Minutes of the Computer System Security and Privacy Advisory Board Meeting

March 16-18, 1999
National Institute of Standards and Technology
Gaithersburg, MD

Tuesday, March 16, 1999

Chairman Willis Ware called the meeting to order at 9:15 a.m. In addition to the Chairman, those members present were: John Davis, Joe Leo, John Sabo, George Trubow, and Rick Weingarten. Gloria Parker attended on March 17 and 18, 1999.

Ed Roback, Board Secretariat, introduced Karen Worstell, Board nominee, who was in attendance. Ms. Worstell is Director of Research and Technology, International Information Integrity Institute (I4) and Principal Consultant for SRI Consulting in Houston, Texas.

Mr. Roback reviewed the meeting agenda and associated handout material. As with all Board meetings, all sessions were open to the public. At the start of the meeting there were five members of the public in attendance.

NIST Computer Security Division Update

Mr. Miles Smid
Chief, Computer Security Division
Information Technology Laboratory, NIST

Mr. Miles Smid discussed the NIST Computer Security Division's program mission and security program strategy **[Ref. #1]**. He said that the Division gets involved when needed standards don't exist, when measurement and testing will make a difference, when government imprimatur is needed, when government is needed in an international role or when the government has its own unique need. NIST has unique resources and expertise and serves as an 'honest broker." Since taking the position in January 1999, Mr. Smid has reorganized the division staff into six different program areas under two pre-existing groups. Each program area has its own goals, technical areas, collaborators, impacts and major projects. Mr. Smid concluded his remarks by saying that NIST is improving the security of commercial products and systems by providing computer security leadership in both federal government and industry; by promoting development and implementation of key security standards and tests for protection of critical national infrastructure systems and by promoting technology transfer to government and industry.

Chairman Ware asked if Mr. Smid felt that the posture and national reputation of NIST's computer security effort is being maintained. Dr. Ware expressed his concern that the NIST staff numbers are not ramping up to meet the needs of today. In response, Mr. Smid agreed that staff has changed over time, but that the recent program units that he has established are a method of grooming upcoming senior management. Another opinion expressed by Board Member Joe Leo was there was not a Senior Executive Service (SES) position for the Chief of the Computer Security Division. The Board was also interested in whether or not the Division was going to be receiving any critical infrastructure protection plan monies and if not, why not. The Board may want to take a look at why computer security efforts at NIST have not gotten more funding.

NIST Cross-Industry Working Group Activities

Mr. Jerry Linn
Associate Director
Information Technology Laboratory, NIST

Mr. Linn briefed the Board on the role of NIST in the Cross-Industry Working Team (XIWT) effort **[Ref. #2]**. The XIWT was chartered to promote and accelerate world-class National Information Infrastructure and interoperability of applications across traditional industry boundaries. It serves as an open forum for dialogue among stakeholder communities in the private and public sectors and fosters cooperative exchange of ideas, interests and information. The membership of the XIWT is comprised of five different sectors. NIST is involved because industry is their client. Their participation allows them to discuss issues, interact with and listen to R&D executives and directors, to understand and synthesize a cross industry perspective and to assess where industry thinks IT is going. The XIWT holds an annual meeting in the Washington, DC area to bring together the federal agencies and Congress to develop policy decisions. They have issued eight white papers since 1994. They can be found at the XIWT website <www.xiwt.org/documents/documents.html>. Board member, Rick Weingarten, pointed out that security was not at the top of the XIWT list of focus areas.

Mr. Linn distributed copies **[Ref. #3]** of a 1998 XIWT report entitled "Customer View of Internet Service Performance: Measurement Methodology and Metrics" to the Board members.

