Office of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 28, 2009

Ms. Marcia Hofmann
Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110-1914

Re: **NPPD09F172**

Dear Ms. Hofmann:

This is the final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated November 19, 2008, and received by this office on November 24, 2008. You are seeking the unredacted "For Official Use Only" version of Secretary Chertoff's July 18, 2008, response to Joseph Lieberman, Chairman of the Senate Committee on Homeland Security and Governmental Affairs, regarding DHS's role in the Comprehensive National Cybersecurity Initiative.

I have determined that 16 pages of the records are releasable in their entirety and one page is partially releasable pursuant to Title 5 U.S.C. § 552 (b)(5), FOIA Exemption 5.

Enclosed are 17 pages with certain information withheld as described below.

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. After carefully reviewing the responsive documents, I determined that portions of the responsive documents qualify for protection under the Government's commercial data privilege that protects various government cost estimates. Release would not only cause harm to the Government's decision-making process, but would also provide a contractor with insight into the Government's price negotiation position. This would place the Government at a disadvantage in its efforts to obtain fair and reasonable prices in the future.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), U.S. Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at www.dhs.gov/foia.

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the $14 minimum, there is no charge. 6 CFR § 5.11(d)(4).

If you need to contact our office again about this matter, please refer to **NPPD09F172**. This office can be reached at NPPD.FOIA@dhs.gov.

Sincerely,

FOIA OFFICE
National Protection and Programs Directorate

Enclosure(s): Responsive Documents, 17 pages

Responses to Chairman Lieberman's and Senator Collins's Questions Regarding the National Cyber Security Center

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

The National Cyber Security Center (NCSC) will coordinate and integrate information necessary to help secure U.S. cyber networks and systems and help foster collaboration among Federal cyber groups. In particular, the NCSC will advance the coordination and consultation among the various Federal cyber entities responsible for various parts of the cyber security missions.

Additionally, the NCSC will serve a principal role as a single location for all-source situational awareness about cyber activity and security status of the U.S. networks and systems. The NCSC will interface with those cyber security focal points to provide a single location—both physical and virtual—for increased collaboration and all-source situational awareness. The Center will also analyze the mission areas, authorities, and core capabilities of Federal cyber groups.

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

Although there are numerous healthy information exchanges among departments and agencies—in particular the cyber security focal points within those departments and agencies—there has been no single entity charged with increasing collaboration or serving as a focal point for all-source situational awareness. The NCSC was created to fill this gap.

The NCSC was loosely modeled after the National Counterterrorism Center (NCTC), in particular to function as a focal point without direct ability to execute authorities and missions that are already assigned elsewhere. There was and is widespread support among the cyber security focal points in departments and agencies for the creation of such an entity. With proper support, the NCSC will become a robust focal point for collaboration and all-source cyber situational awareness, an outcome that will benefit all of the participating cyber security focal points in departments and agencies.

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 Expected Appointment, or was he appointed under some other legal authority?*

    Mr. Beckstrom is serving under a limited-term Senior Executive Service (SES) appointment acquired through the Office of Personnel Management (OPM).

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 agreement?*

All rights that are accorded under a limited-term SES appointment, as set forth in 5 U.S.C. 3394, 3395(b)-(d) and 5 C.F.R. 317.601(c).

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

Mr. Beckstrom's appointment was made under 5 U.S.C. 3394, 3395(b)-(d) and 5 C.F.R. Part 317, subpart F.

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 that appointment.*

Please see attached documents.

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?*

The National Cyber Security Division (NCSD), which is an integral part of the Comprehensive National Cyberspace Initiative (CNCI) though its operational unit, the United States Computer Emergency Readiness Team (US-CERT), recruits new employees through any of the following activities:

- Posting all listings on www.USAJOBS.gov and other targeted publications;
- Executing a comprehensive human resources plan to recruit additional government staff;
- Obtaining direct hire authority from OPM to streamline the hiring process;
- Providing additional onsite human resources support for NCSD;
- Prioritizing clearance procedures for the CNCI direct hires;
- Promoting the National Centers of Academic Excellence in Information Assurance Education;
- Participating in numerous recruiting events and job fairs with the private sector and other events sponsored by the Department of Homeland Security (DHS); and
- Collaborating with the National Science Foundation (NSF) and various academic institutions to recruit students in the Cyber Corps program. There are currently 11 cyber scholars in the recruitment pipeline as a result of this effort.

