



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

April 30, 2007

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

Dear Mr. Charbo:

The House Committee on Homeland Security is currently conducting a review of federal information system security. The Subcommittee on Emerging Threats, Cybersecurity, Science and Technology held a hearing on April 19, 2007 at which time it was revealed that networks at the Departments of Commerce and State were hacked in 2006. These incidents jeopardize the integrity of our government's information. We are concerned that similar incidents may be occurring within the networks of the Department of Homeland Security. Please provide answers to the following questions:

1. What responsibility does the Chief Information Officer have over the networks of the Department of Homeland Security? Please explain your relationship to the Chief Information Security Officer, as well as the Chief Information Officers and Chief Information Security Officers of the Department's component agencies.
2. Please provide the Department's information security policy and incident response plan.
3. Please provide a report on how many and what types of incidents have been reported to US-CERT by agencies within the Department of Homeland Security. Please categorize each incident using the "Federal Agency Incident and Event Categories" developed by the US-CERT. Please provide details of the attack or attacks during 2004-2007 that were the most critical (classified "CAT 1" on the US-CERT reporting guidelines). Please include both those that were and were not reported to US-CERT, and indicate which were not reported to US-CERT within the US-CERT reporting timeframe.
4. Has the Department taken an inventory of each access point to its network (e.g., every connected device, wireless device, remote device, etc.), both inside and outside of the firewall, in order to identify potential points of vulnerability? Does a complete network topology diagram exist? If so, please provide that diagram.
5. Has the Department ever conducted both internal and external penetration tests on its systems? Have individual components of the Department ever performed internal and external penetration tests on their systems? Please provide copies of all penetration testing reports and narratives describing the vulnerabilities that were revealed and how those vulnerabilities were mitigated.

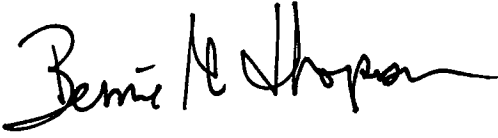
6. When was the last time the Department used ingress and egress filtering on client personal computers? When was the last time the Department replicated client-side attacks on those computers? Has the Department ever conducted a network-wide rogue tunnel audit of all client personal computers? Have you ever conducted audits on the aforementioned compromised personal computers from question 3?
7. Has the Department implemented a secure coding initiative? What portion of software deployed by the Department and its components have been tested using source code analysis tools? What portion of web applications have been tested using web application security tools? How many of the programmers working on Department applications, whether Department or contractor employees, have been trained in secure coding techniques and what skills testing was undertaken to ensure they had mastered secure coding techniques?
8. Has the Department mandated two-factor authentication for all privileged personnel and system administrators? If not, why not?
9. What legal requirements are the Department's hosting companies, data warehouses, software developers, or application service providers contractually obligated to fulfill regarding security? Please provide a narrative of the duties, layers of security, notification of security breaches, and timeliness of responses that the Department requires of these contractors. Is the Department able to audit/penetration test these entities to ensure that that standard of security has been met? Has the Department ever done so?
10. Please provide the annual budgets for the Chief Information Security Officer beginning in fiscal year 2003.
11. How much money, in total, has the Department spent on meeting the requirements of the Federal Information Security Management Act (FISMA)? What percentage of the overall budget does that figure represent? Specifically, how did those reports lead to improved defenses against attacks? What specific changes were made? Are you confident those changes improved your defenses?
12. When the Department purchases software, do procurement documents require that the purchased software operates effectively on the secure configurations? If not, what does the Department do when a purchased package requires security configurations to be weakened in order to run the purchased application?
13. What are your top three initiatives for securing the Department for 2008? How do you measure those goals?

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 May 21, 2007. If you have any questions, please contact, Cheri L. Branson, Chief Oversight Counsel, Committee on Homeland Security at (202) 226-2616.

April 30, 2007

Page 3

Sincerely,



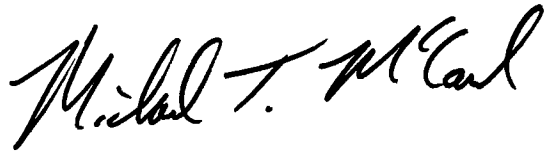
Bennie G. Thompson
Chairman



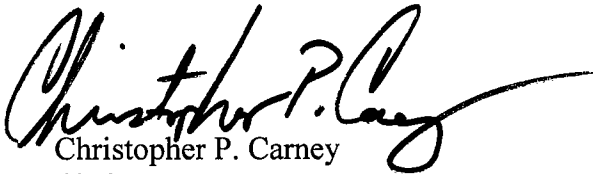
Peter T. King
Ranking Member



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



Michael T. McCaul
Ranking Member
Subcommittee on Emerging Threats,
Cybersecurity, Science and
Technology



Christopher P. Carney
Chairman
Subcommittee on Management,
Investigations, and Oversight



Mike Rogers
Ranking Member
Subcommittee on Management,
Investigations, and Oversight

BGT/jso