OMB Guidance to Implement the Government Paperwork Elimination Act (GPEA) Access America -- Fulfilling the Vision of Electronic Service Delivery

Peter Weiss
Office of Information Policy and Technology
Office of Management and Budget

Mr. Weiss briefed the Board on the current OMB guidance to implement the Government Paperwork Elimination Act **[Ref. #4]**. Following in the theme of Vice President Al Gore's *Access America* project pertaining to the transfer of sensitive information electronically between government and privacy industry and individuals, and among governments, the GPEA calls for agencies to automate interactions with outside partners/customers within five years to the extent practicable; for OMB, in consultation with Commerce and others to promulgate policies and procedures within 18 months, and these established procedures are to encourage both electronic filing and electronic recordkeeping, particularly by employers. Other applicable laws include the Paperwork Reduction Act, the Government Performance and Results Act and the Clinger-Cohen Act (Information Technology Management Act of 1996). Putting these all together should lead to the reduction of the burden to the public and provide customer service in a fundamentally better way. However, electronic forms are not, by themselves, necessarily enough Weiss pointed out. OMB has issued a Federal Register notice (64 Fed. Reg. 10896 dated Friday, March 5, 1999) requesting comments by July 5, 1999, on their implementing guidance. Mr. Weiss reviewed the GPEA's definition of electronic signature and the legal effect and validity of it as it pertains to electronic records. He also reviewed factors to be considered in planning electronic systems covering the nature of the participants to the transaction, the type of transaction and the recordkeeping needs regarding the transaction.

Next, Mr. Weiss spoke on the subject of privacy in electronic commerce. He described the basic principles of privacy and disclosure and stated that information collected will be managed consistent with the Privacy Act, Computer Security Act and any other applicable laws. Practical implications and good practices would indicate that there be collections only if needed, that conditions and limits of use be disclosed, that reasonable personal access with ability to correct and/or update be provided; that protective policies and measures be articulated and disclosed and that personal information be destroyed when no longer needed and that appropriate retention periods be determined.

Mr. Weiss stated that designing an automated system with better authentication and privacy than paper-based systems is not difficult. But, the user, oversight, and advocacy communities as being better must perceive it. A good example of this is the Social Security Administration's Personal Earnings and Benefits Estimate Statements (PEBES) on-line program. He said that Federal managers should keep the Privacy Act and Computer Security Act in mind when dealing with the paperwork elimination effort. The GPEA should not be construed as a 'cookbook' but a 'green light' guidance document.

Mr. Weiss welcomed the Board's comments as a group or on an individual basis and reminded them of the July 5, 1999, deadline for submission of any comments.

Federal Computer Incident Response Capability (FedCIRC) Activities Update

Judith Spencer
FedCIRC Management Center
General Services Administration (GSA)

Ms. Spencer provided an update on the activities of the Federal Computer Incident Response Capability (FedCIRC) **[Ref. #5]**. She reported on the collaborative effort of working with advisory groups, partners and participating agencies. Currently, there are 72 agency points of contact, seven agencies have signed Letters of Agreement and briefings have been provided to numerous conferences and exhibit booths. There is an extensive website at <www.fedcirc.gov> which has been averaging 2000 hits per month. Ms. Spencer discussed the trends in incidents as they have been reported by CERT between 1988-1998. The nature of the trends has changed over the years. In 1988 passwords and known vulnerabilities were exploited. However, today exploiting of just about everything is found. Also, today's definition of "an incident" is that time when any one comes against us with a known hacker tool, whether successful or not.

Ms. Spencer said that continuing initiatives include the Federal certification for IT security professionals' curriculum, expansion of the partners group, more user forums and workshops and continued outreach efforts. GSA has furnished the funding for this year's program. It is expected that in the near future funding will be a line item in the budget. The Board indicated that it is willing to support the GSA effort in the funding development effort.

National Infrastructure Protection Center Briefing
Partnership for Protection

Douglas Perritt
National Infrastructure Protection Center
Federal Bureau of Investigation

Mr. Doug Perritt provided a briefing on the status, capabilities and direction of the National Infrastructure Protection Center (NIPC)**[Ref. #6]**. The definition of critical infrastructures is services so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. Adversaries come in different forms and intrusions can be strategic attacks or unstructured incidents. The decision-maker has to answer several questions to make the determination of what kind of intrusion is taking place. The intelligence and law enforcement community, CERTs, systems administrators, infrastructure owners and operators all can contribute to finding out the answers. Though there are many challenges, solutions can be found with government partnering with the private sector and involvement by many government agencies. Also a clear understanding of the role of law enforcement is necessary. Don't focus on arrests but rather focus on their authorities to get answers to the critical questions.

