INFORMATION SECURITY AND PRIVACY ADVISORY BOARD
SUMMARY OF MEETING

DoubleTree Hotel and Executive Meeting Center
1750 Rockville Pike
Rockville, MD

March 21-23, 2006

Tuesday, March 21, 2006

In the absence of Chairman Reeder, Board Member Leslie Reis called the meeting to order at 8:54 a.m. Members in attendance were Joe Guirreri, Daniel Chenok, Morris Hymes, Sallie McDonald, Steve Lipner, Howard Schmidt, Susan Landau, Rebecca Leng and Lynn McNulty. Chairman Reeder joined the meeting by noon. Alex Popocwyz joined the meeting via teleconference during portions of the agenda.

Professsor Reis announced that Mr. Guirreri's appointment to the Board was now official. She also announced that her appointment to the Board and Dr. Susan Landau's appointment to the Board had been extended by one year.

It was announced that Dr. William Jeffrey, the NIST Director, approved the appointment of Board Member Daniel Chenok as the new Chairman of the Advisory Board, effective April 1, 2006. Current Chairman Franklin Reeder's appointment term expires as of March 31, 2006.

Board Member Morris Hymes announced that Mr. Richard Schaeffer is the replacement for Mr. Dan Wolff as head of the National Security Agency's Information Assurance Directorate.

Board member Susan Landau reported on her current efforts regarding the Federal Communications Commission recent rulings on the Communications Assistance for Law Enforcement Act's applicability to Voice over Internet Protocol.

Board member Howard Schmidt reported on his testimony before a hearing of the Subcommittee on Regulatory Reform and Oversight of the House Small Business Committee. The Acting Director of the NIST Information Technology Laboratory, Ms Cita Furlani, was also one of the witnesses to testify at this hearing.

There were seven members of the public in attendance during the meeting.

Federal Privacy Policy Review

Board Member Reis reviewed the draft mission statement and work plan approach of this review effort. She reported that she had met with Mr. Jim Harper and Mr. John Sabo of the Department of Homeland (DHS) Security Data Integrity and Privacy Advisory Board in early January to discuss this mutual work effort. Professor Reis distributed a copy of the DHS's Advisory Board framework document on this same area to the Board members. She noted that this particular framework document pertains primarily to DHS programs as opposed to any legal framework overall for federal agencies. The ISPAB is looking at the effort from the Fair Standards Principles approach. Actions for the Board are to determine what the ISPAB's approach would be in working with DHS on this effort. Professor Reis said that the ISPAB needs to develop a list of specific policies and recommendations that they want to examine for the subcommittee to research and report back to the Board, keeping in mind that the ISPAB task would cover the general, broader area. Board Member Joe Guirreri noted that there is a lack of an objective statement along with the mission statement. Board Member Chenok commented that the Board's objective is not to attempt to suggest any revisions to the Privacy Act but to identify and review the legal and policy framework issues, especially in light of technology changes since the passage of the Act. There is a need to identify what areas of technology such as RFID, automation issues, categories or areas of technology like encryption and the demands that these new technologies create. Mr. Chenok suggested that the creation of two lists could be useful. One list could contain legal and policy items and the other list could contain those issues brought about by technological changes. The proposed output of this activity could consist of one or two recommendations along with a white paper outlining the resulting findings. The members of this subcommittee work effort include the following Board Members: Leslie Reis, Dan,Chenok, Lynn McNulty, Howard Schmidt and Sallie McDonald.

Remarks by Acting ITL Director, Cita Furlani

Ms. Cita Furlani, Acting Director of the Information Technology Laboratory, met with the Board. Her remarks covered NIST's involvement in the President's American Competitiveness Initiative in the science arena where it is anticipated that over the next ten years there will be a doubling of investment dollars in the NIST laboratories and infrastructure. Ms. Furlani will be focusing on the development of an IT strategy for the Laboratory that will reinforce NIST's role in measurement science and technology innovation. ITL will need to define what their priorities are, where to put their resources, and where they can get the largest impact. Ms. Furlani said that she believes that the Board could help ITL with these issues. She announced that there were plans for an upcoming offsite of ITL managers and that she would like to come back to the Board at the next opportunity and bring them up-to-date on ITL activities. In the meantime, Ms. Furlani said that she would welcome any input from the Board that they may want to forward to her at any time.