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?*

NCSD recognizes the need to achieve a balanced mix between government employees and contractors. During fiscal year 2007, NCSD evaluated and developed a comprehensive human resources plan to convert contracted support personnel to additional government staff. The specific aim of this effort was to increase the ratio of government staff to contractors and to ensure that inherently governmental functions are retained by government personnel. The "right" balance has been identified and its implementation is underway. NCSD remains optimistic that a sustainable level of government personnel is within reach in the next 18 to 24 months, which will provide operational stability that is consistent with its missions and associated tasks.

6. *On January 16, 2008, 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 the RFP designed to extend current services that contractors are providing for NCSD or to expand the services that contractors will provide?*

   This solicitation was developed prior to the approval of the CNCI. Furthermore, the work identified by the RFP does not explicitly support CNCI, although some support to certain initiatives related to incident response are within the scope of the contract contemplated by the RFP. The RFP was primarily designed to extend current support services that have been in place since April 2006.

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

   NCSD is undergoing a major change as a result of the CNCI both functionally and organizationally. NCSD is examining the impact of these changes as it relates to the mission requirements of the organization. The ten-month Mission Support for the National Cyber Security Division is a "bridge" task order that will support operations until all requirements are finalized and a long-term contract is competed. The long-term contract vehicle will reflect the emerging and new support requirements resulting from the aforementioned organizational changes. NCSD is currently planning and developing the necessary documentation for the long-term mission support contract.

   Under the existing task order, current services terminate on July 3, 2008. A ten-month task order "bridge" is required to cover support during the competition for the long-term contract which has a projected award date in FY 2009.

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

The Department does have a management plan for transitioning contracted personnel after the ten-month bridge contract is completed. In FY 2009, NCSD has requested 46 additional full time employees above those received through the FY 2008 appropriation. The ten-month bridge will continue current support pending the FY 2009 enacted appropriations. The Department is also examining additional contractor-to-Federal conversions to provide the appropriate level of Federal and contractor support to NCSD.

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

Current support services have been in place since April 2006 and performed by Booz Allen Hamilton. Mission support work is being re-competed at this time because current support services will end on July 3, 2008.

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?*

DHS realizes the limits of contractor support; consequently, the NCSD program provides appropriate oversight to ensure that the contractors under these efforts do not intrude on inherently governmental functions. Specifically, contractor performance is closely monitored by DHS program managers and the DHS contracting officer technical representative (COTR) to ensure that tasks and activities are in compliance with the appropriate statement of work.

The statement of work does cover the following tasks: intelligence analysis, coordinating with law enforcement, coordinating between government offices, and responding to congressional requests. However, the description of these tasks mentioned under this contract refers to contractors supporting the Government program managers in establishing and maintaining programmatic activities within the NCSD/US-CERT.

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

NCSD/US-CERT requires its vendors to provide monthly status reports that are closely reviewed by the COTR, task managers, and program managers. Additionally,

program managers conduct internal reviews and assessments of deliverables and milestones accomplished as part of their program management activities.

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

The Department plans to have one COTR oversee this contract, as is standard for a contract of this size.

8. *In the response to the recommendation 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 base." 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?*

This is a short term ten-month transition contract that requires flexibility. DHS understands that Time and Materials is not considered the optimal contracting method; however, given the current situation, it is deemed appropriate for the services required during this period of transition for NCSD. NCSD is currently planning for a more robust contract vehicle. The statement of work for the ten-month effort imposes progress reporting requirements on the contractor, this will allow NCSD to obtain useful metrics to convert some, if not all the tasks in the follow-on, long-term contract from Time and Materials to Fixed Price. Until the Department determines all necessary requirements, a Time and Materials contract is the best short-term contract vehicle.

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

DHS will closely monitor the vendor's monthly status report and monthly invoices to ensure the performance and cost are aligned, and that costs are fair and reasonable.

