain and update procedures. The process of updating the procedures discontinued once the director departed. Further, US-CERT officials determined that the outsourced procedures did not fully address the mission or the day-to-day activities that cyber analysts encounter. According to the officials, outsourcing off-site was not the best method to update these policies and procedures since US-CERT personnel have a better understanding of its mission. After internal reassessment, US-CERT officials decided to use contractor support on-site to develop more concise and direct SOPs.

Currently, US-CERT is in the process of developing approximately 80-90 standard operating procedures (SOP) for its four sections pertaining to various areas of activity, such as, network and targeted analyses, malware submission handling, and signature template development. The goal is to have a structure that maps to functions, roles, the organization, and the mission. US-CERT is attempting to make the procedures understandable and practical with contents based on analysts' experiences.

According to the *Homeland Security Act of 2002*, the head of each agency is responsible for implementing and overseeing an information security program as well as developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements. Additionally, Office of Management and Budget (OMB) Circular Appendix -123, Management's Responsibility for Internal Controls defines policies, and procedures as tools to help program managers achieve results and safeguard the integrity of their programs.

---

## Recommendations

We recommend that the Under Secretary of NPPD require the Director of NCSD to:

**Recommendation #1:** Establish specific outcome-based performance measures and a strategic plan to ensure that US-CERT can achieve its mission, objectives, and milestones.

**Recommendation #2:** Approve policies and procedures to ensure that US-CERT can effectively detect, process, and mitigate incidents as well as perform its roles and responsibilities in a consistent manner.

## Management Comments and OIG Analysis

NPPD concurred with recommendation 1. In April 2010, US-CERT released planning guidance to detail how US-CERT will conduct mission and resource planning; establish planning priorities; identify interrelationships between planning efforts; assign responsibilities for planning; and identify general timelines for its planning effort. US-CERT is developing a strategic plan that will map outcome-based objectives to the mission goals and identify performance measures that are measurable, attainable, realistic, and timely. Through these performance measures, US-CERT will continually evaluate its organizational performance to determine whether projects and initiatives are achieving desired results and to select improvement initiatives with the greatest positive organizational impact. US-CERT plans to complete the strategic plan and identify performance measures by July 15, 2010.

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

NPPD concurred with recommendation 2, insofar as there is a need for US-CERT to approve and review SOPs regularly to ensure that US-CERT can perform the roles and responsibilities in a consistent manner, including the detection, analysis and mitigation of incidents. Specific operational procedures, internal functions, and processes are defined within supporting SOPs that are approved by US-CERT leadership. Due to its operational nature, the dynamic

---

threat, and evolving cyber community (including within DHS), US-CERT officials stated that it cannot accurately determine the number of SOPs that may be required, as new SOPs are often identified on a regular basis and SOPs are sometimes combined to improve coordination efficiency within US-CERT. Once approved, an SOP will be reviewed at least bi-annually.

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

### **Better Information Sharing and Communication Can Enhance Coordination Efforts With the Public**

US-CERT needs to improve its information sharing and communication efforts with federal agencies to ensure that threats and vulnerabilities are mitigated timely. Specifically, officials from other federal agencies expressed concerns that US-CERT was unable to share near real-time data and classified and detailed information to address security incidents.

We interviewed officials from eight federal agencies to obtain feedback on Einstein and to determine whether US-CERT shared sufficient information and communicated effectively. Overall, these agency officials indicated that Einstein is an effective tool but expressed concerns regarding the effectiveness of US-CERT's information sharing and communication.

Officials from six agencies expressed concerns regarding US-CERT not sharing Einstein data and analysis results. According to some of the federal agency officials we interviewed, US-CERT agreed that they would have access to the Einstein flow data but subsequently did not provide the information. This data could assist agencies in performing analyses with their locally collected data to identify potential threats and vulnerabilities. Also, agency officials stated that it would be helpful for US-CERT to list which agencies are being attacked and provide common trends to other agencies to determine whether the incident is isolated or systemic.