Board member feedback followed.

Ms. Leng commented that the Division has been doing very well over the past few years. She specifically pointed to the risk-based standards FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. Ms. Furlani

indicated that NIST would continue to invest resources to oversee the implementation of both of these standards.

With regard to security and measurement issues, Mr. Lipner asked if NIST had any plans to go back and review 'lessons learned' or perform an impact assessment' to see if FIPS 199 and FIPS 200 are working and adjust the programs accordingly. Mr. McNulty suggested that a cost benefit analysis could be done.

Mr. Guirreri observed that there appears to be a need to come up with a method for measuring how good the computer security programs are across the government. Perhaps the approach now is not the most efficient one.

Mr. Schmidt also noted that there is a need for a mechanism to insure that improvements are made after measurements are made and improvement areas are identified.

Mr. McNulty asked about the status of filling the position of the Director of the Information Technology Laboratory. Ms. Fulani replied that candidate interview process is currently underway. However, she also indicated that NIST is still accepting applications for the position.

Ms. Leng expressed her concerns that ORACLE's recently announced FIRMWARE platform had not been tested. She made the suggestion that perhaps a laboratory program such as NIAP could test commercial software. It was noted that the National Voluntary Laboratory Accreditation Program (NVLAP) is a source at NIST that tests commercial software. Mr. Hymes pointed out that the NSTISSP#11 Directive mandates common criteria evaluation for any commercial software used by the federal government. Ms. Furlani suggested that Ms. Leng raise her concerns to OMB.

Mr. McNulty asked if there was any on-going collaboration between ITL and NIST's Manufacturing Engineering Laboratory and if there were any budget dollars available toward that end. Ms. Furlani said that there was no collaboration between the two Labs at this time.

Mr. Chenok asked about NIST's quantum information science area. Ms. Furlani said that while it was basic research driven and falls primarily in the physics area, ITL is involved in the networks program and quantum encryption areas. ITL will also be more involved in the Bioimaging effort in FY07 looking at multi-biometrics issues.

Ms. Leng asked about the ITL effort pertaining to Homeland Security Policy Directive #12. Ms.Furlani said that ITL is still working in the testing area.

Briefing on NIAP Review

Mr. Tom Anderson of the Department of Defense's (DOD) Office of Information Assurance presented a briefing on the DOD/DHS sponsored review of National Information Assurance Partnership (NIAP). **[Ref. #1]** He reported that the NIAP Review document is undergoing vetting and will be made publicly available at a later date.

The Board members engaged in conversation with Mr. Anderson as he addressed the issues found in the IDA draft report findings.

The IDA Draft Report offers six options.

The Government Accountability Office's (GAO) independent audit of the NIAP program has not been released as of yet. However, it does not recommend that NIAP activity cease. The report takes a look at whether or not it is beneficial for expanding the requirement of the NIAP evaluation process to non-national security systems.

In response to the Board's offer to help, Mr. Anderson stated that if the Board agrees that product evaluation is important to the government then this Board should make such a recommendation to OMB, NIST, and others deemed appropriate to increase support for the program and make the modification necessary to make the program more effective.

Software Assurance Session

Board member Lipner introduced the participants of the software assurance session and presented a general overview of what the session was to cover.

Mr. Joe Jarzombek, Director of Software Assurance at the Department of Homeland Security (DHS) was the first speaker. His presentation covered DHS' infosec/privacy considerations for software in advancing the national strategy to secure cyberspace. **[Ref. #2]** He reviewed the role of DHS' National Cyber Security Division to provide the framework for addressing cyber security and software assurance challenges. Mr. Jarzombek referred to areas in IT software assurance that need to be addressed. Software and IT vulnerabilities jeopardize infrastructure operations, business operations and services, intellectual property, and consumer trust. Adversaries have capabilities to subvert the IT software supply chain. There is growing concern about the inadequacies of suppliers' capabilities to build/deliver security IT software. Current education and training provides too few practitioners with requisite competencies in secure software engineering and enrollment is down in critical IT and software-related programs. There is a need for national focus in countries to stay competitive in a global IT environment. Processes and technologies are required to build trust into IT and software.

