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

May 31, 2007

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

Dear Mr. Charbo:

Thank you for your timely response to the April 30, 2007 letter from this Committee. I have several follow-up questions based on the materials you provided:

1. The network topology diagram provided to the Committee is incomplete. Please provide the full network topology diagram.

2. Has the Department identified any security concerns as it moves forward with the "OneNET" proposal, and, if so, what plans are in place to remedy any vulnerabilities prior to the convergence of the networks?

3. Please provide a list of all mitigation actions tracked within the Department's Trusted Agent FISMA (TAF) tool, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.

4. Please provide a list of all vulnerabilities that are recorded and tracked within the TAF Plan of Action and Milestone (POA&M) folder, including the name of the component, date of assignment, scheduled completion date, mitigation action, and completion date.

5. During a meeting with Committee staff, you stated that you are authorized to reduce funding to agency components that do not mitigate their POA&M vulnerabilities in a timely fashion. Please provide a list of funding reductions or recommendations for funding reductions that you made to Secretary Chertoff. Please also provide a narrative of Secretary Chertoff's response to your recommendations.

6. If you have not provided funding cut recommendations to the Secretary, please provide a list of any agency components that have not mitigated their POA&M vulnerabilities and a narrative explaining your decision not to recommend a funding reduction.

7. According to the Department's policy on Contractors and Outsourced Operations, "components shall conduct reviews to ensure that the IT security requirements in the contract are implemented and enforced."[1] When was the last Department-wide review of these contracts? Were these reviews conducted by component CIOs or by personnel within your line of authority? What vulnerabilities were identified in the review and when were they remedied? Please provide the Committee with each component review of their outsourced operations, as well as the Departmental review of the components' work.

8. According to the Department's policy on Risk Management, "components shall conduct risk assessments whenever significant changes to the system configuration or to the operational/threat environment have been made, or every three years, whichever comes first."[2] Please provide these risk assessments, including the dates the assessments were conducted.

9. According to the Department's policy on IT Security Review and Assistance, "the DHS CISO shall conduct IT security review and assistance visits throughout the Department to determine the extent to which the Component security programs comply with IT security policy, standards, and procedures."[3] When were these security reviews completed? How many components passed or failed this review?

10. The Department's policy on "Wireless Systems" requires "annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions."[4] Please provide the Committee with those assessments.

11. When did the Department last audit the MCI MPLS Cloud or the Sprint MPLS Cloud? What were the results of the audit? Did the Department require MCI or Sprint to mitigate vulnerabilities?

12. The Committee requested and received a list of the FY 2005 and FY 2006 incidents reported to the Department's Security Operations Center (DHS SOC).

    a. Please define a "classified data spill." How is this incident different from an incident where a Department employee sends a classified email through a non-classified system?

    b. Please explain what disciplinary actions were taken against the contractors in DHS Incident # 2006-08-031.

    c. Please provide a list of the FY 2007 incidents reported to the DHS SOC.

---

[1] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 19.
[2] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 22.
[3] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 22.
[4] Department of Homeland Security Sensitive Systems Policy Directive 4300A, p. 37.

Pursuant to Rule X (3) (g) and Rule XI of the Rules of the House of Representatives, I request a response in writing by not later than June 15, 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

BGT/jso