---

Further, agencies indicated that US-CERT has not provided sufficient training on the Einstein program. Some agencies indicated that they received compact disk, portable document format brochures, and handbooks about the Einstein program, while other agencies received nothing. Agencies indicated that they would like to receive additional Einstein training from US-CERT.

US-CERT officials acknowledged that there are communications issues regarding sharing classified and detailed information with other agencies. For example, US-CERT collects and posts information from several systems and sources to different portals, all of which have different classification levels. As a result, US-CERT officials believe that communications needs could be best addressed by developing a consolidated information sharing portal. The consolidated portal could provide a multiple classification platform and serve as a central repository to meet the needs of the stakeholders.

A challenge US-CERT faces is that many intelligence agencies communicate classified information on Top Secret/Sensitive Compartmented Information networks. Since not all agencies have access to classified networks, US-CERT is limited in what it can convey. Some agencies do not have secure facilities, equipment, and cleared personnel to send or receive classified information.

Additionally, US-CERT has to deal with the various network architectures of the different agencies. Since US-CERT does not have access to each agency's architecture, it is imperative to have the agency Chief Information Officer (CIO) and Chief Information Security Officer (CISO) involved in addressing cyber activities. Establishing direct, regular communication with agency CIOs/CISOs or key security assurance personnel ensures that US-CERT's cybersecurity efforts are implemented. For example, US-CERT and the CIO/CISO can determine what should be implemented to improve the agency's situational awareness. Further, they can address network and cybersecurity challenges such as fragmented infrastructures, legacy systems, and limited budgets.

Currently, US-CERT uses working groups and portals to share information with the public and private sectors. For example, US-CERT established the Joint Agency Cyber Knowledge Exchange and Government Forum of Incident Response and

---

Security Teams (GFIRST) to facilitate collaboration on detecting and mitigating threats to the “.gov” domain and to encourage proactive and preventative security practices. The Joint Agency Cyber Knowledge Exchange meetings are held at a classified level to discuss threat-related tactics, techniques, and protocol. Additionally, US-CERT disseminates various reports and notices through the GFIRST and US-CERT portals.<sup>5</sup> These products contain a summary of the incident, mitigation strategies, and best practices. The products are disseminated to stakeholders on an as-needed, daily, monthly, or quarterly basis.

It is essential that US-CERT and the public and private sectors share cybersecurity information to ensure that appropriate steps can be taken to mitigate the potential effect of a cyber incident. US-CERT cannot defend against and respond consistently and effectively to cyberactivity without other agencies’ involvement. By sharing potential security threats collected through its data sources, US-CERT can provide agencies with detailed information regarding attacks to their networks.

## **Recommendations**

We recommend that the Under Secretary of NPPD require the Director of NCS&D to:

**Recommendation #3:** Improve communications with federal agency CIOs and CISOs to address their concerns, to identify areas of improvement about the program, and to enhance US-CERT’s ability to combat cybersecurity challenges.

**Recommendation #4:** Establish a consolidated, multiple classification level portal that can be accessed by the federal partners that includes real-time incident response related information and reports.

**Recommendation #5:** Develop a process to distribute and share Einstein trends, anomalies, and common/reoccurring attacks with other federal agencies.

---

<sup>5</sup> Products US-CERT disseminates include: Situational Awareness Reports, Critical Infrastructure Information Notices, Federal Information Notices, Early Warning Indicator Notices, and Malware Initial Findings Reports.

---

**Recommendation #6:** Provide training to federal agencies on using available features of Einstein to foster better cooperation in analyzing and mitigating security incidents.

## **Management Comments and OIG Analysis**

NPPD concurs with recommendation 3. US-CERT recognizes the need for stronger communication with departments and agencies. Moreover, US-CERT must maintain a technical interchange with agency security operation centers and relationships with departments and agencies to share cybersecurity posture information regarding their agency and how they can enhance it.

