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

April 6, 2007

The Honorable Condoleezza Rice
Secretary
U.S. Department of State
2201 C Street NW
Washington, DC 20520

Dear Secretary Rice:

The House Committee on Homeland Security is currently conducting a review of federal information system security. On April 19, 2007, the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology will hold a hearing that will examine a cyber attack targeting the computers of the State Department in July 2006. I request that you provide the Committee with the following information:

1. Was the Department aware of the break-in to its computers immediately upon its occurrence? If the Department did not immediately know, when did it become aware?

2. Does the Department know how long the perpetrators of the break-in were inside its computers before their presence was discovered?

3. What other systems were compromised during the time the perpetrators had control of Department computers? (Did the Department, for instance, conduct both internal and external penetration tests to detect all other vulnerable clients?) Please provide the Committee with all documents and communications related to those penetration reports.

4. Did the Department completely eliminate any infestations that could have occurred while the perpetrators had control of its systems? (Did the Department, for example, completely wipe the disks of all agency systems and reload from back-ups from before the time the systems were compromised?) Please provide all documents and communications related to the Department's efforts to wipe disks and reload back-ups.

BGT/jso

5. There is evidence from infestations of military systems that attackers nearly always leave back doors through which they can return any time to change data or steal new information or take over other systems. How certain is the Department that all back doors have been eliminated? (Did the Department, for example, conduct rogue tunnel audits? Were backup systems examined for the presence of rogue tunnels?)

6. When was the last time the Department tested all personal computers for a comparison of egress and ingress?

7. The Federal Information Security Management Act (FISMA) requires federal computers to be certified and accredited. How many of the systems that were compromised were certified and accredited?

    a. How much money, in total, has the Department spent on performing certification and accreditation studies and reports to comply with FISMA? Specifically, how did those reports lead to improved defenses against attacks? What specific changes were made to systems based on those reports? Is the Department confident those changes improved its defenses?

    b. Overall, how much does meeting the FISMA requirements cost the Department?

    c. FISMA calls for each federal agency to use secure configurations. At the time of the incident, what model secure configurations did the Department use for its Windows systems? Since the incident, has the Department issued a policy requiring that secure configurations be used? When did the Department last test all Windows systems to ensure they have actually implemented the secure configurations? Please provide a copy of the report summarizing those configuration tests.

    d. When purchasing software, do the procurement requirements of the Department demand 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?

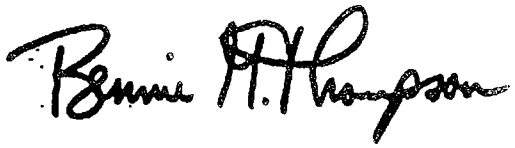
    e. When was the last time the Department ran web security testing tools against its Internet-facing applications? Please provide the report summarizing the results of that study.

8. Please provide all documents and communications between your agency and the Department of Homeland Security during and after the incident. Please include a narrative explaining the stage at which you contacted the Department of

Homeland Security and the Department of Homeland Security's response to the incident.

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 April 16, 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

cc: Peter T. King, Ranking Member, Committee on Homeland Security
James Langevin, Chairman, Subcommittee on Emerging Threats, Cybersecurity, Science and Technology
Michael McCaul, Ranking Member, Subcommittee on Emerging Threats, Cybersecurity, Science and Technology

BGT/jso