Mr. Perritt reviewed the goals of the Presidential Decision Directive 63 and its establishment of the NIPC. The mission of the NIPC is to provide a national focal point for gathering information on threats to the infrastructures. It will provide the principal means of facilitating and coordinating the Federal government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. It is composed of multiple government agencies, Federal, state and local law enforcement and private sector representatives. Currently it has a staff of approximately 100 representatives from the FBI and other government agencies. On the international side, the NIPC has entered into investigative cooperation with G8 and the Council of Europe. It also has participated in State-led efforts to define international cooperative efforts.

Mr. Perritt also described InfraGard, Federal Computer System Intrusion Detection Network (FIDNET), ISAC, and Y2K preparations. In closing, he said that the NIPC is open to ideas and suggestions and encouraged the CSSPAB to share any thoughts and observations that they might have.

Public Participation Period

The Chairman called for any public participation. There were no requests for public comment so the meeting continued onto its next topic.

Critical Infrastructure Protection: Toward an Effective R&D Agenda

Mr. John C. Davis, NSA representative
Critical Infrastructure Protection R&D
Interagency Working Group (IWG)

Mr. Davis updated the Board on the working group's current activities **[Ref. #7]**. The President's Commission on Critical Infrastructure Protection has recommended a $4.75 billion investment from FY98-FY04 in six technology areas. The IWG has identified 71 programs in six of the infrastructure categories. They developed R&D options for FY2000. Option 1 included the banking and finances sector, the information and communications sector and the energy sector. Option 2 included the transportation sector, vital human services sector and interdependencies. These options carried no fiscal constraints and offered no guarantees that any, much less all, would survive the FY2000 Federal budget process. Mr. Davis described the IWG's focus plans from February - June 1999. The FY2001 CIP R&D budget process will rely heavily on the outcome of the FY2000 review. Management challenges he cited included:

- ensuring proper R&D coordination among government agencies
- keeping up with rapid march of technology
- coordinating with state and local governments

- managing a program of this magnitude
- international dimension of critical infrastructure protection
- developing a close, cooperative partnership with industry.

The IWG recognizes that partnership and cooperation with industry and academia are the key elements to the success of this R&D program. Mr. Davis said that they would welcome any feedback from the Board on how to best foster this partnership, what type of partnership makes most sense and whether or not they are going in the right direction with their R&D agenda.

AES Activities Update

Ed Roback
Computer Security Division, NIST

Mr. Roback gave the Board an update on the activities of the Advanced Encryption Standard (AES) **[Ref. #8]**. The first issue he discussed was the revision of FIPS 186-1, the Digital Signature Standard (DSS). A Federal Register notice was published in December 1998 announcing this FIPS as an interim final standard. Comments were invited from the public, academic and research communities, manufacturers, voluntary standards organizations and Federal, state and local government organizations. Based on the comments that were received, NIST modified the interim final standard. NIST expects to issue FIPS 186-2 as soon as it completes the approval process and is signed by the Secretary of Commerce.

The next topic Mr. Roback discussed was the results from Round 1 of the Advanced Encryption Standard effort. He explained the NIST efficiency testing and random testing processes of the 15 Round 1 AES candidates and the surveys and comparisons used to accomplish this. NIST plans for testing for Round 2 will focus on efficiency testing on larger key sizes. Tests will be done on C code on 64-bit processors using compilers that generate 64-bit applications and, they may also test assembly language implementations.

The March 22, 1999, AES2 conference will be held in Rome, Italy. They expect approximately 180 attendees with 23 countries represented. Twenty-one papers will be presented. The goals of the conference are to present the analysis of Round 1, to discuss relevant issues and to provide NIST with a clearer understanding of which candidate algorithms should and should not qualify for Round 2. Main issues to be addressed include security, efficiency and flexibility.
Mr. Roback will brief the Board on the results of this conference at the June meeting.

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

Wednesday, March 17, 1999

The meeting was reconvened at 9:00 a.m.

New Directions Briefing

Michael J. Jacobs, Deputy Director
Information Systems Security, NSA

Mr. Jacobs briefed the Board on the mission of the recently restructured Information Systems Security Organization (ISSO) at the NSA. As a result of world changes in the 1980s the traditional role of the ISSO had to progress to keep up with the pace of customer needs. The networking environment has brought about a new threat called cyber attacks. DOD systems and networks have been actively exploited. The threat to the National Information Infrastructure is real and growing. The Internet has made it easy by identifying the potential vulnerabilities and posting the tools that would be needed to exploit these vulnerabilities. Both NSA and NIST must engage industry to partnership with them to develop programs that will assure a higher level of products coming from the commercial sector. Mr. Jacobs outlined National Information Assurance strategy components such as cyber security awareness, strong cryptography such as digital signature and encryption, global security management infrastructure, defense infrastructure made up of a national attack sensing and warning capability and a coordinated response mechanism. These components should be coupled with enabling legislation and international agreements.