Mr. Jarzombek referenced three recent reports that address the status of the IT software assurance issues. First, a 2006 report done by the Association for Computing Machinery (ACM) Job Migration Task Force entitled Globalization and Offshoring of Software. The report provides the emerging trends, debunked myths and a more realistic picture of the current state and likely future of IT. Second, a report resulting from the United States 2nd National Software Summit, "Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness," that was produced in April 2005. The report identified four major National Software Strategy programs: (1) improving software trustworthiness; (2) educating and fielding the software workforce; (3) re-energizing software research and development; and (4) encouraging innovation within the U.S. software industry.

The DHS Software Assurance Program encourages the production, evaluation and acquisition of better quality and more secure software. Mr. Jarzombek discussed the

four areas that the programs resources target: people, processes, technology and acquisition.

Mr. Jarzombek noted that DHS had recently sponsored a Software Assurance Forum on March 16-17, 2006. The intent of the Forum was to bring together members of Government, industry, and academia with vested interests in software security to discuss and promulgate best practices and methodologies that promote integrity, security, and reliability in software. The next forum is being planned for October 2006.

Mr. Kris Britton of National Security Agency (NSA) was the next participant in the session. **[Ref #3]** Mr. Britton briefed the Board on the activities of NSA's Center for Assured Software (CAS). The Center was set up in November 2005 with a focal point for software assurance issues with the following objectives: partner with customers, government, the private sector and academia to identify software assurance issues and resolutions; to develop and utilize tools and methods to analyze the trustworthiness of software; evaluate mission critical components; and, establish/identify software standards and practices to increase the availability of assured software products. Their definition of software assurance is the level of confidence that software is free of exploitable vulnerabilities, either intentionally designed into the software or accidentally inserted and that the software functions in a manner as expected. The NII-sponsored Software Assurance Tiger Team identified two specific problem areas: (1) the ubiquity of software and its development and usage without consistent engineering, has resulted in ad hoc management and mitigation efforts in a race to protect systems against breaches, and, (2) there is two much software and too little assurance. Mr. Britton's presentation covered the DOD software assurance continuity of operations, domain of operation, measuring software assurance by acceptance, extraction/inspection, analysis, meta-analysis and reporting methods and identification of what CAS is working on at the present time. Mr. Britton welcomed NIST's taking a more active role in the software assurance program activity.

Board Member McNulty believes that the Board should be given a briefing on the National Science Foundation's Federal Cyber Service Scholarship Program activity to see if it is succeeding.

At this point in the meeting, Chairman Franklin Reeder joined the Board meeting. Mr. Reeder offered his congratulations to Mr. Chenok for his appointment as the incoming Chair of the Advisory Board.

Briefing on Real ID Project Activities

Mr. Jonathan Frenkel of the Department of Homeland Security (DHS) briefed the Board on DHS's responsibilities as a result of the Real ID Act of 2005. This bill was enacted as a result of the September 11, 2001, World Trade events to establish regulations for State's driver's license and identification documents to aid in the prevention of further terrorist assaults on the United States.

The DHS has the responsibility for developing the minimum issuance standards for such documents that require: (1) verification of presented information; (2) evidence that the applicant is lawfully present in the United States; and (3) issuance of temporary driver's licenses or identification cards to persons temporarily present that are valid only for their period of authorized stay (or for one year where the period of stay is indefinite).

Applicants must present proof of their lawful presence within the United States, proof of their principle residence and their originally issued Social Security card. The Social Security number is not required to appear on the license or ID documentation. There is also a requirement for mandatory checks of State database records to see if other driver's licenses have been issued in other States to the same applicant. Therefore, States will be required to share their driver license data electronically to allow access by a State to information contained in the motor vehicle databases of all other States. The advantages of using a federated distributed database approach are that there is no need for centralized databases to be created and the States don't have to do a lot to their existing data. The only requirements are that the State motor vehicle database must contain, minimally, all data fields printed on drivers' licenses and identification card issued by the State and the motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on licenses.

The Department of Homeland Security is meeting with the Chief Information Officers of the States to make certain that all issues are addressed.

Mr. Frenkel commented that the Department would be issuing a notice of proposed rulemaking in the Federal Register. His expectation is that OMB will allow a full 90 days for public comments. Also, a cost-benefit analysis needs to be done. They are consulting with the Department of Transportation and the States asking them to provide any cost projections figures that they can.