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?*

The Federal Government has a number of mechanisms to distribute information to Federal officials with a need to know, including:

- Partnership for Critical Infrastructure Security;
- Government Coordinating Council (GCC);
- Federal Senior Leadership Council;

- Policy Coordinating Committee;
- Federal Chief Information Officers Council; and
- Joint Interagency Cyber Task Force.

In addition, last May, DHS published the Information Technology (IT) Sector Specific Plan (SSP), which is part of the overarching National Infrastructure Protection Plan (NIPP). Each SSP outlines our common priorities, enhances sharing of information, identifies research and development priorities, and sets goals and implementation metrics. The IT SSP was collaboratively developed with the producers and providers of IT products and services through the IT Sector Coordination Council (SCC). Each of the other critical infrastructure plans also addresses cyber security, which means for every sector, be it energy, water treatment, or transportation, the Department has looked at how information technology impacts the sector, and has built that into the planning process.

The next step is implementing the plans and making sure they are followed. The Federal Government can provide incentives and in some cases exert regulatory authority to compel the private sector to act. The NIPP framework, which encompasses critical infrastructure/key resources (CIKR) owner/operator institutions and their designated trade or equivalent organizations that are identified as members of existing SCCs, is a process that has been successful. In partnership with representatives from GCCs for each sector, DHS has developed a model that works. The Department will continue using the NIPP partnership framework to advance the important mission of protecting CIKR, of which Federal networks are a part.

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

There is no unclassified version of NSPD-54/HSPD-23. However, the matter is being reviewed by original classification authorities within the Federal Government.

ROLE OF 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)?

The CNCI will comply and comport with all statutory requirements in regard to privacy and public comments. The Department's Privacy Office is fully engaged and will implement its responsibilities under the CNCI in strict compliance with the *E-Government Act*, the *Privacy Act*, and the *Homeland Security Act* to protect privacy. All DHS privacy requirements have been and will continue to be met, including the development of privacy impact assessments (PIA). DHS issued the first PIA for the EINSTEIN system in 2004 and published an updated PIA on May 19, 2008, for the improvements planned for EINSTEIN. This PIA was published on the DHS website (www.dhs.gov/privacy) for the public to read prior to those upgrades being implemented. Additionally, the Department's Office for Civil Rights and Civil Liberties has been actively involved in reviewing CNCI and ensuring safeguards are in place to protect civil liberties.

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

The Trusted Internet Connection initiative does not impair the public's access to government websites; rather, it simply creates an improved gateway that all communications to and from the government will traverse. This initiative will improve the computer network security posture of the Federal Government and in turn will help facilitate the availability of information to the public.

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

Protecting the privacy of Americans and their personally identifiable information (PII) is a priority and is required by statute. As managed under the direction of the Director of the Office of Management and Budget, each Federal agency that currently operates a website or otherwise uses information technology that collects, maintains, or disseminates information that is in an identifiable form or collects identifiable information through the use of information technology must provide a publicly available PIA. Accordingly, Federal agencies continuing to operate their websites that receive PII will be required to execute a PIA and protect the public's PII.

Additionally, Federal agencies are required to post notices on their websites, as well as at other major points of entry, that computer security information is being collected and their system monitored. Such notices cover intrusion detection systems like EINSTEIN 2. Users of Federal computer systems are provided with logon banners and sign user agreements that specifically notify them of the computer network monitoring. Participating agencies using EINSTEIN 2 are required to certify to the US-CERT that they have appropriate notices, banners, and measures in place to provide individuals with notice that their interaction with Federal networks is subject to monitoring for computer network security purposes.

As for the Department of Homeland Security and its use of EINSTEIN as an intrusion detection system, the Department published the PIA on May 19, 2008. The EINSTEIN system provides improved computer network security and, in turn, improves the protection of the public's PII by detecting and preventing the use of malicious computer exploits that target PII. Developed in 2003, EINSTEIN 1 provides an automated process for collecting, correlating, and analyzing computer network security information from voluntary participating Federal executive agencies. This program operates by collecting network flow records. Flow records are records of connections made to a Federal executive agency's IT systems. The records identify: the source Internet Protocol (IP) address of the computer that connects to the Federal system; the port the source uses to communicate; the time the communication occurred; the Federal destination IP address; the protocol used to communicate; and, the destination port. There is no PII collected, maintained, or disseminated under this system.

