INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

December 10, 2008

The Honorable Jim Nussle
Director
The Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Mr. Nussle:

I am writing to you on behalf of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) (P.L. 107-347). One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

On September 5, the Board heard briefings about the EINSTEIN and EINSTEIN2 programs, intrusion detection systems that monitors the network gateways of government departments and agencies in the United States for unauthorized traffic, and a separate non-classified briefing on the Comprehensive National Cybersecurity Initiative (CNCI) including EINSTEIN.

ISPAB believes that the CNCI, as we understand it, is an important step to ensuring information security in the government. We also applaud the moves that we have heard discussed toward creating more transparency of the initiative and EINSTEIN. I write today on behalf of the Board, in part, to suggest that greater clarity and transparency is necessary to ensure both the effectiveness and trustworthiness of the program. We are not suggesting that the government expose classified or other overtly sensitive information that could be used by adversary or would violate letter or spirit of FISMA or other security laws, but instead that it provide enough information for better oversight of privacy and security law and policy.

Specifically, we commend the Department of Homeland Security (DHS) on its steps to make information on EINSTEIN2 available, but we have some concerns over broader questions raised by the Privacy Impact Assessment (PIA) for the program.

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

First, the PIA only covers DHS and not the individual agencies where information will be collected prior to transmission to DHS from the EINSTEIN2 sensors. We suggest that each agency draft a small addendum that would be attached to the DHS PIA, discussing how the agency works with DHS and any effects on agency handling of personally identifiable information -- including how law enforcement and other agencies may use information specific to that agency. We were pleased to see that US-CERT will enter into Memoranda of Agreement with each participating Federal agency that will ensure that agencies "post notices on their websites and on other major points of entry that computer security information is being collected and that the agency systems are monitored agency" according to the DHS privacy office Annual Report. We urge OMB to monitor this process and, consistent with the appropriate national security exemption in Section 208 of the E-Government Act, ensure that adequate PIA addenda are created by each agency as part of the DHS PIA.

We also have concern over specific language in the EINSTEIN2 PIA. The PIA suggests that "...Internet users have no expectation of privacy in the to/from address of their messages or the IP addresses of the sites they visit" (page 18). Written this broadly, the statement is a change from previous government policy that has suggested that there is an expectation of privacy based on the use of Internet header information such as IP address including OMB guidance on privacy policies (OMB Memorandum M-99-18), which indicates that agencies should provide notice that they collect IP addresses and that this information may be shared; most agency web sites, including those of the White House and the DHS, state that users have some expectation of privacy to know that header information is being collected. Also, agencies have denied Freedom of Information Act (FOIA) Requests for the IP address of visitors to the agency Web site under the privacy exemption of FOIA -- suggesting that users have legal expectations of privacy over that information.

We urge OMB to recommend that DHS clarify the above language in the PIA to explain that any privacy interest in IP address and other header information is being adequately addressed by DHS through fair information practices, considering the significant law enforcement and national security interest in use of this information by EINSTEIN2.

Based on briefings before the Board, there are other issues in the broader CNCI where further transparency and oversight would be useful. First, the CNCI necessitate that civilian agencies now interface more with national security systems. As such, PIAs for non-national security systems now increasingly address classified information, which has led to the withholding of those PIAs under the E-Government Act's exemption for classified data. In order to meet the goals of the Act and build trust in government Web sites, we suggest that where classified PIAs are withheld, an independent but appropriately cleared government entity review such PIAs to determine whether privacy has been adequately addressed and protected without releasing the information. We would be pleased to assess further where such an entity could be best placed in the government, and what the qualifications of the members should be.

Second, we are concerned that the overarching PIA for the CNCI is not public. Because the CNCI relates to systems that are both classified and non-classified, we advise that OMB work with the Director of National Intelligence (DNI) to release a complete, unclassified PIA consistent with the E-Government Act's requirements. We commend OMB and DNI for moving

to release more information about the initiative; we believe that the release of a full unclassified version of the CNCI PIA, rather than just a redacted version or the current PIA, would be useful to those who are interested in understanding the initiative's impact on privacy. We would also recommend that information on which CNCI systems are covered by the Privacy Act and where the Privacy Act Systems of Records Notices are published be made publicly available.

We appreciate the opportunity to offer the Board's views on this critically important issue. Please let me know if the Board can answer any questions or take additional actions to support implementation and oversight of the EINSTEIN and CNCI projects.

Sincerely,

Ari M. Schwartz
Information Security and Privacy Advisory Board