COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

Washington/North Gaithersburg Hilton Hotel
620 Perry Parkway
Gaithersburg, MD

December 3-5, 2002

Tuesday, December 3, 2002

Board Chairman, Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board Meeting (CSSPAB) for its fourth meeting of the year at 9:00 a.m.

In addition to Chairman Reeder, members present during the meeting were:

Peter Browne
Lynn Bruneau
Mary Forte
Susan Landau
Leslie Reis
John Sabo
Jim Wade

Chairman Reeder also welcomed Susan Zevin, Acting Director, Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST).

The entire meeting was open to the public. Over the three days of the meeting, there were 15 members of the public in attendance.

Because of impending inclement weather predicted for Thursday, December 5, the Board agreed to conduct all of it business and adjourn by the end of the meeting session on Wednesday, December 6.

Briefing on Homeland Security

Mr. David Howe, Chief of Staff, White House Office of Homeland Security (OHS) briefed the Board on the current draft of the President's Critical Infrastructure Protection Board's (PCIPB) National Strategy to Secure Cyberspace **[Ref. 1]**. Mr. Howe discussed the background of the strategy and where it is today. The outline of the Strategy included the case for action, policy and principles and the audience that it was intended for: home users and small business, large enterprises, critical sectors such as the Federal, State and local, higher education and private industry, national priorities and global.

Mr. Howe said that priorities at the national level are to secure shared systems, create a reinforcing economic and social fabric, and the development of national plans and policy. The Federal government will be a model for the rest of the country. OHS recognizes that cyberspace is an international infrastructure, and they will work with those international partners to make cyberspace more secure.

With regard to the cooperative effort between the public and private sector organizations, Mr. Howe said that their view is that mandates and regulations are not good strategies for the

Government to impose on the private sector arena. Engaging in private sector relationships is a better vehicle to create partnerships to accomplish the goals of the Plan.

Mr. Howe indicated that the establishment of the Department of Homeland Security should help to identify the specific responsibilities and tasks and who will carry them out. A subsequent implementation plan will be developed on how some of these things will take place.

To the question of corporate America's impact in the requirements and regulations in the area of computer security, Mr. Howe answered that the Government will encourage accountability and sharing of information and that ISC's are expected to continue to play as positive a role as they are now.

Mr. Howe said that there were no plans to release the comments that they had received on the draft Strategy out of respect for the privacy of the statements made through the White House system. They will, however, synthesize the comments and make that information available.

Chairman Reeder commented that it had been said that the main problem with the draft Plan was a lack of an real-time alert system. Dick Clark has indicated that the real problem was not the lack of a threat analysis but of a vulnerability analysis. Mr. Howe indicated that part of the issue is once the comprehensive plan is put in place we need to allow for time to see what happens and reflect before considering making adjustments to the Plan.

Susan Zevin, ITL Acting Director, stated that NIST has been involved in the area of continuity of operation especially in the health care sector. She reflected that there was not much in the Plan about information assurance. Dr. Zevin said that she believed that there should be a stronger emphasis on information assurance for laboratory certification and accreditation in all areas, not just in the health care area. Mr. Howe said that they had done some coordination with different members of the health care sectors and as it grows, it will be reflected in the Plan. On the issue of information assurance, Mr. Howe said that there had been strategy discussions with the National Information Assurance Partnership (NIAP) effort to see if there is an effective way to develop incentives. The PCIPB looks at NIAP as an example of what can be done.

Chairman Reeder asked Mr. Howe how the Board could help to advance the Plan in making Government systems more effective. Mr. Howe replied that the comments offered by the Board at the meeting were invaluable. He said that it would be useful to have this Board help to coordinate the flow of information out to the Federal government, to look at the Federal section of the strategy, and from the Board's perspective, tell them what ways the Board can assist in making progress on the implementation of the strategy. Mr. Reeder offered to have the PCIPB task the Board with any assignment that would promulgate this work effort. Mr Howe indicated that he would relay the Board's offer.

Update on Activities of the NIST Computer Security

Next to present was Mr. Ed Roback, Chief of the NIST Computer Security Division **[Ref. #2].**

Mr. Roback's briefing focused on three recently passed computer security-related Congressional Acts: the Homeland Security Act, Cyber Security Research and Development Act and the Federal Information Security Management Act.

The Cyber Security Research and Development Act expands the role of the Board to include that they (the Board) identify research topics for the NIST grants to higher institutions (in accordance with the Act, Section 8a), including research needs related to computer security, privacy and cryptography. It also provides for the Board, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.

