On Wednesday, June 20, the House Homeland Security Committee (HHSC) convened a subcommittee hearing on cybersecurity at the Department of Homeland Security (DHS). The Honorable James R. Langevin, Chairman of Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, chaired the hearing.

The following witnesses testified:

- Mr. Scott Charbo, Chief Information Officer, Department of Homeland Security
- Mr. Gregory C. Wilshusen, Director of Information Security Issues, U.S. Government Accountability Office (GAO)
- Mr. Keith Rhodes, Chief Technologist, GAO

**AOC Awareness:**

Cyberspace is a relatively newly recognized domain of warfare. It is the dimension through which information travels and is collected, processed, managed, and manipulated. While the concept of cyberspace is evolving, it is based upon the same principles, applications, and objectives as electronic warfare, specifically command and control of the electromagnetic spectrum (EMS). The security of our information systems and computer networks is critical to enabling unfettered access to, maneuvering through, and control of the EMS during military and homeland security operations. Electromagnetic dominance is becoming the primary goal early in any conflict, which means that not only the Department of Defense, but also DHS and every other federal agency must make cybersecurity a priority. It has been AOC’s mission over the years to help ensure dominance of the electromagnetic spectrum, so we are poised to lead in the new cyberspace era as well.

**Background**

Over the past several months, the HHSC has held several hearings on cybersecurity. The Committee has investigated the integrity of federal government networks and the subsequent vulnerabilities to attack and exploitation by adversaries. In April, the Committee discussed a recent series of attacks perpetrated by hackers operating through Chinese Internet servers. These attacks prompted a written exchange between the Committee and DHS out of concern that similar attacks may be occurring within the networks of DHS. The exchanged focused on
the Department’s information security policy, incident response plan, the integrity of firewalls and vulnerabilities of network access points.

**Congressional Statements**

In his opening remarks, **Chairman Langevin** stated that “it has become clear that the infiltration of federal government networks and the possible theft or exploitation of our information is one of the most critical issues confronting our nation.” He went on to say that “it was as shock and a disappointment to learn that the Department of Homeland Security – the agency charged with being the lead in our national cybersecurity – has suffered so many significant security incidents on its networks. DHS reported to the Committee that it experienced 844 “cybersecurity incidents” in fiscal years 2005 and 2006 . . . In spite of the significant vulnerabilities in its systems, the Department doesn’t appear to be in any rush to fix them. According to the September 2006 DHS Inspector General report on DHS information systems, 69 percent of the 3,566 open vulnerabilities that exist on the Department’s networks did not include the resources required for remediating those vulnerabilities. In fact, some agencies aren’t even reporting incidents to DHS Computer Security Incident Response Center (CSIRC), as required by law.

“The fact is, DHS is failing to dedicate adequate funding to network security . . . the failure to invest in defensive measures and mitigate vulnerabilities is jeopardizing the Department’s mission.”

HHSC Chairman Bennie Thompson, questioned DHS saying “how can the Department of Homeland Security be a real advocate for sound cybersecurity practices without following some of its own advice? How can we expect improvements in private infrastructure cyberdefense when DHS bureaucrats aren’t fixing their own configurations? How can we ask others to invest in upgraded security technologies when the Chief Information Officer grows the Department’s IT security budget at a snail’s pace? How can we ask the private sector to [improve cybersecurity] when DHS allows employees to send classified emails over unclassified networks and contractors to attach unapproved laptops to the network?”

**Summary of Testimonies:**

**Mr. Scott Charbo** –

“You have no doubt heard reports of recent information security incidents at various federal agencies, including the Department of Homeland Security. Certainly, we need to increase our vigilance to ensure that such incidents do not happen again, and, in fact, the recent loss of an external hard drive at the Transportation Security Administration has prompted a comprehensive review of how the Department processes and stores privacy information. My office continues to work closely with the Department’s Privacy Office and the Chief Human Capital Office to improve the effectiveness of our controls for privacy information.”

Mr. Charbo outlined three initiatives to enhance the Department’s cybersecurity: (1) collapsing multiple legacy wide-area networks (WANs) into a single enterprise WAN, called OneNet; (2) standardizing all email and directory services into a single framework that is more secure than
the legacy environments; and (3) collapsing multiple datacenters into a common shared environment.

In FY 2007, DHS will spend approximately $4.9 billion for information technology, and $332 million of that is dedicated to IT security. For FY 2008, the Department has requested $5.2 billion and $342 million, respectively. That means that the DHS spends only about 6.8 percent of its IT budget on cybersecurity – well below the average for the private sector, as pointed out by the Committee.

Mr. Charbo concluded by highlighting that DHS is in the third phase of its five-year strategic plan. The first two phases included establishing a baseline for basic information security policy and architecture and completing an accreditation of the Department’s IT systems. The current and future phases focus on “raising the bar” to improve documentation of controls and processes, thereby “enhancing the operational security of every system.”

Mr. Gregory Wilshusen and Mr. Keith Rhodes –

The following is an excerpt of a GAO study executed in preparation for this hearing and included in GAO prepared testimony:

“Shortcomings in DHS information security program remain although progress has been made. In 2005, GAO reported that DHS had not fully implemented a comprehensive, department-wide information security program to protect the information and information systems that support its operations and assets. For example, the department did not have a complete inventory of its systems and component agencies did not fully or effectively perform key program activities such as developing risk assessments, preparing security plans, testing and evaluating the effectiveness of security controls, completing remedial action plans, and developing and testing continuity of operations plans. GAO recommended that DHS take specific actions to address these problems. Since then, DHS has taken steps to improve its security program. It prepared a complete inventory of its major applications and systems for the first time in fiscal year 2006. DHS has also implemented key program activities such as contingency plan testing, security control testing, and system certification and accreditation, on an increasing percentage of its systems. However, the quality or effectiveness of these activities was not assured and deficiencies continue to exist.

These program deficiencies contribute to significant weaknesses in computer security controls that threaten the confidentiality, integrity, and availability of key DHS information and information systems. For example, DHS’ independent auditors reported that security over its financial systems was a material weakness in internal control for fiscal year 2006. In addition, GAO determined that CBP did not implement controls to effectively prevent, limit, and detect access to certain computer networks, systems, and information since it did not (1) adequately identify and authenticate users; (2) sufficiently limit access to information and information systems; (3) ensure that controls adequately protected external and internal boundaries; (4) effectively implement physical security at several locations; (5) consistently encrypt sensitive data traversing the communication network; and (6) provide adequate logging or user accountability for the mainframe, workstations, or servers. CBP also did not always ensure that responsibilities for system development and system production were sufficiently segregated. As a result, increased risk exists that unauthorized individuals, internal and external to the
organization, could read, copy, delete, add, and modify sensitive and personally identifiable information and disrupt service on DHS systems.

Until DHS and its components act to fully and effectively implement its security program and mitigate known weaknesses, they will have limited assurance that sensitive information and computer systems will be sufficiently safeguarded or that departmental missions and goals will be achieved. Implementation of GAO’s recommendations will assist DHS in mitigating the deficiencies described above.”