EINSTEIN 2, the next version of EINSTEIN, adds to EINSTEIN 1 a network intrusion detection technology that will monitor for malicious activity at Federal executive agencies' Internet Access Points. EINSTEIN 2's network intrusion detection technology uses a set of pre-defined signatures based upon known malicious network traffic. When malicious traffic triggers an alert, intrusion data will be captured along with the data that is transmitted in proximity to that alert and related to that connection. When data is captured due to an alert being triggered, there is a slight risk that personal information may be transmitted along with a malicious activity. It is the malicious activity that is the focus of data collection, and any PII information will be incidental. EINSTEIN 2 will maintain this captured information on a separate network under the control of US-CERT, which may disseminate this information with Federal executive agencies according to written standard operating procedures and in accordance with all applicable laws.

These standard operating procedures are being developed and will be implemented prior to EINSTEIN 2 being deployed. Protecting Americans' PII will be paramount in the development of these procedures, which will be similar to other computer network security and defense agency procedures. Specifically being considered as the basis for US-CERT's role are procedures from Joint Task Force Global Network Operations, National Security Agency, Federal Bureau of Investigation, and other CERT organizations. An inherent component of these procedures will be the requirement that US-CERT analysts receive annual training from the DHS Privacy Office as well as intelligence oversight training.

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?*

    While the EINSTEIN program contributes to incident reporting, a majority of the incidents reported to US-CERT comes from the internal security systems of individual departments and agencies. Therefore, the rise in number is, and will be, due both to increased reporting and increased deployment of EINSTEIN.

    The EINSTEIN program provides situational awareness information for the Federal Network Enterprise by deploying sensors that detect and report on security incidents. As the program expands the number of deployed sensors and OMB is successful in reducing the number of Internet Access Points through the implementation of the Trusted Internet Connections (TIC), the number of reported network security incidents is expected to rise. This expected rise may be attributed to the consolidation of connections that may now be scanned by EINSTEIN sensors as well as the expected continuation of attempts by cyber adversaries to gain unauthorized access to Federal networks.

As implemented currently, EINSTEIN informs the U.S. Government on the depth and breadth of the cyber intrusion problem across the entire Federal Network Enterprise. It is an assessment tool that measures the extent of the overall problem, the target (department, agency, or specific information of interest), objectives, and success of the intrusion attempts. It is through this situational awareness information that the U.S. Government can better address identified gap areas and increase its network security posture.

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

NCSD developed a Performance Measures Plan (PMP) to describe the methodology, processes, procedures, and supporting roles and responsibilities for collecting, analyzing, and reporting NCSD performance measures data. The NCSD PMP was initiated to support multiple legislative mandates regarding performance measurement. For example, the *Government Performance and Results Act of 1993* requires each government agency to prepare an annual performance plan that establishes strategic goals and the level of performance in an objective, quantifiable, and measurable form. The Program Assessment Rating Tool program mandated by OMB is another approach NCSD uses to keep itself accountable of its performance requirements. Additionally, the *Clinger Cohen Act of 1996* stipulates establishing performance measurements for improving efficiencies and effectiveness of agency operations.

Initially, NCSD will determine that the CNCI is being fully and successfully executed by measuring the percent of planned EINSTEIN sensors deployed on time throughout the Federal Government. This measure assesses the percent of planned EINSTEIN sensor deployments that are completed on time. With the full implementation of these sensors, visibility into the potentially malicious cyber activity and throughout the Federal cyberspace will dramatically increase. The sensors will provide more comprehensive situational awareness information to help us better understand the current environment and identify vulnerabilities, risks, and mitigation actions.

Additionally, the following potential measures are being evaluated: (1) the percent Resolution Rate of cyber incidents reported is a measure to determine how efficiently US-CERT is resolving incidents reported to them by various stakeholders; (2) Average Resolution Time in calendar days when cyber incidents are reported is a measure to determine how efficiently US-CERT is resolving incidents reported to them by various stakeholders; (3) Average Time (days or hours) used to publish cyber alerts on the website is a measure to see how quickly US-CERT is informing stakeholders of potential cyber danger; (4) number of Cyber Training and Education Programs conducted by NCSD is a measure to determine how well NCSD is educating their stakeholders on cyber issues; and (5) number of civilian agency's preparedness and contingency planning tests and exercises conducted is another performance measure to validate how well NCSD is preparing their stakeholders for potential future cyber attacks and teaching their stakeholders how to protect their

information. DHS will continue to develop robust measures of success moving forward.