US-CERT offers multiple products, services, and forums to support agency engagement. Recently, US-CERT has been providing contextual classified and unclassified briefings to agency CIO offices and their staff on the cyber threat. US-CERT is also evaluating an agency-specific product that would help each agency understand the Einstein 2 activity identified in context of the larger, consolidated dataset of on-going attacks and threats. US-CERT is planning to distribute this agency-specific product by the end of Fiscal Year (FY) 2010. Additionally, US-CERT is developing a more comprehensive information sharing and collaboration environment as part of its Einstein program to support continuous communications on vulnerabilities, indicators, and mitigation with initial deployment planned for FY 2012. As US-CERT's goal is to hire additional staff in FY 2011 and FY 2012, US-CERT plans to establish better outreach strategies, such as a customer advocacy program wherein each agency would have a specific contact person at US-CERT with whom to interact. This will enable US-CERT to maintain a more proactive relationship with each agency. US-CERT plans to draft the Outreach Strategy by the second quarter of FY 2011.

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

NPPD concurs with recommendation 4 and agrees with the need to share information and collaborate with federal partners across multiple levels of classification. However, US-CERT currently generates very limited classified data to be shared with federal agencies. This limits the efficiencies that would be realized by

---

creating a multiple classification level portal. As US-CERT's capabilities continue to grow, it is anticipated that increasing amounts of classified data will be produced. Prior to implementing a multiple classification level portal, US-CERT will assess the feasibility of various portal models and create one at the appropriate level of classification.

In the meantime, US-CERT is developing a strategy for an information sharing environment that can be employed at all levels of classification. US-CERT is developing a more robust information sharing and collaboration environment across its private and public sector constituents with the initial deployment planned for FY 2012. Additionally, US-CERT will develop a more effective information sharing and collaboration presence on the classified networks.

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

NPPD concurs with recommendation 5. US-CERT is currently evaluating an agency-specific product that would help each agency understand the activity that Einstein detects for that agency against aggregated constituent data. US-CERT is prototyping the report and plans to provide fully processed products to agencies by the end of FY 2010. As part of the Einstein 2 effort, US-CERT is also developing an information sharing portal to enable each agency to have a direct view of its serialized Einstein data and to be able to compare that to the broader federal community.

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

NPPD concurs with recommendation 6. Currently, federal agencies only have access to netflow data within Einstein. The NCSD's Network Security Deployment Branch is responsible for Einstein deployment and discusses netflow data access with the federal agency during system installation. The Network Security Deployment Branch will ensure that a discussion and instructions on how to access flow data is included as a formal agenda item during each Einstein deployment. Additionally, US-CERT will be

---

evaluating netflow and other Einstein training requirements for federal agencies and will provide periodic training in FY 2011.

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

### **Improved Situational Awareness and Identification of Network Anomalies Can Better Protect Federal Cyberspace**

US-CERT is unable to monitor federal cyberspace in real time. The tools US-CERT uses do not allow real-time analyses of network traffic. As a result, US-CERT will continue to be challenged in protecting the federal cyberspace from security-related threats.

Currently, US-CERT maintains near real-time situational awareness as it performs information aggregation activities. US-CERT collects data real-time but it must perform analysis on the data in near real-time. Cyber analysts receive information from a variety of sources and other US-CERT activities to identify potential incidents and to assess their possible scope and impact on the nation's cyber infrastructure (see Figure 2).

