BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

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

February 1, 2008

The Honorable Michael Chertoff
Secretary
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Chertoff:

Last year, the House Committee on Homeland Security investigated the information technology security posture at the Department of Homeland Security. The results of our investigation suggested that the Department was 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. Along with Chairman James Langevin, I asked Inspector General Richard Skinner and the Department's Office of Security to immediately begin an investigation into these incidents to determine the severity and seriousness of the breaches. These investigations remain ongoing.

During the course of the investigation, the Committee asked the Department's Chief Information Officer, Scott Charbo, to testify at a hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. The testimony that the Committee received was deeply troubling. Although the Chief Information Officer is ultimately responsible for the security of the Department's numerous information networks, Mr. Charbo seemed unaware and unconcerned about any serious malicious activity on the networks he was charged with securing. For example, when asked if he or his security team had requested or received intelligence briefings about Chinese hackers penetrating federal networks, or if Department computers ever exfiltrated information to Chinese servers, Mr. Charbo responded "you don't know what you don't know." This answer was typical of the laissez faire attitude that he exhibited throughout the investigation, and suggested that neither he nor the rest of the Department was taking the issue of cybersecurity seriously.

The Committee's investigation found the following:

- Dozens of Department of Homeland Security computers were compromised by hackers under Mr. Charbo's leadership. These incidents were unnoticed for months after the initial attacks. It is likely that they are still compromised due to insufficient mitigation efforts by the Department and the contractor responsible for information technology services.

- Hackers exfiltrated information out of Department of Homeland Security systems to a web hosting service that connects to Chinese websites.

- 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.

Ultimately, the evidence uncovered by our investigation suggests that while Mr. Charbo may have created information technology services and capabilities throughout the Department, he did so at the expense of security. In this day and age – where the cyber threat both from home and abroad is real and dangerous – this is an incredible and unacceptable dereliction of duty.

In recent months, this Administration announced plans for the largest cybersecurity initiative in the history of the federal government, with the Department of Homeland Security playing a leading role in securing federal networks. Your decision to promote Mr. Charbo to Deputy Under Secretary of National Programs and Plans effectively places him in charge of the cyber initiative at the Department. Given his previous failings as Chief Information Officer, I find it unfathomable that you would invest him with this authority. This decision raises concerns about the seriousness and credibility of the Administration's initiative.

Please contact me at your earliest convenience to discuss this matter.

Sincerely,

Bennie G. Thompson
Chairman

BGT/jso