PRIVATE SECTOR

15. *It is 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?*

    The CNCI formalizes a series of continuous efforts designed to further safeguard Federal Government systems and to reduce potential vulnerabilities, to protect against intrusion attempts, and to better anticipate future threats. The vision, plans, and processes involved in the CNCI initially were crafted and driven by senior Federal Government officials. This was essential because the CNCI is primarily a Federal strategy for Federal Government systems. In developing the CNCI, these Federal officials used the prevailing standards and best practices recognized by government, as well as private sector subject matter experts.

    The Department will continue to work with the private sector moving forward, just as we have done to date and as outlined in the initiative.

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

    Many cyber security experts were not consulted, but their expertise as reflected in published standards and best practices that were incorporated in the development of CNCI where relevant.

    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?*

    Last May, DHS published the IT SSP, which is part of the overarching National Infrastructure Protection Plan (NIPP). Each SSP outlines our common priorities, enhances sharing of information, identifies research and development priorities and sets goals and implementation metrics. The IT SSP was collaboratively developed with the producers and providers of IT products and services through the IT Sector Coordination Council (SCC). Each of the other critical infrastructure plans also addresses cyber security, which means for every sector, be it energy, water treatment, or transportation, the Department has looked at how information technology impacts the sector, and has built that into the planning process.

The next step is implementing the plans and making sure they are followed. The government can provide incentives and in some cases exert regulatory authority to compel the private sector to act. The NIPP framework which encompasses CIKR owner/operator institutions and their designated trade or equivalent organizations that are identified as members of existing SCCs is a process that has been successful. In partnership with representatives from the Government GCCs for each sector, DHS has developed a model that works. The Department will continue to use the NIPP partnership framework to advance the important mission of protecting CIKR, of which Federal networks are a part.

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?*

DHS has been working with industry partners since its inception. The Department greatly values these partnerships and looks forward to finding ways to build upon the strong foundation that has been created. DHS must carefully balance two factors with regards to private sector engagement:

1. Procurement sensitivities such as those detailed in the Federal Acquisition Regulation; and
2. Ethical questions surrounding perception.

In addition, the possibility of confusion and frustration is increased if DHS officials meet with the non-Federal sector before knowing fully what is needed from them. To that end, DHS tries to make a concerted effort to engage our NIPP partners with clear objectives, plans for action, timelines, and value propositions for why they should be there. DHS has had varying levels of success with these efforts, but has made a commitment and has set up processes to improve. Many of the CNCI's efforts are not ready yet for non-Federal sector engagement.

The government built the CNCI to define and clarify many difficult issues that relate to securing Federal networks and systems. Among them is leadership, definitions of need, and how to handle both procurement and Federal Advisory Committee Act issues. The Federal Government is in the process of preparing multiple projects for some level of industry engagement. It should be expected that some of the efforts will be at the classified level, while others will be For Official Use Only.

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

The non-classified portions of CNCI will be coordinated with the IT Sector Coordinating Council under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate effective coordination between Federal infrastructure protection programs and the infrastructure protection activities of

private sector IT owners and operators. The CIPAC is a partnership between government and CIKR owners and operators. CIPAC provides a forum where government and industry CIKR owners and operators can engage in a broad spectrum of strategic coordination and protection activities to advance the interests of critical infrastructure protection. CIPAC will enable government and relevant industry to coordinate on matters of mutual interest regarding 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 the 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?*

    The Privacy Impact Assessment for EINSTEIN 2 was published to the DHS website, www.dhs.gov/privacy, on May 19, 2008. A copy of the PIA is enclosed.

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

    Under the current Office of Management and Budget (OMB)-led TIC Initiative, all Federal Government agencies are to identify their required Internet Access Points to OMB by June 2008. Once that is accomplished, the Federal agencies' Internet Access Points will be prioritized for the purpose of determining where the EINSTEIN Intrusion Detection System (IDS) will initially be deployed. The Department plans to begin deployment in late summer 2008.