The question was raised about the scope of the Department's regulatory authority. Mr. Frenkel responded that there was nothing that could be done to compel a State to start moving toward compliance until a State wanted to. However, if a State should decide to hold out, and it is determined that DHS is right, then that particular State will be behind the compliance curve and this could be detrimental to its residents; for example, the ability to travel by air would be restricted.

The Statue called for the regulation to take effect on May 11, 2008.

The meeting was recessed at 5:15 p.m.

Wednesday, March 22, 2006

The meeting was reconvened at 8:40 a.m.

Board Discussion Period

The Board discussed the dates for the remainder of their 2006 meetings. The Board will meet on June 8-9, September 14-15 and December 7-8. If another half-day session is needed because of agenda specific actions, then the Board will convene the afternoon of the previous day of each two-day meeting session. Incoming Board Chairman, Dan Chenok stated that he would contact each member individually to gather their thoughts for the Board's agenda for the remainder of the year.

The Board discussed the NIAP program issue. Board member Chenok suggested that the Board might want to come up with the right answer for the use and kinds of programs that should be covered under NIAP. From that the Board could issue their

recommendation to OMB. One of the first topics to be suggested would be to conduct a cost benefit analysis of monies saved because of the evaluations performed on commercial-off-the-shelf products. Board member Lipner said that NIAP/Common Criteria evaluations do provide characterization of the software of products and suggested that not having NIAP in place is a missed opportunity to actually having some evaluation process that would tell customers something about the real software quality and future vulnerability. Mutual recognition is another important factor, especially to the vendors. Board member Hymes said that the Board could comment on the recommendations of the report once it is released. There is some concern that the report does not present a full dialogue with some of the key businesses and industries involved. The Board could recommend that this model be explored and recommend that the government open another stream of the NIAP program. It was suggested that the Board could take the action to produce a plan of action over the next three months as to what they might propose on this issue. Chairman Reeder suggested that the Board inform OMB that they are looking in this direction to address the many open questions that are out there.

Next, the Board reviewed the draft minutes of the December 2005 Board meeting. A motion was made by Board member McNulty and seconded by Board member Reis that the minutes of the December 2005 meeting be approved. The motion carried.

Suite B Cryptography

Ms. Elaine Barker of the NIST Computer Security Division briefed the Board on NIST's activities in Suite B Cryptography. **[Ref. #4]** NIST algorithms are not used for classified data. NIST and NSA got together and came up with a suite of coordinated standardized public algorithms to be used to protect both classified and unclassified national security systems and information. Suite B algorithms cover encryption, digital signature, key exchange and hashing. During her talk, Ms. Barker reviewed the comparable security strengths of all the involved algorithms and she discussed why AES-256 and ECC-384 were part of Suite B.

Board member Hymes mentioned a recent conversation he had with Bill Burr of NIST's Computer Security Division, to suggest that NIST produce a document describing the level of algorithms needed to achieve interoperability. Mr. Hymes said that a document such as this would be very beneficial to the community.

Briefing on Testing Laboratory Process for PIV Implementation

Ms. April Giles of the Office of Technology Strategy at the General Service Administration (GSA) briefed the board on GSA's FIPS 201 Evaluation Program. [**Ref. #5]** The purpose of this program is to determine if FIPS 201 product/service complies with mandated requirements and to establish an approved products/services list (APL) for use by agencies in the acquisition of FIPS 201 products/services. GSA is the designated executive agent for government-wide acquisitions of information technology. They report to OMB annually on the activities undertaken as an executive agent. To ensure government-wide interoperability, all departments and agencies must acquire products and services that are approved and compliant with the Standard and are included on the approved products lists. Ms. Giles stated that personal identity verification (PIV) cards and readers, both physical and logical, will need to adhere to GSA acquisition requirements and FIPS 201 normative requirements in order to support

interoperability. She also provided some examples of products/services that are not bound by specific FIPS 201 requirements; i.e., system integrators and computers. Ms. Giles reviewed the implementation timeline since the Office of Personnel Management authorized GSA to approve products/services in August of 2005. She also discussed the stages of development of the evaluation program and the vision of this program for the future.