The Federal Information Security Management Act (FISMA) establishes an information technology framework based on NIST standards. Continuing key areas include developing security standards, guidelines, and associated methods and techniques for information services and conducting security research to understand vulnerabilities and develop new security techniques. New key areas identified include (1) developing information categorization based on levels of sensitivity; (2) developing guidelines for information classification for each category; (3) developing minimum security requirements by category; (4) incident detection and handling guidelines; (5) assistance to agencies and the private sector; (6) developing performance indicators/metrics; (7) evaluating security policy and technologies for federal use – private sector and national security systems; and (8) identification of national security systems guidelines. Mr. Roback indicated that NIST has several draft Special Publications already in place that address many of the new key areas outlined in the Act. NIST is also required to solicit recommendations of the Board on draft standards and guidelines. FISMA renamed the Board to the "Information Security and Privacy Advisory Board." It also augmented its mission to state that the Board is "*to advise the Institute, the Secretary of Commerce, and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including through review of proposed standards and guidelines developed under section 20."* The Act also requires that the Board submit an Annual Report.

Advisory Board Responsibilities and CSSPAB Role

Mr. Michael Rubin, NIST Counsel, informally covered the role of advisory committees/boards: what they do, where they meet, and whom they report to. This Board has been chartered to advise that agency that chartered it (NIST) and NIST typically works with the Board to set up an agenda that would be of equal interest to the Board and give the Federal agencies the benefits of the advice of the Board members. The Board does not take on specific functions for the Government. Mr. Rubin stated that to advise well is to reach common understanding of things that would be useful to the Board and the agency. As to the question of who does the Board report to, Mr. Rubin said that there was a set of mixed messages in this situation. Congress has expanded the scope of the Board to advise Congress. However, Commerce has identified the Board members as Special Government Employees and, as such, they are subject to the same restrictions as all Commerce employees. Therefore, letters to the Congress have to go through the appropriate chain of command up to the Secretary of Commerce for transmittal to the Congress. Mr. Rubin did acknowledge the problems inherent in this type of mechanism. Mr. Rubin did point out that any meeting that is duly noted in the Federal Register that takes place and produces reports, findings, letters, etc, automatically becomes part of the public record. Also, each member could transmit any of these items as a private individual as long some type of disclaimer is made that the views expressed are those of the sender only and not of the Board collectively. Mr. Rubin acknowledged that he did not think that it is in the best interest of NIST or Commerce to not forward what the Board recommends.

Mr. Rubin stated that he wants the Board to advise NIST if they see anything that is unlawful or unethical. The proposed grants program affiliated with the Cyber Security Research and Development Act is one area that Mr. Rubin would like for the Board to pay special attention to.

On the topic of meeting venues, Mr. Rubin believes that the public should be able to reach the Board geographically and that should be taken into consideration when planning meeting venues. The Board should stay within the United States and conduct their meetings at facilities that are open to the public.

In closing, Mr. Rubin said that the charter of the Board would be amended to reflect its new name and changes to its mission. With regard to the Board's interaction on the proposed NIST grants program, he would like to see it follow along the lines of what has been done with NIST's Advanced Technology Program (ATP) effort. Mr. Rubin would like to see the Board be consulted

while this effort is in its early procedures/preparation stage, as he would like for this Board to assist in defining good procedures.

OMB Updates

The next speaker was Mr. Norman Lorentz, Chief Technology Officer, Office of Management and Budget. He briefed the Board on the status of the Federal Enterprise Architecture (FEA) effort **[Ref. #2]**. This project was first headed by Debra Stouffer, now the Chief Technology Officer at the Environmental Protection Agency, prior to Mr. Lorentz's arrival in January 2002.

The FEA provides OMB and Federal agencies with a new way of describing, analyzing, and improving the Federal government and its ability to serve the citizen. It will eliminate the organizational obstacles that have historically hindered improvement without forcing reorganization. The FEA is a business-focused approach and is not just for Information Technology. It provides a common framework for improving a variety of key areas such as budget allocation, cross-agency collaboration, improved service to the citizen, e-government, etc.

The Chief Information Officer (CIO) Council has sanctioned this program and they serve as the sponsors. A first version of the FEA is expected to be available in early 2003.

