



One Hundred Tenth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515

September 21, 2007

Richard L. Skinner  
Inspector General  
Department of Homeland Security  
Washington, D.C. 20528

Dear Inspector General Skinner:

Over the previous five months, the House Committee on Homeland Security has investigated the information technology security posture at the Department of Homeland Security. The results of our investigation suggest that the Department is the victim not only of cyber attacks initiated by foreign entities, but of incompetent and possibly illegal activity by the contractor charged with maintaining security on its networks. We ask you to immediately commence an inquiry into these matters, and, if necessary, refer this matter for criminal investigation.

The infiltration of Federal Government networks by unauthorized users is one of the most critical issues confronting our nation, but it is hardly a new threat. For years, these attacks have resulted in the loss of massive amounts of critical information. Though many of these attacks are classified, a 2005 report in Time magazine famously publicized a series of coordinated attacks against Department of Defense systems.<sup>1</sup> Those attacks – code-named “Titan Rain” – are believed to be Chinese in origin, although their precise nature (i.e. state-sponsored espionage) is uncertain. Unfortunately, this is not an isolated incident. In 2006, networks at the Departments of Commerce and State were penetrated by foreign-based hackers, most likely Chinese. More recently, the Financial Times reported that the Chinese military hacked into a Pentagon computer network in June 2007.<sup>2</sup> Cyber espionage is an issue of national security, and we must improve our defensive posture to prevent the theft of data or the compromise of the integrity of our data.

On April 19, 2007, the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology held a hearing to discuss hacking activity against Federal agencies. The testimony was disturbing. An official from the Department of Commerce discussed a cyber attack against their systems, which was widely reported to have been launched by hackers operating through Chinese Internet servers. The official testified that hackers penetrated Commerce computers with a “rootkit” program, a form of software that allows the attackers to mask their presence and then gain privileged access to the system. Although IT specialists discovered the incident in October 2006, they could not determine the date of the initial hack or the amount of information that was exfiltrated out of Commerce systems. The attackers, it seemed, left little evidence behind them.

---

<sup>1</sup> “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),” *Time*, August 29, 2005.

<sup>2</sup> “Chinese military hacked into Pentagon,” *Financial Times*, September 3, 2007.

Troubled that similar incidents could occur elsewhere, the Committee initiated an investigation into the security posture of the Department of Homeland Security's information networks. On April 30, 2007, the Committee began requesting information from the Department's Chief Information Officer, Scott Charbo, to obtain a perspective on the adequacy of the Department's efforts. This correspondence is attached as an addendum.

Our investigation yielded interesting results. In a May 21, 2007, response, the Committee learned that the Department experienced 844 "cybersecurity incidents" on its networks during FY 2005 and FY 2006.<sup>3</sup> While the frequency and type of incidents is both high and unacceptable, we were primarily concerned about the similarities in the style of attacks against the Department of Homeland Security and the Department of Commerce. Like the Commerce attacks from October 2006, the Committee noticed patterns of infected Homeland Security machines containing password dumping utilities and other Trojan horse activity with suspicious beaconing activity. Beaconing activity over port 80 suggests the placement of malicious code inside a computer that is attempting to communicate with an outside entity. In a private conversation and again at a June 20, 2007, hearing, Subcommittee Chairman Langevin asked Mr. Charbo if he was concerned about the style of these attacks. Specifically, Chairman Langevin inquired about the suspicious beaconing activity and the malicious code, whether Mr. Charbo and his security team had requested or received intelligence briefings about Chinese hackers penetrating Federal networks, and if Department computers ever exfiltrated information to Chinese servers. Mr. Charbo's answers – "you don't know what you don't know" – suggested that neither he nor the rest of the Department was taking this issue seriously, so the Committee continued the investigation.<sup>4</sup>

On September 4, 2007, the Committee received additional materials from the Department regarding several specific incidents that occurred on networks at the headquarters complex. The incident reports provided by the Department describe the placement of a hacking tool, a password dumping utility, and other malicious code on over a dozen computers, and give the Committee a clearer understanding of the scope of the incidents.

The Committee's investigation finds the following:

- Dozens of Department of Homeland Security computers were compromised by hackers. These incidents were not noticed until months after the initial attacks. These computers may still be compromised due to insufficient mitigation efforts by the contractor responsible for information technology services at the Department.
- Hackers exfiltrated information out of Department of Homeland Security systems to a web hosting service that connects to Chinese websites.

---

<sup>3</sup> Under the Federal Information Security Management Act (FISMA), each Federal agency is required to report "cybersecurity incidents" to the Federal clearinghouse, located at the US-CERT. Department of Homeland Security components (Customs and Border Protection, Transportation Security Administration, etc.) each report their incidents to the Department's "Security Operations Center" (DHS SOC).

<sup>4</sup> U.S. Congress, House, Committee on Homeland Security, *Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security*, 110th Cong., 1<sup>st</sup> sess., 20 June 2007 (testimony by Chief Information Officer Scott Charbo).

September 21, 2007

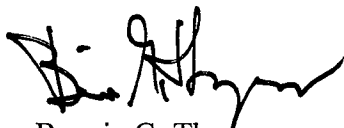
Page 3

- Information was exfiltrated from the Office of Procurement Operations (OPO) and transferred to unauthorized individuals, despite the Department of Homeland Security's assertions to the contrary.
- Although the Department of Homeland Security contracted for network intrusion detection systems as part of the Information Technology Managed Services (ITMS) contract, these systems were not fully deployed at the time of the initial incidents. If network security engineers were running these systems, the initial intrusions may have been detected and prevented.
- Contractors provided inaccurate and misleading information to Department of Homeland Security officials about the source of these attacks and attempted to hide security gaps in their capabilities.
- When presented with the reality that hackers were within their systems, Department officials preferred to complete the fiscal year's financial transactions rather than immediately take steps to mitigate the problem. This decision could have further compromised critical financial information at the Department.

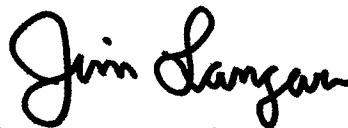
We request that you initiate an investigation into these incidents and the actions of the contractor. As you know, 18 U.S.C. 1001 makes it a crime to knowingly and willfully make a materially false, fictitious or fraudulent statement or representation to the United States government. If your investigation determines that violations of Federal law may have occurred, we expect that you will provide this information to the appropriate officials at the U.S. Department of Justice. We also request a review of the actions of government officials responsible for overseeing this contract to determine whether any breaches of duty occurred. Finally, we are disappointed by the Department's misleading responses to the Committee's requests for information, and request that you determine whether the intent of these misstatements was to obstruct the Committee's investigation.

The Committee will continue to investigate security breaches, particularly those occurring among commercial contractors. We look forward to working with you in these efforts. If you have any questions, please contact Jacob Olcott, Subcommittee Director and Counsel, Committee on Homeland Security at (202) 226-2616.

Sincerely,



Bennie G. Thompson  
Chairman



James R. Langevin  
Chairman  
Subcommittee on Emerging Threats,  
Cybersecurity, Science and Technology

Enclosure

cc: Paul Clement, Acting Attorney General, U.S. Department of Justice  
Michael Chertoff, Secretary, Department of Homeland Security  
Scott Charbo, Chief Information Officer, Department of Homeland Security  
Robert West, Chief Information Security Officer, Department of Homeland Security