OMB Update

Ms. Kim Johnson, Senior Policy Analyst in the Office of Information Security Policy at OMB briefed the Board on the FISMA annual report to Congress on the Federal government's security performance, the March 16, 2006, Oversight Hearing on the review of the 2005 Federal Computer Security Scorecards, and the ongoing activities of the OMB security line of business effort.

This year's FISMA annual report revealed that progress was made in several key security performance measures: certifying and accrediting systems, assigning a risk impact level, quality of certification and accreditation and quality of agency corrective plans of action and milestone process. GAO reviewed the report and identified areas of reporting that needed improvement. Testing of contingency plans, accuracy of major systems, and risk assessment were among those areas noted. The GAO offered OMB several recommendations for revising future FISMA instructions to obtain better results.

This year's FISMA report also included a questionnaire pertaining to privacy. While the results were not reported in the FISMA Annual Report, they were addressed in the FY05 Report to Congress on the Implementation of the E-Government Act of 2002.

Board member Chenok asked what OMB's position was on the NIAP report. Ms. Johnson replied that OMB had read the IDA NIAP report and reviewed the options presented by the report. OMB is meeting with NSC to discuss performance metrics. OMB believes that there is a need for expansion of good performance metrics that demonstrate the benefits and that these benefits are worth the cost. Ms. Johnson also acknowledged the report by GAO on the NIAP program.

The Computer Security Report Card for 2005 was issued on March 16, 2006. Seven of the 24 agencies received an "A" grade while eight received an "F" grade. Incident reporting was identified as one of the weak areas. Not all agencies are reporting their incidents. OMB will be addressing this issue later this summer. OMB uses the definition of what a system is as it is stated in NIST document Special Publication 800-30, Risk Management Guide for Information Technology Systems. Ms. Johnson indicated that the President's Management Agenda scorecard would continue to be used. OMB plans to meet with agencies that are not making the grade. Next's year's FISMA report will contain the same questions and will include an expanded FAQ section. One of the areas to be addressed in the FAQ section will be the emphasis on certification and accreditation.

Ms. Johnson reported on the activities of the OMB Interagency task force on information security line of business. The task force is focusing on training and knowledge sharing, incident response capabilities, program management and selection evaluation and implementation of security products. They are also working with DHS on the establishment of several Centers of Excellence. It is their goal to have the first two

centers in place by April 2007. One will be for security training and the other for FISMA training.

The Board offered NIST assistance with getting the word out about Certification and Accreditation process procedures versus other process procedures such as system life cycles. NIST Acting Division Chief Joan Hash said that she would relay this to ITL management and report back to the Board.

FISMA Reporting and Privacy Responsibilities Review

Board Members Hymes led a discussion on the review of the current privacy responsibilities/questions in the FISMA reporting questionnaire and the possibility of the Board identifying additional questions that they could forward to OMB for their consideration. It was noted that the language of the current questions relate to privacy compliance as opposed to Privacy Act regulation requirements. Two issues were identified: retention policy and OMB oversight over the agencies policies and procedures governing how they use personal information. Board member Chenok said that OMB would have to first issue guidance before dealing with the questions of retention. Also, Privacy Impact Assessments already cover some of the issues that the Board may want to raise. These assessments cover system-by-system operations while FISMA covers general operations overall. The Board needs to identify the issue they are trying to resolve. Should it be the question of does the set of reporting requirements that OMB imposes on the agencies give OMB good insight into the quality of agencies information privacy practices and create the right incentives to report the practices? The Board should also look at the larger question of how OMB gathers intelligence about how the agencies are doing. The Board will invite OMB's Privacy Officer, Eva KIeederman to attend the June meeting to discuss some of these concerns before taking a stronger position on this topic,

Board member McDonald said that she is working on the project to develop security and privacy profiles under the Federal Enterprise Architecture program. Under this effort, agencies are being asked to let them know if they do have a privacy program, how they are doing, and if they have developed plans to cover any gaps they encounter. Ms. McDonald agreed to present a briefing on the project to the Board at their June meeting. The Board also will plan a work session at the June meeting to obtain feedback from several agencies Chief Privacy Officers (CPO) to hear from them about how the CPO functions are doing, what is working well, what challenges remain, and how technology and security issues interrelate with their work. It was also suggested that the Board hear from a member of a privacy advocacy group as to whether or not the public has confidence in the government's privacy oversight.

