INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

The Honorable Karen Evans
Administrator for Electronic Government and
Information Technology
The Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Ms. Evans:

I am writing to you as the Chair 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 Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act of 2002. 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.

At its December 2006 and March 2007 meetings, the Information Security and Privacy Advisory Board received outstanding briefings on disaster recovery operations following Hurricane Katrina and the 9/11, World Trade Center attacks. We would like to commend these briefings to the Federal information technology community. Moreover, the Board believes that IT security and privacy considerations should be built into disaster recovery planning and implementation going forward, to ensure that new problems are not introduced in providing critical emergency services. Once the immediacy of a disaster recovery subsides, seemingly less important security or privacy vulnerabilities can continue and introduce new risks or threats if not dealt with directly. Such risk reduction should be done in a manner consistent with important Administration policy goals for disaster recovery, including those outlined in HSPD 20.

Specifically, Gilbert Hawk, the Chief Information Officer at the Department of Agriculture National Finance Center (NFC), spoke at our December meeting on the implementation of the NFC's information technology contingency plan following Hurricane Katrina. The Board was very impressed with the institutionalized disaster recovery planning process that NFC has implemented. We noted that this greatly facilitated the nearly seamless restoration of information processing services to the Department of Agriculture and other supported agencies. This is truly an example of contingency planning "done right."

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-8670

At the March 2007 meeting, we heard from representatives of Verizon and AT&T about how they restored data and voice communications capabilities to lower Manhattan following the 9/11 attacks. Once again, the Board was very impressed with the communications restoration capabilities that these companies demonstrated following this catastrophic event.

The Board discussed whether IT, information, and personnel security issues were addressed by those leading the response to Katrina and 9/11. For the most part, such issues were seen as the job of others, such as CIOs or CSOs, who worked with the lead first responders. However, in developing temporary communications networks during crisis response, reconstituting data centers and business processes during recovery, and providing physical and logical access to emergency planners and responders, new vulnerabilities can occur at each step if these and similar actions do not account for proper security and privacy protocols. Absent such protocols, for example, sensitive information that is shared during an emergency may continue to be shared without appropriate notice or consent, after the emergency situation subsides. During its public meeting on June 6-7, 2007, the ISPAB approved the following recommendations:

- The ISPAB recommends that OMB and NIST work with DHS and other involved agencies to issue guidance on incorporating sound security and privacy practices into emergency response. For example:
  - Emergency response guidance should note that security and privacy vulnerabilities must be identified as part of planning.
  - Mitigation strategies should be introduced during implementation.
  - With regard to security, while protecting the availability of information is a key consideration in disaster recovery planning, more attention should be paid to planning for protecting the confidentiality and integrity of information as well.
- The ISPAB recommends that the OMB, working with NIST, GSA, and DHS, work with the National Coordinator under HSPD 20 to develop means of disseminating outstanding examples of effective contingency planning within the government, such as those cited above. This effort should also address how to incorporate security and privacy into these activities. It is recommended that special attention be made to involve senior managers at the CIO level.

The ISPAB appreciates the opportunity to comment on this important issue.

Sincerely,

Dan Chenok
Chairperson
Information Security and Privacy Advisory Board

cc.: Mr. Jim Nussle, Director, The Office of Management and Budget