Next, Mr. Jacobs described the NSA model for enhancing information assurance. There are three basic elements: increased protection against cyber attack; the ability to detect an attack as it is occurring and the capability to respond and/or recover when an attack is detected. Implementation of this model requires the use of commercial and government-developed products in a manner where the solution adequately mitigates the risk without being too costly to implement and use. The National Information Assurance Program (NIAP), the NIST/NSA joint initiative to meet security testing needs of both information technology producers and users, has received positive feedback. The Trust Technology Assessment Program (TTAP) is a NSA program that supports NIAP functions. To date, four products have completed the NIAP/TTAP process. Mr. Jacobs acknowledged that one of the current difficulties is that there are no constraints on what a government agency can purchase. They are not bound by the use of any Evaluated Products Lists (EPL). He would like to see that change and is working on drafting a recommended policy. The relationship between NIST and NSA has been strengthened considerably over the last five to ten years. Mr. Jacob believes that the NIAP program has been the linchpin to this success.

On the subject of the Advanced Encryption Standards (AES), NSA has been assisting NIST in the AES selection effort by contributing NSA personnel effort to review the candidate algorithms. Mr. Jacobs believes that once the new AES standard is in place there will be rapid movement to it. It is expected that the AES process will produce a truly strong algorithm. In that event, the ISSO intends to use COTS products incorporating AES (with the proper assurance) and to produce GOTS products for use in unclassified and classified applications, especially when interoperability is an issue.

Privacy Panel

Ari Schwartz, Center for Democracy and Technology
Solveig Singleton, Cato Institute
Maya Bernstein, Office of Management and Budget

Ari Schwartz of the Center for Democracy and Technology, Solveig Singleton of the Cato Institute and Maya Bernstein of the Office of Management Budget were invited to brief the Board on the protection of individual privacy in systems owned or operated by the government. Mr. Schwartz directed his comments toward the changes in the traditional role that the government had played in the past and how the proposed Government Paperwork Elimination Act is bringing the computer era into this role. In the past the government has been the 'identification' creator. However, with this new computer age, people have more systems available to them and this creates the need for better privacy and security authentication. Privacy has to be thought of as a basic concern. He offered as an example the INTEL process serial number. Security could be compromised if the government purchased software the required a single identity computer user. Mr. Schwartz felt that there are broader options available and that they should be considered.

Solveig Singleton Director of Information Studies at the Cato Institute presented her observations on privacy issues in Federal systems **[Ref. #9]**. She addressed the danger to human rights from Federal information systems and the security concerns such as identity theft, as distinct from privacy concerns. In the past, Federal agencies and employees have used information stored in federal systems to carry on personal or political vendettas or violations of rights on a grander scale. She mentioned several examples of this. As a result of the growth of centralized information databases, identity theft has become a serious problem that is yet distinct from concerns about privacy related to human rights. Ms. Singleton pointed to the use of a social security number as a password as the wrong kind of database information that is frequently improperly used. She believes that if Federal systems are to be more secure against identity theft and other security breaches, then better passwords need to be used. These may include true passwords, like PIN numbers, that can be changed from time to time; digital signatures, the use of biometrics data like a voice print or fingerprint, and the use of encryption. She expressed her reservations about whether legislation is called for to establish Federal procedures for accepting and using digital signatures. A premature Federal standard could become a tool of unrelated policy goals, doom Federal systems to become obsolete and cut off competition among competing signature models.

Next, Ms. Singleton focused on the issue of privacy as a fence against violations of human rights. She said that the more ambitious regulatory programs and agendas that are adopted by the Federal government, the more likely the agencies that administer them are to begin to demand vast amounts of information from U.S. citizens about their personal lives. She described several examples of how some government programs have done exactly that. The U.S. Constitution created and has abandoned a government of narrowly defined and enumerated powers. It is her opinion that a return to the limited government model would be the best defense against dangers to privacy and attendant dangers to human rights. She also believes that more attention should be paid to taking the Fourth Amendment seriously which limits the means by which personal information can be collected and holds information collectors accountable to the judiciary.