Two additional topics that were identified were how OMB uses the feedback from the FISMA privacy responsibilities questions because a cross agency sharing strategy appears to be missing, and a concern for information collection of data outside of the reporting process given that the current process is a very audit driven mentality.

The Board will address this at their June meeting with plans to develop a recommendation to forward to OMB for their consideration.

Board Discussion

Board member Reis revisited earlier discussion on the Board's activities of the Federal Privacy Policy Review of the Privacy Act. Several options were suggested for conducting an open discussion of this issue. The Board could consider holding an all day meeting in September or December, perhaps outside of the Washington, D.C. area and extend invitations to identified speakers. Speakers would be asked to address a predetermined set of questions for strengthening the legal and policy framework of the Privacy Act.

The Board commented on DHS's presentation on the Real ID Project. The Board sees a security issue in this. To avoid security vulnerability the architecture has to be very clear so that there is no potential for misuse. The Board should consider more discussion on this topic to look at this issue from the different perspectives: State's Department of Motor Vehicles, users, and federal. Board members McNulty and Schmidt will furnish the members with documentation from the ITAA Identity Management committee. A suggestion was made to learn what concerns and constraints were placed on the U.S. Postal Service through the use of the E-passport initiative.

Public Participation

Ms. Brenda Abrams, IT Audit Manager, Office of the Inspector General, Information Audit Office of GSA, asked if the Board could recommend to OMB that they stress the importance of the need for agency security reviews to be on-going throughout the year, She also expressed her concern about acquisition issues and encouraged the Board to review this issue and offer OMB any recommendations that the Board might identify.

The meeting was recessed at 5:00 p.m.

Thursday, March 23, 2006

The chair re-convened the meeting at 8:40 a.m.

NIAP Program Briefing

Ms. Audrey Dale, Director of the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), briefed the Board on the activities of this program. **[Ref. #6]** There are currently 23 different nations participating in this common criteria arrangement. The governing policies of this effort are NSTISSP 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products that protect national security information by mandating that all these types of products be evaluated by CC, NIAP or FIPS beginning in July 2002; DoD Directive 8500.1, October 2002 which mandates compliance with NSTISSP 11, requiring products to be evaluated or in evaluation (with successful evaluation a condition of the purchase); and, DoD Instruction 8500.2, February 2003 which mandates products being evaluated also conform to a Government Protection Profile (whenever one exits). Ms. Dale's presentation covered an explanation of NIAP and CCEVS. She also presented a status of current product evaluations. There are 10

accredited testing laboratories plus four candidate labs. No additional labs will be accepted pending budget increases. Ms. Dale discussed the IDA draft NIAP report findings and the recommendations of GAO's audit report on NIAP. She also reviewed the actions being taken to improve the NIAP/CCEVS program.

IA Personnel Readiness: Training, Certification and Workforce Management

Mr. George Bieber, of the Department of Defense's Defense-wide Information Assurance Program briefed the Board on the current status of DOD's IA Personnel Readiness in Training, Certification and Workforce Management. **[Ref #7]** The vision of this effort is a professional, efficiently managed IA workforce with knowledge and skills to securely configure information technology, effectively employ tools, techniques and strategies to defeat adversaries, and proactively identify and mitigate the full spectrum of rapidly evolving threats and vulnerabilities in order to protect the network. Objectives of this program are to certify the workforce, manage the workforce, sustain the workforce and extend the discipline.

The Board may want to weigh in on the issue of professional credentials using the vehicle of the annual authorization legislation of the Department of Defense as a DOD. Authorization bill is passed every year. The Board could be helpful to DoD's IA program through the mechanism of DOD contacts and networks that already exist.

Board Discussion

The Board plans to continue their review of the reports issued on the NIAP program. They are also interested in following the impact of the Real ID project.

Board member Lipner shared some talking points he proposed regarding NIAP and Software Assurance.