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

    As the PIA states, the updated version of EINSTEIN will incorporate network intrusion detection technology capable of alerting US-CERT to the presence of malicious or potentially harmful computer network activity in Federal executive agencies' network traffic. EINSTEIN principally relies on commercially available intrusion detection capabilities to increase the situational awareness of US-CERT. This network intrusion detection technology uses a set of pre-defined signatures based on known malicious network traffic. The signatures currently being considered are based on malicious code and are not based on PII, nor are the IDS programmed specifically to locate or capture PII. Future signatures might be developed in response to threats that use what appears to be PII. The purpose of the signature is to prevent malicious activity from reaching Federal networks,

not to capture PII. For example, if a computer security exploit chose to use PII in the delivery of malicious code, as was done with the Melissa Virus, a signature could be developed in response to that exploit which could contain PII. Accordingly, while the IDS will collect some PII that is related to malicious code being transmitted to the Federal networks, its main focus is to identify the malicious code and protect Federal networks, not to collect PII. Identifying malicious code across the Federal networks increases situational awareness and provides an improved real-time ability to address computer network incidents on Federal systems.

As for the technology of the system, two-factor authentication (e.g., a password and a physical token) is required for access to the EINSTEIN 2 flow records by participating agencies and for access to the portal that contains more detailed trend and computer network security information. EINSTEIN 2 information itself is not shared outside the Department, except in the form of reports on subjects including general computer network security trends, specific incidents after minimizing PII, and anomalous or suspicious activity observed on Federal networks.

The EINSTEIN system is located on a separate fire walled network used only by trained US-CERT personnel. Data integrity and security have been built into the EINSTEIN program from the very beginning. US-CERT analysts are required to undergo extensive training and background checks to ensure that they conform to the established policies, procedures, and processes required by US-CERT. Furthermore, the systems that collect the information in EINSTEIN have undergone certification and accreditation and are monitored 24 hours/seven days a week for integrity and security. US-CERT uses two-factor authentication and robust information security practices to maintain the integrity, confidentiality, and availability of the system.

OTHER RESPONSIBILITIES OF DHS

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

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

    The investment of $115 million enacted by Congress toward DHS's cyber security efforts this year and the additional $192 million in the President's FY 2009 budget make up the financial foundation that will fund a dramatic increase in our staffing, technical capabilities, and equipment. All funding decisions are monitored by Appropriations Counsel and the Office of the Chief Financial Officer to ensure compliance with Federal appropriations law and Congressional intent. The Department takes this responsibility seriously and recently reorganized the NCSD. Many NCSD division heads will now be

members of the Senior Executive Service. This will provide NCSD with the necessary senior level management to guide it through this growth period and beyond.

In addition to ensuring that CNCI resources are being used in direct support of the CNCI mission, NCSD established a separate recordkeeping mechanism to track, monitor, and execute the CNCI funding appropriately. NCSD has requested funding for the other cyber security missions at approximately the same level beyond FY 2008 for activities not under CNCI.

NCSD recognizes the critical importance of its responsibilities relating to its other cyber security missions. The supporting initiatives and products of non-CNCI activities are essential to improve the security of cyberspace and America's cyber assets in the United States by working collaboratively with public, private, and international entities.

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?*

NCSD is the focal point for coordinating national cyber preparedness activities, including preparing for and responding to catastrophic incidents that could degrade or overwhelm the networks, systems, and assets that operate our Nation's IT and cyber infrastructure. NCSD's primary mission is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. It also serves to focus and provide direction for the Division's activities, programs, and services.

The following is a summary of Division goals and objectives that ensure cyber security is enhanced overall, and not just within government networks:

GOAL 1: Manage cyber risk to the Nation and integrate cyber security into public and private sector preparedness efforts.

- Promote the cyber security of the Nation's CIKR;
- Reduce cyber risk related to control systems;
- Promote the security of software across the development, acquisition, and implementation lifecycle;
- Promote the development of cyber security standards and best practices and identification of cyber security research and development requirements;
- Foster training and education programs to promote the development of cyber security professionals in support of the Nation's cyber security needs; and
- Conduct cyber exercises and workshops to improve America's cyber security preparedness, protection, and detection capabilities.