---

# Information Workflow

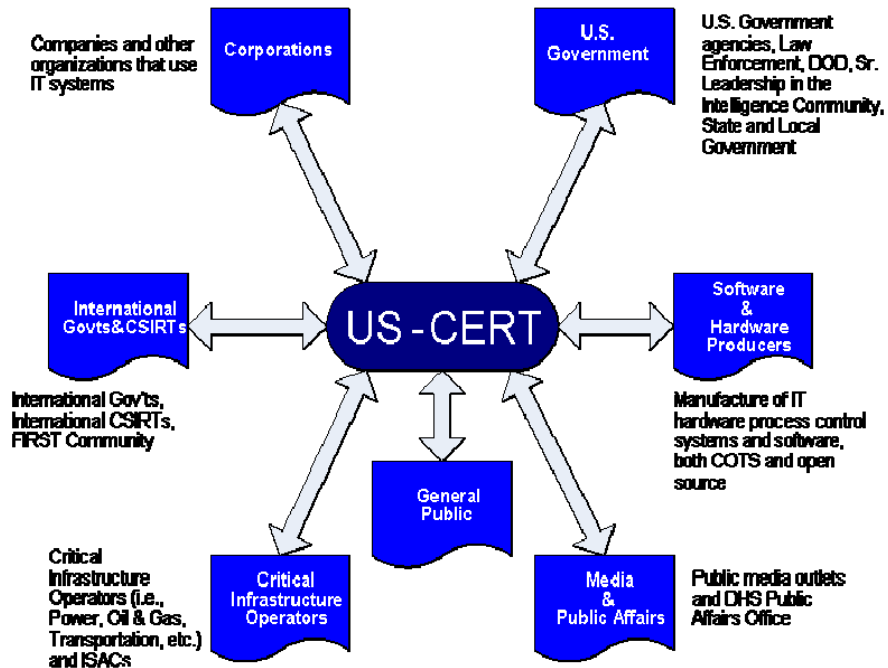


Figure 2. US-CERT's Information Workflow. Source: US-CERT

Einstein is being deployed in three different versions, whereby, each builds on the capabilities of the previous version:

- Einstein 1 (E1) collects and relies on net flow analysis capability and uses net flow collectors. Net flow data is queried for analysis.
- Einstein 2 (E2) is an intrusion detection system, but is still passive, performing analysis while traffic is continuous.<sup>6</sup> E2 looks for anomalous activity from net flow information based on every session between two computers on the internet. E2 is more beneficial for detecting and mitigating cyber incidents because of its ability to analyze packet data. Additionally, E2 performs full session packet analysis.

---

<sup>6</sup> Intrusion detection is the process of monitoring the events occurring in a computer systems or network and analyzing them for signs of possible incidents that violate or imminently threaten to violate of computer security policies, acceptable use policies, or standard security practices.

- 
- Einstein 3 (E3) draws on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision making on network traffic entering or leaving the executive branch networks.<sup>7</sup> This system also deploys an intrusion prevention feature.<sup>8</sup>

Additionally, US-CERT employs technology, systems, and tools to fulfill its mission requirements to protect and defend the nation's infrastructure against potential threats from cyberspace, and respond to security incidents. Currently, US-CERT uses the following list of tools to detect and mitigate cybersecurity incidents: Remedy, SiLK, Sharepoint, Wire Shark, Jabber Server, Deep Sight, and Sourcefire.

With Einstein, US-CERT can gather more network traffic information and identify cyber activity patterns. However, US-CERT cannot capture all network traffic because Einstein has not been deployed to all federal agencies. Initially, the deployment of E1 to federal agencies was entirely voluntary. In September 2008, OMB made Einstein part of the Trusted Internet Connections initiative and required all agencies to install sensors on their networks.<sup>9</sup>

As of October 2009, NCSA's Network Security Deployment Branch had deployed E1 to 19 agencies and E2 to 8 agencies. Currently, US-CERT is conducting a pilot exercise of E3 to evaluate its capabilities. According to the Comprehensive National Cybersecurity Initiative and US-CERT officials, E3 will contain real-time full packet inspection and an intrusion prevention feature. These additions should give US-CERT better response and monitoring capabilities.

According to US-CERT officials, many agencies have not installed Einstein because they have not consolidated their gateways to the

---

<sup>7</sup> Packet inspection refers to performing some type of stateful protocol analysis, often combined with a firewall capability that can block communications determined to be malicious.

<sup>8</sup> Intrusion prevention is the process of performing intrusion detection and attempting to stop possible incidents.

<sup>9</sup> OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection Compliance*, September 2008. OMB Memorandum M-08-05, *Implementation of Trusted Internet Connection*, November 2007 defined the purpose of Trusted Internet Connections initiative as an approach to optimize individual agency network services into a common solution for the federal government to reduce its external connections, including internet points of presence.