Maya Bernstein, Office of Information and Regulatory Affairs from the Office of Management and Budget was next to present her views. She said that OMB Director Jacob J. Lew had announced the appointment of Mr. Peter Swire to serve as the Chief Counselor for Privacy for the Administration. His responsibilities will be to coordinate the Federal government's privacy issues. The types of government databases that exist today cover such areas as child support enforcement, gun regulations (Brady Bill), and compensation for those incarcerated. These databases are operated under tight control and some have been created explicitly by legal statute. Ms. Bernstein pointed out that a problem that often arises with these types of databases is the temptation to use them for additional purposes as they have already been established.

Discussion with the Board and the panelists followed their presentations. Some general observations were that there is much debate on where privacy issues are covered within the government and there is no guarantee that even if there were to be privacy advocacy strongly in place in the government, there would be the win of efficiency over policy issue decisions. Another suggestion was to amend the Privacy Act to give the Courts more clout in this area.

Privacy "White Paper" Discussion

Professor George Trubow
Board Member

Professor Trubow briefed the Board members on his privacy "white paper" entitled Watching the Watchers: The Coordination of Federal Privacy Policy **[Ref. #10]**. This paper proposes that Congress establish an independent agency charged with the responsibility to protect Federal information privacy. It outlines how this agency might be structured. It also carries with it the strong suggestion that State governments and the private sector should also be implementing proper privacy policy.

In addition to the "white paper" discussion, Professor Trubow also presented an outline on the expanding use of criminal history records since the enactment of the Crime Control Act of 1973. Several observations that he pointed out were that those who are clean stay clean and those that have been soiled can't get clean. There is no mechanism in place for backing out incomplete data and the assumption has always been that all data is accurate and complete.

Board Discussion Period

Following Professor Trubow's brief, the Board continued to discuss the role of privacy in government. A major issue yet to be resolved is whether or not the Office of Management and Budget is the proper place for privacy. Some possible alternatives were identified such as the Justice Department or the National Archives and Records Administration. It was pointed out that going with an entity that was already in place is both cost effective and saves time, especially in light of the current wave of downsizing the Federal government, in general. Another suggestion made was to consider the establishment of a public advocacy role. However, it would most likely be more difficult to determine where such a position should be housed within the Federal government. A possible answer could be to house the public advocacy role within the Consumer Product Safety Commission.

It was suggested that the Board could prepare an issue paper on the privacy topic and make it available to the public. The Board will invite Mr. Peter Swire to the next meeting. They will also endeavor to arrange for a briefing on the status of the introduction of new legislation to revise the Computer Security Act of 1987.

The minutes of the March 1999 meeting were presented and unanimously approved.

The comment period for the Federal Register notice regarding the Government Paperwork Elimination Act closes on July 5, 1999. If the Board would like to develop a collective response they should come prepared to the June meeting to develop a point paper of comments to be submitted.

Next, the Board members considered topics for future meetings. Also, there was discussion on how this Board could assist the NIPC efforts and NSA's collaborative effort with the civilian and private sector. This topic will continue to be kept high on the priority list throughout the year. The Board would also like to commend NSA's current work effort direction, and the Chairman was directed to draft a commendation letter to that effect. Professor Trubow suggested that the Board contact John Koskinen, the Administration's Y2K czar, to inquire what Y2K funds can be used for the critical infrastructure protection (CIP) effort. It was also noted that it would be useful if there is documentation of any types of incidents that may occur on January 1, 2000. The

Board Chairman indicated that he would get in contact with Ed Springer at OMB and discuss this recommendation with him.

The meeting was recessed at 5:10 p.m.

