



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

July 27, 2007

Scott Charbo  
Chief Information Officer  
Department of Homeland Security  
Washington, D.C. 20528

Robert West  
Chief Information Security Officer  
Department of Homeland Security  
Washington, D.C. 20528

Dear Mr. Charbo and Mr. West:

The House Committee on Homeland Security is currently conducting a review of federal information system security. On July 18, 2007, the Department of Homeland Security's Inspector General released a troubling report about information technology management at the Department. The "Information Technology Management Letter for the DHS FY 2006 Financial Statement Audit" contains observations and recommendations related to information technology internal controls on the Department's financial management systems. Unfortunately, the audit indicates that significant vulnerabilities remain prevalent on Department systems.

While some Department components demonstrated improvement over the previous year, auditors found that most did not measurably enhance their security posture. During the 2006 IT testing, auditors identified over 200 vulnerable conditions on financial management networks that were in need of mitigation. Though the Department closed 44 percent of those risks, more than 150 new findings were discovered this year. The vulnerabilities identified by the audit include: 1) excessive access to key Department financial applications; 2) misconfigured logical security controls to key Department financial applications and support systems; and 3) application change control processes that are inappropriate, and in other locations not fully defined, followed, or effective. Unfortunately, failing to mitigate these conditions jeopardizes the integrity of the Department's financial systems.

This recent report on financial systems follows several studies issued by the Inspector General in 2006 that examined information security at Department components. For instance, in June 2006, the Department of Homeland Security Inspector General released a report assessing the strengths and weaknesses of the

Science and Technology Directorate's (S&T) laptop computer security controls. The report found that "significant work remains for S&T to further strengthen the configuration, patch, and inventory management controls necessary to secure its data stored on government-issued laptop computers." Weaknesses at components like S&T can have significant consequences to data integrity throughout the Department.

The Committee is deeply concerned that the vulnerable conditions highlighted in recent reports by the Inspector General may facilitate espionage on the Department's computers. We ask that you please provide answers to the following questions:

1. Has there ever been an incident characterized as an "Unauthorized Access" (US-CERT Incident Category 1) or "Malicious Code" (US-CERT Incident Category 3) that took place on a network, a computer, or a computer user account associated with or attributed to the Office of Procurement Operations or the S&T Directorate? Please provide all Incident Assessment Forms and associated reports for each of these incidents.
2. Has a hacking tool or password dump utility ever been loaded on a network, a computer, or a computer user account in the Office of Procurement Operations or the S&T Directorate? If so, what level or position was the user associated with the machine? If not, have any computers in the Office of Procurement Operations or S&T Directorate been connected to a computer containing known malicious logic or hacker tools?
3. Has an infected machine associated with the Office of Procurement Operations or the Science and Technology Directorate ever exfiltrated (transmitted out) information? If so, did the Department perform independent verification and validation assessments to identify a nation state hacker presence? What was the result of these assessments?
4. In previous communications with the Committee, your office provided a list of cybersecurity incidents reported to the Department's Security Operations Center (SOC) from FY 2005-2007. During the June 20, 2007 Emerging Threats, Cybersecurity, and Science and Technology Subcommittee hearing, members discussed several of these incidents that occurred during 2006. Please provide the Committee with all documents, communications, or correspondence regarding the following incidents, including electronic correspondence between and among contractor groups associated with these incidents:
  - DHS Incident #2006-09-030
  - DHS Incident #2006-09-013
  - DHS Incident #2006-09-041
  - DHS Incident #2006-08-031

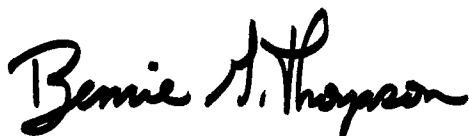
July 27, 2007

Page 3

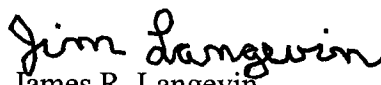
- DHS Incident #2006-08-011
- DHS Incident #2006-06-047
- DHS Incident #2006-06-031

Pursuant to Rule X (3)(g) and Rule XI of the Rules of the House of Representatives, we request a response in writing by not later than August 27, 2007. If you have any questions, please contact Cherri L. Branson, Chief Oversight Counsel, Committee on Homeland Security, at (202) 226-2616.

Sincerely,



Bennie G. Thompson  
Chairman



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

BGT/jso