---

Internet. Further, some agencies have fragmented networks and must upgrade their architectures before Einstein can be deployed.

Additionally, US-CERT does not have an automated correlation tool to identify trends and anomalies. With this vast amount of network traffic, US-CERT experienced a long lead time to analyze potential security threats or abnormalities. To reduce the lead time, NCSD purchased an automated correlation tool to analyze the vast amount of data from Einstein.<sup>10</sup> However, US-CERT is currently experiencing problems with reconfiguring the tool to collect data and understand the overall data flow. US-CERT management stated that it may be 6 months before the problems are corrected and the benefits of the system can be seen.

According to the *Homeland Security Act of 2002*, DHS shall 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 departments and agencies, state and local governments, and the private sector in a timely manner. Further, The National Strategy to Secure Cyberspace recommends that DHS coordinate with other federal agencies to share specific warning information and advice about appropriate protective measures and countermeasures.

An effective analysis and warning program is critical to secure the federal information technology infrastructure. For US-CERT to perform its responsibilities successfully, it must have sufficient state-of-the-art technical and analytical tools and technologies to identify, detect, analyze, and respond to cyber attacks. Additionally, cybersecurity information can provide the public and private sectors with valuable input for mitigating risks and threats, protecting against malicious attacks, and prioritizing security improvement efforts.

---

<sup>10</sup> The automated correlation tool is an event management tool that takes and correlates information from both Sourcefire and SiLK. It will be used to write an event filter if two events occur – connection and detection.



---

## Recommendation

We recommend that the Under Secretary of NPPD require the Director of NCSD to:

**Recommendation #7:** Establish a capability to share real time Einstein information with federal agencies partners to assist them in the analysis and mitigation of incidents.

## Management Comments and OIG Analysis

NPPD did not concur with recommendation 7 to the extent it relates to E2. US-CERT bases the implementation of signatures in E2 on current threats to the federal government. As a result of the events triggered by the signatures, US-CERT is working to provide federal agencies with serialized, near real-time analysis reports derived from E2 data. NPPD officials stated that while some departments and agencies with E1 netflow sensors installed have access to netflow data, that access is not real-time or near real-time. Additionally, NPPD maintained that no such access was ever contemplated by the program. Moreover, for a variety of reasons, ranging from volume of data, need for validation via analysis/processing and classification issues, neither the current E2 deployment, nor the planned E3 solution contemplate sharing unprocessed raw intrusion detection system and intrusion prevention system data with departments and agencies in near real-time.

We consider this recommendation unresolved and will require additional discussion between our offices before disposition. We maintain that due to the dynamic nature of cyber attacks, NPPD should ensure that the least amount of time is used to analyze potential threat and vulnerability data and share the information with other federal agencies in a timely manner to facilitate prompt actions that would minimize the impact of the risk. As a result, NPPD needs to reposition itself from being reactive to proactive in responding to potential risks.

## Appendix A

### Purpose, Scope, and Methodology

---

The objective of our audit was to determine whether US-CERT is effective in its efforts to coordinate national cyber analyses and warnings against and response to attacks within the nation's critical infrastructure. Specifically, we determined whether US-CERT:

- Has implemented an effective national cyber analysis and warning program to protect against cyber attack.
- Is properly managing its collaborative efforts to coordinate and facilitate information sharing on cybersecurity issues among the public and private sectors.
- Is properly administering its tools to assess situational awareness of the cyberspace and identify network anomalies spanning the federal government.

Our review focused on US-CERT's operations based on the requirements outlined in Homeland Security/ Presidential Directive 7, *National Infrastructure Protection Plan* (2009), *The National Response Framework* (January 2008), *The National Strategy to Secure Cyberspace* (February 2003), *The Comprehensive National Cybersecurity Initiative*, and Office of Management and Budget Memorandums for the *Government Performance and Results Act*. We interviewed selected US-CERT and NCSID management officials, as well as personnel from the DHS Network Operations Center/Security Operations Center. Further, we interviewed personnel from departments of Agriculture, Education, Interior, Justice, State, and Transportation, Executive Office of the President, and United States Agency for International Development regarding US-CERT's communication methods, information sharing, tools, incident management, and cybersecurity concerns.