Thursday, March 19, 1999

NIST/IT CIP Effort

Paul Domich
Acting Deputy Director
Information Technology Laboratory, NIST

Mr. Paul Domich, Acting Deputy Director of the Information Technology Laboratory (ITL) presented a briefing on NIST Critical Infrastructure Protection effort and initiatives **[Ref. #11]**. Three areas of NIST will be involved in this effort. In addition to ITL, the Manufacturing Engineering Laboratory and the Building and Fire Research Laboratory will be involved. Within ITL, three divisions will be involved. An information sharing and analysis center (ISAC) will be created. The functions of the ISAC are to collect, analyze and disseminate vulnerability assessments and individual event reports, to ensure confidentiality of proprietary information, to conduct aggregate analysis of patterns and trends, to make *Best Practice* determination/ dissemination and to support crisis management. Mr. Domich believes that for the ISAC to be successful there must be a private sector office that is industry driven and that there must be a private industry/government partnership. In addition to the in-house expertise that NIST offers, it is also recognized as having a reputation as a Trusted Agent. He explained the various roles of each of the divisions in the Laboratory that would be supporting this activity. NIST critical infrastructure protection initiatives are in five areas: security technology, systems survivability, high assurance systems, application of domain-specific expertise and security for Federal systems. Mr. Domich said that they are an extension of our current program. Additional funding has been requested for these initiatives, and it is anticipated that the funding would triple if they were selected.

National Information Assurance Partnership (NIAP) Briefing

Ron Ross
Computer Security Division, ITL

Dr. Ron Ross, Computer Security Division, ITL, presented an overview and conceptual framework of the Common Criteria Evaluation and Validation Scheme **[Ref #12]**. Today's climate reflects the need for greater IT assurance within critical infrastructures in both the public and private sectors. Security requirements need to be defined and conformance needs to be demonstrated. NIST and NSA have established a program under NIAP to evaluate conformance of IT products to help consumers make informed choices when selecting commercial off-the-shelf products in the area of IT security and to help producers of IT security products gain acceptance in the global marketplace. Key participants include product developers, integrators, government agencies, industry consortia and private sector organizations. The Common Criteria Testing Laboratories (CCTLs) and the NIAP validation body are included in this group of participants. Dr. Ross described the concept of operation and the resulting Common Criteria Certificates process. The Common Criteria Mutual Recognition Arrangement provides recognition of Common Criteria certificates by signatories to the Arrangement. It creates virtual single validated products lists for organizations participating in the Arrangement. It eliminates the need for security evaluations in more than one country and provides excellent market opportunities for U.S. developers of IT products. He summarized his presentation by saying that the NIAP Common Criteria Scheme (1) promotes the development of a private sector security testing industry in the U.S., (2) increases availability of evaluated IT products for use by government and private sector consumers; (3) decreases the need for multiple evaluations, and (4) provides IT product developers with the opportunity to sell evaluated products in worldwide markets.

Board Discussion of Agenda topics for June Meeting

The Board identified the following as possible future action items:

- Sponsor a one-day session on significant national and governmental issues on emerging computer security awareness efforts;
- Send out meeting agendas to the CIO community at large, not just the Security Committee of the CIO Council.
- Invite Rich Guida, Chairman of the Government Information Technology Services Security Committee to address the Board on the topic of PKI and the status of the Bridge CA effort.

Chairman Ware presented a certificate of appreciation to Board member, Joseph Leo, Department of Agriculture, who's term expires on the Board as of April 11. Board member, Gloria Parker, Department of Housing and Urban Development, announced that this would be her last meeting. She will not be present at the June meeting because of a scheduling conflict and her appointed term expires in July. Dr. Ware expressed his thanks and gratitude to both outgoing members for their service and dedication to the CSSPAB.

It was also noted that a total of five of the current Board members' appointments will be expiring within this next year and three members were just newly appointed to the Board, thus producing a membership of eight new members within one year. In order to realign these appointments cycles to minimize a large turnover, the possibility of extending some appointments was discussed.

There being no further business, the meeting was adjourned at 11:45 a.m.

/S/

Edward Roback
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting

/S/

Willis H. Ware, Chairman

References:

#1. Smid presentation
#2. Linn presentation
#3. "Customer View of Internet Service Performance: Measurement Methodology and Metrics, October 1998 by Cross Industry Working Team.
#4. Weiss presentation
#5. GSA presentation
#6. Perritt presentation
#7. Davis presentation
#8. Roback presentation
#9. Singleton presentation
#10. "Watching the Watchers: The Coordination of Federal Privacy Policy"
#11. Domich presentation
#12. Ross presentation