- NIAP process does improve security feature quality and consistency.
- NIAP process may improve security (resistant to attack) of dedicated security IA products.
- NIAP process does not materially improve security of IA-enabled products.
- NIAP today is intimately tied to common criteria (CC).
- NIAP is the U.S. CC scheme and what it does is bound up in the CC today.
- Vendor perspective but tries to benefit the government.
- Having a program that achieves mutual recognition is of benefit to vendors and does drive vendors into CC probably beyond what we would have had in the Orange book.

The Board believes that it is not appropriate to suggest that the right conclusions have not been reached. The report needs to be reviewed before a more accurate statement can be made. The report did not ask the right questions; therefore, it is difficult to reach the right conclusions.

DHS has a software assurance initiative that is doing something. The NSA has a nascent software assurance initiative that has a vision but limited resources. The primary focus is on detection of hostile code. NSA's vision encompasses a potential

way forward for product evaluations. However, hard issues of mutual recognition have not yet been addressed.

Board member Reeder offered the suggestion NSA's vision is much broader and robust as contrasted to the CC schemes products and security figures. This creates challenges given the current mutual agreements. They are not value statements.

Possible Board conclusions/recommendations could developed from the following thoughts/actions:

- It is premature to mandate CC evaluation for non-National security applications.
- CC and, thus, NIAP should continue until replaced.
- The DHS initiative should articulate clear goals and approach.
- NSA software assurance initiative should be monitored to see if it develops a viable approach to product evaluation.
- Transition to a new evaluation model will be difficult and must preserve mutual recognition.

The Board would like to see NIST involvement in the early stages should this activity go on to encompass the civilian sector.

Other Board members responded with their opinions of the NIAP issue.

Board member McNulty noted that NIAP is a program on life-support. It would be difficult to imagine that the Government would extend the program to the civilian agencies without the resources available to make it successful. However, the Government could continue to execute the current program successfully enough to keep their commitments to the national security committee and than find out what is happening to develop a transition strategy that includes mutual recognition. Mr. McNulty believes that a mandate to the non-national security agencies seems highly unlikely.

Board member Leng' expressed her concern in the ability to define the Board's actual charge with regards to this issue and how to state the Board's recommendations on the current and proposed options of NIAP/CC to the non-classified civilian agencies. She believes that the Board would do well to think more about this issue from the civilian agency, senior management official point of view.

Board Member Reeder's observation was that the Board hasn't heard enough to come to a specific conclusion. Each member was asked to review the NIAP report and GAO report, especially the conclusions and recommendations. Board members Lipner, Hymes and McNulty were tasked to work on producing a draft letter that could be used to educate the civilian agencies on what the NIAP program is all about. The letter could begin with a statement of the objective as to how to help the civilian departments and agencies and recommend changes to strengthen and encourage additional funding. The letter could include a statement to the Director of OMB, the Secretary of Commerce and the Director of NSA about the Board's concern for the health of the National Common Criteria plan. It could also point out that the NIAP report does not reflect the answers to the right questions. It could be stressed that it would be beneficial if those questions could be clarified in a language that would be understood by the managers.

The Board could raise awareness of the underlying issues of the program and explore and clearly articulate the questions and the need for these requirements across agencies.

After further discussion, it was the consensus of the Board that they are not ready to take a position at this meeting. However, they will review the NIAP and GAO report and the previously identified group of members will work on the developing a position based on the Board's views as discussed earlier. This will be an agenda item for the meeting in June. It was also suggested that the group members might want to get in touch with the Congressional office that sponsored the NIAP program activity to obtain additional input.

Before the meeting was adjourned, outgoing Chairman Reeder expressed his thanks and gratitude to the Board for the dedication and expertise that they had brought to the Board during his tenure as Chair. He said that he was honored to have served with such distinguished and knowledgeable individuals and extended his sincerest best wishes for their continued success in all of the endeavors and the activities of the Advisory Board. Mr. Reeder also extended his thanks and appreciation to the NIST Secretariat staff for their exemplary support of the Board and for helping make his job as Chairman a lighter one.

There being no further business, the meeting was adjourned at 12:30 p.m.

Ref. 1 – Anderson Presentation
Ref. 2 – Jarzombek Presentation
Ref. 3 – Britton Presentation
Ref. 4 – Barker Presentation
Ref. 5 – Giles Presentation
Ref. 6 – Dale Presentation
Ref. 7 – Bieber Presentation

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

Daniel Chenok
Board Chairman