We conducted our fieldwork at both program and management levels and visited the Federally Funded Research and Development Center at Carnegie Mellon University in Pittsburgh, Pennsylvania. We conducted this audit between October 2009 and March 2010 according to generally accepted government auditing standards. Those standards require that we plan and perform a reasonable basis for our findings and conclusions based on our audit

## **Appendix A**

### **Purpose, Scope, and Methodology**

---

objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Major OIG contributors to the audit are identified in Appendix D.

The principal OIG points of contact for the audit are Frank W. Deffer, Assistant Inspector General, Information Technology Audits, at (202) 254-4041, and Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

## 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**

MAY 20 2010

### INFORMATION MEMORANDUM

MEMORANDUM TO: Frank Deffer  
Assistant Inspector General

FROM: Rand Beers   
Under Secretary

SUBJECT: Response to Office of Inspector General Draft Report, *U.S. Computer  
Emergency Readiness Team Makes Progress in Securing Federal  
Cyberspace, but Challenges Remain*

This correspondence responds to your April 7, 2010, memorandum requesting the National Protection and Programs Directorate's (NPPD) comments to the Office of Inspector General (OIG) draft report, *U.S. Computer Emergency Readiness Team (US-CERT) Makes Progress in Securing Federal Cyberspace, but Challenges Remain*.

First, we sincerely appreciate the opportunity to respond to the draft report. In addition to this response memo, we are providing related supporting documents under separate cover.

The OIG reports a finding that *Enforcement Authority Could Help Mitigate Security Incidents*, but does not provide a corresponding recommendation. The Department of Homeland Security (DHS) has broad authority related to directing and supporting the operation and defense of Federal systems which is drawn from the Homeland Security Act, the Federal Information Security Management Act (and related Office of Management and Budget guidance), Homeland Security Presidential Directive 7, and Homeland Security Presidential Directive 23. NPPD agrees, however, that codification and/or clarification of DHS authorities in these areas could assist US-CERT in coordinating the mitigation of cyber incidents that could negatively impact Federal cyber infrastructure.

Responses to the seven recommendations directed to NPPD are set forth below. Questions concerning specific comments should be addressed to Michael McPoland, Director, NPPD GAO-OIG Audit Liaison Office at 703-235-2175.

We thank you for the opportunity to work with the OIG during this engagement and look forward to continuing this partnership in the future.

**U.S. Computer Emergency Readiness Team Makes Progress in Securing Federal Cyberspace, but  
Challenges Remain**

## Appendix B

### Management Comments to the Draft Report

---

**Recommendation #1:** *Establish specific outcome-based performance measures and a strategic plan to ensure that US-CERT can achieve its mission, objectives, and milestones.*

**Response:**

NPPD concurs with this recommendation. To begin development of a strategic plan, US-CERT held two facilitated offsite leadership team meetings in October 2009. These sessions allowed US-CERT to define its mission based on authorities and DHS strategies and to establish a five-year vision. In April 2010, US-CERT released planning guidance to detail how it will conduct mission and resource planning; establish planning priorities; identify interrelationships between planning efforts; assign responsibilities for planning; and identify general timelines for its planning efforts. The planning guidance memo is provided under separate cover.

US-CERT is developing a strategic plan that will map outcome-based objectives to the mission goals and identify performance standards that are measurable, attainable, realistic, and timely. Through these performance measures, US-CERT will continually evaluate its organizational performance to determine whether projects and initiatives are achieving desired results and to select improvement initiatives with the greatest positive organizational impact. US-CERT plans to complete the Strategic Plan and identify performance measures by July 15, 2010.

**Recommendation #2:** *Finalize policies and procedures to ensure that US-CERT can effectively detect, process, and mitigate incidents as well as perform its roles and responsibilities in a consistent manner.*

**Response:**

NPPD concurs with this recommendation insofar as there is a need for US-CERT to approve and regularly review standard operating procedures (SOPs) to ensure that US-CERT can perform the roles and responsibilities of its mission in a consistent manner, including the detection, analysis and mitigation of incidents. US-CERT's operating guidance is established through its Concept of Operations Plan (CONOPS) and through supporting SOPs. US-CERT began using an operational draft of its CONOPS on March 1, 2010. The CONOPS provides a framework for the implementation of US-CERT's operational capabilities necessary to accomplish its mission and is not intended to define US-CERT's governance structure. Specific operational procedures, internal functions, and processes are defined within supporting SOPs that are approved by US-CERT leadership. Due to its operational nature, the dynamic threat, and evolving cyber community (including within DHS), US-CERT cannot accurately baseline the number of SOPs that will be required, as new SOPs are often identified on a regular basis and SOPs are sometimes combined to improve coordination efficiency within US-CERT. Once approved, an SOP will be reviewed at least bi-annually.

**Recommendation #3:** *Improve communications with Federal agency CIOs and CISOs to address their concerns, to identify areas of improvement about the program, and to enhance US-CERT's ability to combat cybersecurity challenges.*

**Response:** NPPD concurs with this recommendation. US-CERT recognizes the need for stronger communication with departments and agencies. Moreover, US-CERT must maintain a technical interchange with agency security operation centers and relationships with departments

## Appendix B

### Management Comments to the Draft Report

---

and agencies to share cybersecurity posture information and how they can enhance it for their agency.

US-CERT offers multiple products, services, and forums to support agency engagement. Recently, US-CERT has been providing contextual classified and unclassified briefings to agency CIO offices and their staff on the cyber threat. US-CERT is also evaluating an agency-specific product that would help each agency understand the EINSTEIN 2 activity identified in context of the larger, consolidated dataset of ongoing attacks and threats. US-CERT is planning to distribute this agency-specific product by the end of FY2010. Additionally, US-CERT is developing a more comprehensive information sharing and collaboration environment as part of its EINSTEIN program to support continuous communications on vulnerabilities, indicators, and mitigation (see response to the next recommendation) with initial deployment planned for FY2012. As US-CERT hires additional staff in FY2011 and FY2012, it plans to establish better outreach strategies, such as a customer advocacy program wherein each agency would have a specific contact person at US-CERT with whom to interact. This will enable US-CERT to maintain a more proactive relationship with each agency. US-CERT plans to draft the Outreach Strategy by the second quarter of FY2011.

**Recommendation #4:** *Establish a consolidated, multiple classification level portal that can be accessed by the Federal partners that includes real-time incident response related information and reports.*

**Response:** NPPD concurs with this recommendation and agrees with the need to share information and collaborate with Federal partners across multiple levels of classification. However, US-CERT currently generates very limited classified data to be shared with Federal agencies. This limits the efficiencies that would be realized by creating a multiple classification level portal. As US-CERT's capabilities continue to grow, it is anticipated that increasing amounts of classified data will be produced. Prior to implementing a multiple classification level portal, US-CERT will assess the feasibility of various portal models and create one at the appropriate level of classification.

In the meantime, US-CERT is developing a strategy for an information sharing environment that can be employed at all information security levels. US-CERT maintains information sharing sites on a public-facing Internet site, a portal secured by two-factor authentication, and classified networks to encourage collaboration among constituents and disseminate audience-specific alert and warning information. US-CERT is developing a more robust information sharing and collaboration environment across its private and public sector constituents with the initial deployment planned for FY2012. Additionally, US-CERT will develop a more effective information sharing and collaboration presence on the classified networks.

