STATEMENT OF RICHARD L. SKINNER

INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

JUNE 16, 2010

Chairman Thompson, Ranking Member King, and Members of the Committee:

Thank you for inviting me here today to discuss the Department of Homeland Security's US Computer Emergency Readiness Team, or US-CERT.

My testimony today will address US-CERT's progress made thus far, and remaining challenges for its analysis and warning program. The information provided in this testimony is contained in our June 2010 report, "*U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain"* (OIG-10-94).

BACKGROUND

The Department of Homeland Security (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 (NCSD) 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.

Further, NCSD developed the national Cybersecurity protection System, operationally known as 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 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 regarding threats and vulnerabilities.

Actions 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. 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. 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.

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 operations. Training relates to packet capture analysis and signature development; malware; and web browser security.

- 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.

Improvements Needed to Strengthen the Cybersecurity Program

Notwithstanding its many accomplishments over the past several years, US-CERT is still 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 and approved its 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 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.

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. 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. However, without the enforcement authority to implement recommendations, US-CERT continues to be hindered in coordinating the protection of federal cyberspace.

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 (.gov) 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.

Strategic Plan and Performance Measures are 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 and performance measures, US-CERT may have difficulty in achieving its

goal to provide response support and defense against potential cyber attacks for the federal government.

According to program officials, US-CERT is developing a strategic plan and revising the performance measures to align with the strategic plan. The 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, strategic plan and performance measures will aid US-CERT in evaluating its progress in building an effective organization capable of mitigating long-term cyber threats and vulnerabilities and improve program operations by promoting the appropriate application of information resources.

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 appropriately 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.

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

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.

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. 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.

- 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. This system also deploys an intrusion prevention feature.

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.

As of October 2009, NCSD'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 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. 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.

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.

Conclusion and Recommendations

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, Office of Cybersecurity and Communications established a unified operations center, which 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.

While progress has been made, US-CERT still faces numerous challenges in effectively reducing the 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.

We recommended in our report that the Under Secretary of National Protection and Programs Directorate (NPPD) require the Director of NCSD to:

- Establish specific outcome-based performance measures and a strategic plan to ensure that US-CERT can achieve its mission, objectives, and milestones.
- 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.
- 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.
- 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.
- Develop a process to distribute and share Einstein trends, anomalies, and common/reoccurring attacks with other federal agencies.
- Provide training to federal agencies on using available features of Einstein to foster better cooperation in analyzing and mitigating security incidents.
- Establish a capability to share real time Einstein information with federal agencies partners to assist them in the analysis and mitigation of incidents.

Mr. Chairman and members of the Committee, you can be sure that my office is committed to continuing our oversight efforts for this challenging and complex issue in the months and years ahead.

This concludes my prepared statement, and I welcome any questions from you or Members of the Committee.