Kamela White of OMB's Office of Information and Regulatory Affairs briefed the Board on the recent computer security activities. Ms. White reported that Congressman Steve Horn had issued his annual grading of Federal agencies computer security program effectiveness and the Government received a failing grade again this year. In recent OMB testimony, Mark Forman said that progress was made in most every agency and not all problems identified could be fixed within one year. The key to success is to establish a process so that when problems are identified, a plan of action is in place to correct them. OMB will prepare a summary report of their reviews to send to Congress. They will also transmit their findings to the respective agencies. Ms. White reported that FISMA continues the Government Information Security Reform Act (GISRA) requirements. Basic agency requirements do not change but stronger enforcement may be put into place. OMB will issue guidance on the changes early next year. The materials that OMB used to evaluate agencies grades were the agencies annual reports, IG reports, and any past assessment reports performed by the General Accounting Office. OMB does not see the grading process stopping because Congressman Horn will be retiring from Congress at the end of this Congressional session. It is anticipated that Representative Tom Davis (R-VA) will take over as chairman of the House Government Reform Committee from Representative Dan Burton.

Activities of the National Archives and Records Administration's (NARA) Electronic Records Archive Group

Mr. L. Reynolds Cahoon, NARA's Chief Information Officer, presented a briefing on the activities of their electronic records archive project **[Ref. #4]**. The mission of NARA is to ensure continuing access to essential evidence that documents the rights of American citizens, the actions of Federal officials and the national experience. NARA's strategic goals are that (1) essential evidence will be created, identified, appropriately scheduled, and managed for as long as needed; (2) essential evidence will be easy to access regardless of where it is or where users are for as long as needed; (3) all records will be preserved in an appropriate environment for use as long as needed; and (4) NARA's capabilities for making changes necessary to realize their vision will continuously expand. Mr. Cahoon explained the definition of what an electronic record or digital document was in a recordkeeping context and the challenges to preserving an electronic record. NARA's vision is that the Electronic Records Archives (ERA) will authentically preserve and provide access to any kind of electronic record, free from dependency on any specific hardware or software. Mr. Cahoon reported that the Architecture component of the CIO Council assisted NARA in developing the components for the ERA. When operational, ERA will make it

easy for NARA customers to find records they want and easy for NARA to deliver those records in formats suited to customers' needs. ERA will preserve essential evidence and make it more accessible in every sector of society. Mr. Cahoon would welcome returning to brief the Board on the progress of this activity in the future.

The meeting was recessed for the day at 5:10 p.m.

December 4, 2003

Chairman Reeder reconvened the meeting at 9:05 a.m.

NIST Digital Records Activities

Chairman Reeder introduced Dr. Victor McCrary, Chief of the Convergent Information Systems Division at NIST. Dr. McCrary began his presentation with an overview of the activities of his Division **[Ref. #5]**. These activities focused the digital dilemma issues facing the industry for digital content; and a legislative and government initiatives overview. NIST has a digital data preservation laboratory. The lab partners with industry to work towards voluntary industry standards conformance, and convening the industry to develop sector solutions. They look at the different types of strategies that have been employed. They also look at the different technology development trends in areas such as analog, longevity, migration, and emulation/technology preservation. NIST has an optical disk compliance test program available. There are standard and interoperability test functions available for customers to download and apply. Dr. McCrary said that NIST is interacting with other Federal agencies' libraries as well as outside entities to see how they are pursing the development of standards to migrate into this area. Chairman Reeder noted that two issues of interest from the computer security perspective are authentication [non-repudiation] of media and the correlation between confidentiality and preservation of the data. Dr. McCrary said that NIST is working with the biometrics community on this issue.

NIST Guidelines for Security Certification and Accreditation of Federal Information Technology Systems

The next speaker was Mr. Ron Ross of NIST's Security Testing and Metrics Group. Mr. Ross briefed the Board on assessing the security of Federal information technology systems **[Ref. #6]**. The complexity of today's systems and networks presents great security challenges for both producers and consumers of information technology. Mr. Ross pointed out that there needs to be greater confidence in the security of enterprise IT systems, consistency in the approaches used to assess the capabilities and limitations of IT systems in Federal agencies. The shortage of software engineers and IT personnel in general is another one of the challenges being faced. To assist agencies in meeting the requirements of OMB Circular A-130, NIST is developing a guidance document covering security certification and accreditation of Federal information technology systems. The first phase of this program objective is to develop standardized guidelines for conducting security certification and accreditations of federal IT systems. NIST already has three Special Publications available [SP 800-37, SP 800-53, and 800-53A]. The second phase is to create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the standardized guidelines.
The NIST Security Accreditation Model (1) defines standardized IT system security controls for confidentiality, integrity, and availability, and defines standardized techniques and procedures to verify correctness and effectiveness of security controls; and, (2) looks at the risk assessment and security plan and defines the standardized security certification and accreditation process for IT systems. The certification and accreditation process is done in four phases: pre-certification, certification, accreditation, and post accreditation. Mr. Ross reviewed the key security factors

used and the levels of concern for each of the three factors. He explained the criteria for the three levels of security certification and reviewed the definitions for management, operational and technical controls. The certification package will consist of an updated security plan, security test and evaluation reports, a final risk assessment report and certifier's statement.