GOAL 2: Maintain and enhance national cyber response capabilities.

- Enhance cyber security situational awareness and analysis to protect against, prevent, and detect cyber attacks and disruptions;
- Build and maintain effective incident response for cyber security events; and
- Provide reconstitution and recovery capabilities.

GOAL 3: Build and maintain a world-class organization to advance the Nation's cyber security preparedness and raise awareness across the Nation of cyber security.

- Promote an understanding of vision, mission, and strategy while maintaining planning, programming, budget, and financial execution plans;
- Attract and retain a skilled and motivated workforce; and
- Empower all Americans—businesses, academia, and the general population—to secure their own parts of cyberspace and collaborate with international partners.

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 classification guide for CNCI is in development. Once that document is available, the Department will provide the Committee access to the document in the appropriate setting.

- *A summary document describing all portions of the CNCI deemed unclassified;*

  An unclassified summary document describing all portions of the CNCI does not exist, but is currently being developed and will be shared with the Committee when finalized.

- *An unclassified, detailed 5-year breakdown of the DHS budget for the CNCI;*

  An unclassified, detailed 5-year breakdown of the DHS budget for the CNCI is provided in the chart that follows:

DHS CNCI BUDGET FY 2008-FY 2013 (only includes the funding for NCSD)[1] (in millions)			
Initiative, Activity, Sub-Activity	FY 2008	FY 2009[2]	
Trusted Internet Connection	$5.7	$10.8	
Intrusion Detection	$109.3	$176.4	
Analytics	$8.3	$8.5	
Front-End System	$26.3	$118.1	
US-CERT Data Center	$18.0	$14.0	(b)(5)
US-CERT Facility	$42.9	$4.9	
US-CERT Operations	$13.8	$30.9	
Cyber Education & Expertise		$5.0	
Supply Chain Risk Management		$5.0	
GRAND TOTAL	$115.0	$197.2	

[1] This chart does not include any funding for the NCSC.
[2] This chart does not contain a FY 2009 Overguidance Request (OGR) for an additional $25 million for the Front End System.

- *An unclassified summary of the roles and responsibilities of the NCSC, including the level at which the Center will be funded.*

  The National Cyber Security Center (NCSC) will coordinate and integrate information necessary to help secure U.S. cyber networks and systems and help foster collaboration among Federal cyber groups. In particular, the NCSC will advance the coordination and consultation among the various Federal cyber entities responsible for various parts of the cyber security missions. The funding level has yet to be determined. DHS will be happy to provide the Committee with a briefing in the appropriate setting.

- *A detailed implementation plan of DHS's responsibilities under the CNCI, including how contract staff will be used to support the NCSD;*

  The Committee has received classified briefings regarding DHS's responsibilities under the CNCI. In addition, Under Secretary Robert Jamison testified before your Committee on March 4, 2008, in a classified session to discuss the specifics of the Comprehensive Cyber Security Initiative, as well as the roles and responsibilities of DHS. Additionally, Under Secretary Jamison testified before the House Homeland Security Committee on February 28, 2008, in an open, unclassified session on the two unclassified portions of the CNCI: TICs and EINSTEIN. DHS is happy to provide the Committee with unclassified briefings regarding these two programs.

Concerning the unclassified detailed DHS implementation plan of CNCI, the following activities have been initiated by US-CERT/NCSD to implement the CNCI:

- NCSD is developing a comprehensive implementation plan, which outlines roles, responsibilities, and staffing levels for Federal and contractor personnel;
- NCSD is in the process of converting a target number of 50 contractor personnel positions into Federal positions. This will result in a cost-savings to the program and a more stable workforce; and
- NCSD is currently evaluating future program requirements and the appropriate contract type (firm-fixed price, time and material, etc.) needed as it relates to financial and mission risk to the government.

- *Any plans pertaining to enhancements of the EINSTEIN Program.*

Technological upgrades and planning activities are classified. DHS will be happy to provide the Committee with a briefing in the appropriate setting.