Improved information sharing and collaboration using classified networks is being enabled, in part, by Federal agency implementation of the Office of Management and Budget and DHS-led Comprehensive National Cybersecurity Initiative's (CNCI) Trusted Internet Connections (TIC). Specifically, the TIC Reference Architecture requires that each agency serving as a TIC Access Provider (TICAP) satisfy 51 critical capabilities, including maintenance of appropriately credentialed 24x7 staffing, the capability to handle any national security information based on the requirements established by the Committee for National Security Systems, and the capability

## Appendix B

### Management Comments to the Draft Report

---

to house Top Secret - Sensitive Compartmented Information (TS/SCI) equipment in a compartmented secure facility. A copy of the TIC Reference Architecture is provided under separate cover.

**Recommendation #5:** *Develop a process to distribute and share Einstein trends, anomalies, and common/reoccurring attacks with other Federal agencies.*

**Response:** NPPD concurs with this recommendation. US-CERT is currently evaluating an agency-specific product that would help each agency understand the activity that EINSTEIN detects for that agency against aggregated constituent data. US-CERT is prototyping the report and plans to provide fully processed products to agencies by the end of FY2010. As part of the EINSTEIN 2 effort, US-CERT is also developing an information sharing portal to enable each agency to have a direct view of its serialized EINSTEIN data and to be able to compare its data with that of the broader Federal community.

**Recommendation #6:** *Provide training to Federal agencies on using available features of Einstein to foster better cooperation in analyzing and mitigating security incidents.*

**Response:** NPPD concurs with this recommendation. Currently, Federal agencies only have access to netflow data within EINSTEIN. The National Cyber Security Division's Network Security Deployment Branch is responsible for EINSTEIN deployment and discusses netflow data access with the Federal agency during system installation. The Network Security Deployment Branch will ensure that a discussion and instructions of how to access flow data is included as a formal agenda item during each EINSTEIN deployment. In addition, US-CERT will be evaluating netflow and other EINSTEIN training requirements for Federal agencies and will provide periodic training in FY2011.

**Recommendation #7:** *Establish a capability to share real time Einstein information with Federal agencies partners to assist them in the analysis and mitigation of incidents.*

**Response:** NPPD non-concurs with this recommendation to the extent it relates to EINSTEIN 2. US-CERT bases the implementation of signatures in EINSTEIN 2 on current threats to the Federal Government. As a result of the events triggered by the signatures, US-CERT is working to provide Federal agencies with serialized, near real-time analysis reports derived from EINSTEIN 2 data.

Although some departments and agencies with EINSTEIN 1 Netflow sensors installed have access to Netflow data today, that access is not real time or near real time, and no such access was ever contemplated by the program. Moreover, for a variety of reasons, including volume of data, need for validation via analysis/processing, and classification issues, neither the current EINSTEIN 2 deployment nor the planned EINSTEIN 3 solution contemplate sharing unprocessed raw intrusion detection system and intrusion prevention system (IDS/IPS) data with departments and agencies in near real time.

**Appendix C**  
**Major OIG Contributors to this Report**

---

**Information Security Audit Division**

Edward Coleman, Director

Chiu-Tong Tsang, Director

Tarsha Cary, Audit Manager

Pamela Chambliss-Williams, Senior IT Auditor

Shannon Frenyea, Senior Program Analyst

David Bunning, IT Specialist

Swati Nijhawan, Referencer



## Appendix D Report Distribution

---

### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
Executive Secretary  
Assistant Secretary, Legislative Affairs  
Assistant Secretary, Policy  
Assistant Secretary, Public Affairs  
General Counsel  
Office of Security  
Office of Privacy  
Assistant Secretary, Cyber Security and Communications  
Chief Information Officer (CIO)  
Deputy CIO  
Chief Information Security Officer  
Director, NCSD  
Director, US-CERT  
Information Systems Security Manager, NPPD  
Director, Departmental GAO/OIG Liaison Office  
Director, Compliance and Oversight Program  
Audit Liaison, NPPD  
Audit Liaison, DHS/CISO  
Audit Liaison, DHS/CIO  
Director, Information Security Audit Division (ISAD)  
Audit Manager, ISAD

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

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

### **Congress**

Appropriate Congressional Oversight and Appropriations  
Committees



#### 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.