Chairman Reeder thanked Mr. Ross for his presentation and stated it was his observation that this work effort was very complimentary to the Board's focus on setting minimum benchmark standards.

Briefing on GSA's E-Authentication Program Activities

Mr. Stephen Timchak, eAuthenication Program Manager, GSA, briefed the Board on the status of this work effort **[Ref. #7]**. Mr. Tyson Young, a team leader from NASA's Gateway Development effort, accompanied Mr. Timchak. The project's mission is to establish public trust in the security of information exchanged over the Internet. Its goals are to build and enable mutual trust needed to support wide spread use of electronic interactions, minimize the burden on the public when obtaining trusted electronic services from the Government and to deliver common interoperable authentication solutions. Mr. Timchak identified the challenges to interoperability and the need for authentication gateways that will simplify and unify that interoperability. He reviewed the accomplishments of this effort during FY02 and the course of action for FY03. Mr. Timchak summarized his presentation by stating that Authentication Gateway capabilities exists in FY03; acquisition of production Gateway services will be conducted early in the second quarter of FY03; a draft Statement of Objectives is scheduled for release later in this month of December; industry is proprietary and moving towards open solutions; no FY03 funding has been received; and e-Gov applications and others can be interfaced to the Gateway at this time.

Public Participation

Mr. Peter Bachman of CEQUS Inc., addressed the Board as a member of C=US Directory X.500. The X500 is working with the European Community to develop a European human rights charter in IT design format. Mr. Bachman wanted to inform the Board of his efforts in getting privacy issues into the European project. He welcomed their comments on this activity.

Board Discussion Period

The motion was made to accept the minutes as edited. The vote was unanimous.

Dr. Fran Nielsen, NIST Secretariat, brought the Board's attention to a number of emails that she had received in opposition to the Total Information Awareness (TIA) Program. These requests were asking for the Board to recommend that the TIA program not be adopted. These comments were noted and it was the view of the Board that this was not a matter that the Board would take action on at this time.

Chairman Reeder acknowledged the resignation of Board Member, Mary Forte, who was leaving the Board to accept another assignment within NSA. He said that her balance of humor and insight was an invaluable asset to the Board and, on behalf of the Board, he wished her success in her new position. NSA will nominate another candidate to fill this position in the near future.

Chairman Reeder also thanked Board Secretariat members, Elaine Frye and Tanya Brewer-Joneas for the seamless job that they perform for the Board. Mr. Reeder offered special thanks to Dr. Fran Nielsen for being a substantive contributor to the efforts of the Board as the Designated Federal official (DFO) of the Board. Dr. Nielsen will be relinquishing this role to take

on other priorities for NIST. The new DFO will be Ms. Joan Hash, Manager of the Management and Assistance Group at NIST.

Board Member John Sabo presented his draft letter to transmit the Board's comments on the draft National Cybersecurity Plan. After review and discussion, the Board approved a final letter to be forwarded to the attention of Mr. Howe in the Office of Homeland Security **[Ref. #8]**

Board Members Susan Landau and John Sabo presented their proposal for a possible session to be titled "Myths and Reality: Privacy and e-Authentication. What are the Real Issues?" The proposal listed five possible panels: (1) Tracking Our Citizens: Privacy Issues Raised by E-government Services; (2) Simplicity, Cost, and Ease of Use: The Architecture of e-Authentication; (3) Designing Privacy into E-government; (4) Security Issues in E-government; and (5) The Privacy Act and E-government: Are They Compatible? The Board would provide two roles in this effort: they would organize the sessions, and provide a brief and timely report to NIST and the Department of Commerce and OMB with a clear discussion of the privacy/security/cost and risk management trade-offs. Members provided their feedback to the proposal and suggested possible speakers for the panel sessions. Board Members Landau and Sabo will continue to refine this effort.

There being no further business, the meeting was adjourned at 4:31 p.m.

Ref. 1 – Howe presentation
Ref. 2 – Roback presentation
Ref. 3 – Lorentz presentation
Ref. 4 – Cahoon presentation
Ref. 5 – McCrary presentation
Ref. 6 – Ross presentation
Ref. 7 – Timchak presentation
Ref. 8 – Letter to David Howe on National Cybersecurity Plan

Fran Nielsen
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman