United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

May 1, 2008

The Honorable Michael Chertoff
Secretary
U.S. Department of Homeland Security
Washington DC 20528

Dear Secretary Chertoff:

On March 4th, Robert Jamison, Under Secretary of National Protection and Programs, and other government officials, testified before the Senate Homeland Security and Governmental Affairs Committee in a closed hearing on the role of the Department of Homeland Security (DHS or "the Department") in the Comprehensive National Cybersecurity Initiative (CNCI). This initiative will fundamentally change, and we hope strengthen, the government's efforts to secure the critical cyber networks on which our government, indeed our way of life, depend.

When the Department was established five years ago, we were optimistic that it would play a key role in securing cyber networks. Given the extent of the threat, it is clear that there must be a greater emphasis on securing our information technology systems. The CNCI is evidence that the Department, and the Administration, is rethinking its approach to cybersecurity, and we welcome this initiative.

Overall, we are pleased that the Department is taking additional steps to secure federal computer networks and that you have decided to make cybersecurity one of the Department's top four priorities for this year. Nonetheless, we are writing to ask some additional questions on the Department's role in the CNCI and its goals for cybersecurity overall. To aid our examination of this program, we also request certain documents relating to the CNCI.

The CNCI – officially established in January when President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks. DHS has been tasked to lead or play a major role in many of these tasks. This bold, much-needed approach to cyber security will lead to a fundamental shift in the way the Department approaches the security of U.S. networks.

DHS has requested substantial new resources for cyber security, and it is critical that the funds are spent carefully and appropriately. The Department has requested an additional $83 million dollars for the National Cyber Security Division (NCSD) for fiscal year 2009. Including the $115 million that was awarded for the initiative in the FY 2008

omnibus appropriations bill, this would be a nearly $200 million dollar increase, tripling the amount of money spent on cyber security in DHS since 2007.

The Department's plan to use contractor personnel to support the initiative merits some scrutiny in light of this Committee's past work in this area. On January 16, DHS issued an RFP for "Mission Support for NCSD" seeking services to support the Directorate for 10 months, presumably to assist with the additional responsibility given to DHS under the CNCI. However, the request does not appear to incorporate the recommendations made to the Department by the Government Accountability Office (GAO) in a report we requested last year ("Department of Homeland Security: Improved Assessment and Oversight Needed to Manage Risk of Contracting for Selected Services," GAO-07-990). One of these recommendations, which the Department agreed with, was that contract requirements should be defined to "clearly describe roles, responsibilities, and limitations of selected contractor services as part of the acquisition planning process." We have several questions to better understand the Department's intentions with respect to staffing and for the procurement of service to support the NCSD.

We also have concerns about how information has been shared with Congress and other stakeholders concerning this initiative and the potential impact this lack of collaboration may have on the success of the initiative. While certain operational details of the program are necessarily classified, additional efforts, where appropriate, to downgrade the classification or declassify information regarding the initiative would aid congressional oversight and permit broader collaboration with the private sector and outside experts. Given the scope of this initiative and the broad cross section of stakeholders – both in the government, the private sector, and elsewhere – this oversight and collaboration are critical components of a successful program.

We are also concerned that the lack of information about the CNCI being provided to the public, other agencies, and private entities that conduct business with the government might be creating confusion and concern about the initiative. Given the broad nature and goals of this initiative, agencies may be less likely to plan for their future information technology needs, fearing that systems they purchase might not comply with the initiative. Similarly, industry will be less likely to do business with the government given the uncertainty about future technical requirements. Additionally, the public, of course, must be reassured that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties.

At the same time, there appears to be some confusion within the Executive Branch concerning what information about the CNCI is and is not classified. In some cases, DHS officials have publicly revealed information that had previously been presented to Committee staff as classified. For example, on March 20th, you announced that Rod Beckstrom would be the Director of the new National Cyber Security Center (NCSC) within DHS. Prior to this announcement, committee staff had been instructed that the existence of the NCSC itself was classified. Moreover, the Department has yet to publicly disclose very many details on the role of the NCSC beyond the brief press

release. To clarify these matters, we renew our request for an unclassified summary of the CNCI – a request made by Committee staff over five months ago.

Given the confusion over what the NCSC will do and a lack of clarity over what information pertaining to the NCSC is classified, we also request additional information to better understand the role of the NCSC within the Department. Additionally, we have questions about the nature and duration of the position of Director of the National Cyber Security Center.

We are also concerned about of the relative lack of private industry involvement in this initiative to date. The private sector controls the vast majority of our nation's cyber infrastructure and is an important partner in our efforts to protect government systems. While the CNCI takes immediate steps to secure government systems, identifying the actions necessary to secure private networks must be a long term goal. We are pleased that "Project 12," a component of the CNCI, will assemble a group of industry leaders to help the Department issue a report on how the government should work to protect the larger cyber infrastructure. However, beyond "Project 12," we are not aware of any substantial industry involvement with the development or implementation of the CNCI. Given their expertise, and the role that private industry must necessarily play in securing government and private sector networks, we urge you to ensure that they are appropriately involved in this initiative.

We would like to reiterate our support for the Administration's increased focus on cyber security. At the same time, we believe that increased openness and information sharing with the Congress, the private sector, and the American public will aid in the eventual success of the initiative. To that end, we would appreciate your responses to the following questions:

THE NATIONAL CYBER SECURITY CENTER

1. What is the role of the National Cyber Security Center?

2. Why was the determination made to create the National Cyber Security Center?

3. In Acting Deputy Secretary Schneider's answers to pre-hearing questions for his nomination, Mr. Schneider stated that the appointment of Mr. Beckstrom as Director of the National Cyber Security Center "is for two years."

    a. Under what authority was Mr. Beckstrom appointed and is he serving? For example, was he given a Schedule C Excepted Appointment, or was he appointed under some other legal authority?

    b. Please explain what is meant by a "two-year" appointment. What obligations and/or rights do Mr. Beckstrom and the federal government have under this arrangement?

c. Under what legal authority was Mr. Beckstrom's appointment made "for two years"?

d. Please provide to the Committee a copy of any document or other record that effectuates Mr. Beckstrom's appointment or that memorializes any terms or conditions of the appointment.

CONTRACTING

4. For their role with CNCI, the Department intends to increase quickly the number of staff supporting the program. How do you intend to find and recruit people with sufficient qualifications?

5. In the Department's view, what is the right balance between contract and government staff to carry out the responsibilities of the NCSD at DHS?

6. On January 16, DHS issued an RFP (Solicitation HSHQDC-08-R-00025) for Mission Support for the National Cyber Security Division. This RFP lays out 18 pages of responsibilities under the contract, which include supporting numerous activities under NCSD.

   a. Is this RFP designed to extend current services that contractors are providing for NCSD or to expand the services that contractors will provide?

   b. Why was the determination made that this contract would be for a 10-month period?

   c. Does the Department have a plan for transitioning from contractor support to FTE's after the 10-month period?

   d. What contractor has been performing this work to date, and why is it being recompeted at this time?

7. Several of the tasks requested in the statement of work appear integral to DHS's mission and will closely support certain inherently governmental functions. These tasks include: intelligence analysis, coordinating with law enforcement, coordinating between government offices, and responding to congressional requests.

   a. How will DHS provide appropriate oversight to ensure that the contractors support efforts do not intrude on inherently governmental functions?

b. How will DHS ensure enhanced scrutiny of contractor performance as required by federal procurement regulation and guidance?

c. How many Contracting Officer's Technical Representatives (COTRs) does the Department plan to have overseeing this contract?

8. In the response to the recommendations in GAO's report, DHS stated "Better requirements definition for service contracts will lead to fewer Time and Materials type contracts and more effective use of Performance Based Service Contracts throughout DHS." Additionally, in a memo written in August of last year, Chief Procurement Officer Elaine Duke wrote, "requirements for services must be clearly defined with appropriate performance standards and, to the maximum extent practicable structured as performance-based." Despite this statement, this RFP anticipates the award of a Time and Material task order.

a. Why was the determination made to make this a Time and Materials task order?

b. How will DHS ensure that costs are being controlled after this contract is awarded?

CLASSIFICATION

9. Given that this initiative is highly classified, how will you ensure that government officials and members of the private sector have the necessary information to carry out their respective roles in the initiative?

10. Are there plans to issue an unclassified version of HSPD-23, similar to President Clinton's release of an unclassified version of PDD-63?

ROLE OF THE PUBLIC

11. How does this new policy comport with privacy and public comment requirements in existing statute, such as the E-Government Act (P.L. 107-347) and the Privacy Act (P.L. 93-579)?

12. As this initiative is deployed, how will you ensure that American citizens retain the maximum possible electronic access to government agencies' websites?

13. How will you ensure that the privacy of Americans who access government websites and provide personally identifiable information through electronic means will be protected?

METRICS

14. On March 1, OMB reported that for FY07 there were 12,986 security incidents, more than doubling the number of incidents reported in FY06. Much of this increase may be attributable to increased reporting, and consequently we might expect that number to rise as the Einstein program is further deployed.

    a. Given the likelihood that this number will rise, how will we determine when this initiative is succeeding and Einstein is measuring something tangible?

    b. Overall, what metrics will be used to evaluate success?

PRIVATE SECTOR

15. Its our understanding that the private sector was not consulted before the CNCI was drafted and that very few members of the private sector have been briefed on CNCI to date.

    a. To what extent were private sector experts involved in the development of the CNCI?

    b. Is it possible that important cyber security experts who might have valuable expertise were not consulted?

    c. Given that private sector cooperation is crucial to effectively protect federal government networks, how do you plan to work with this sector in the implementation of the CNCI?

    d. Will there be a chance for select portions of industry to provide feedback on the CNCI, other than "Project 12," prior to the finalization of ongoing implementation plans currently being prepared?

    e. Will there be a chance for the public to comment on the non-classified portions of CNCI?

PRIVACY IMPACT ASSESSMENTS

16. The new version of Einstein, instead of only looking at information traffic to and from government networks, could be used to look at the content of this traffic as well. Undersecretary Jamison testified before the House Homeland Security Committee that a privacy impact assessment (PIA) is being conducted as the new version of Einstein is developed. The PIA requirement from the E-government Act of 2002 requires PIAs to be conducted and published before the development

of new information technology systems that will collect or store personal information electronically.

a. When do you expect the Privacy Impact Assessment to be completed for the new version of Einstein?

b. When do you expect the new version of Einstein to be deployed?

c. How will any identified privacy concerns be addressed in the new version of Einstein?

OTHER RESPONSIBILITIES OF DHS

17. While securing federal government networks is clearly an important goal, the NCSD has a number of other priorities in securing cyberspace outside of government systems.

a. How will the Department ensure that its responsibilities under the CNCI do not divert resources from its other cybersecurity missions?

b. What are the goals for the NCSD for this year, beyond the protection of government networks, to ensure that cyber security is enhanced overall, and not just within government networks?

In addition, please provide the following information to the Committee:

- A classification guide that clarifies which portions of the CNCI are classified and at what level;
- A summary document describing all portions of the CNCI deemed unclassified;
- An unclassified, detailed 5-year breakdown of the DHS budget for the CNCI;
- An unclassified summary of the roles and responsibilities of the NCSC, including the level at which the Center will be funded;
- A detailed implementation plan of DHS's responsibilities under the CNCI, including how contract staff will be used to support the NCSD; and
- Any plans pertaining to enhancements of the Einstein Program.

Thank you in advance for your attention to this matter. We look forward to reviewing the information that you provide. Please feel free to have your office contact Adam

Sedgewick or Deborah Parkinson with Senator Lieberman at (202) 224-2627 or John Grant or Asha Mathew with Senator Collins at (202) 224-4751 if you have any questions.

Sincerely,

Joseph I. Lieberman
Chairman

Susan M. Collins
Ranking Member

cc: The Honorable Robert Jamison, Undersecretary, National Protection and Programs Directorate;
Rod Beckstrom, Director, National Cyber Security Center