Information Security and Privacy Advisory Board (ISPAB)
Minutes of Meeting

July 13, 14, 15, 2011

Homewood Suites by Hilton D.C., 1475 Massachusetts Avenue, NW, Washington, DC 20005

	Present:	
	Board Members	Non-Board members
Wednesday, July 13, 2011 8:40 A.M. – 4:47 P.M. Thursday, July 14, 2011 8:30 A.M. – 5:30 P.M. Friday, July 15, 2010 8:10 A.M. – 12:18 P.M. Presentations http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/July-2011.html	Dan Chenok (Chair) Julie Boughn Brian Gouker Joe Guirreri Ed Roback Phyllis Schneck Fred Schneider Gale Stone Matthew Thomlinson Peter Weinberger	Donna Dodson Cita M. Furlani Matthew Scholl (DFO) Annie Sokol (DFO) See Annex A for record of presenters and visitors

Wednesday July 13, 2011

The meeting was called to order at 8:18 A.M. Gale Stone joined the meeting via teleconference. The Chair began the meeting with the review of the agenda items. The board members provided updates of their recent activities. Phyllis Schneck briefly described the development since Intel bought McAfee. Gale Stone expressed her concerns on how reorganization at SSA may impact governance and cybersecurity, and with imminent budget cuts the agency may be allowing more services on the web without the necessary security precautions. Brian Gouker had started his new assignment as a professor. Fred Schneider will be presenting his final update as this will be his last ISPAB meeting.

NIST Update (Presentation provided)[1]

Donna Dodson, Division Chief, Computer Security Division, NIST
Matt Scholl, Deputy Division Chief, Computer Security Division, NIST

Donna Dodson updated the board on current activities in Computer Security Division (CSD), NIST. The new reorganization for CSD has five new groups: Cryptographic Technology, Security Components and Mechanisms, Secure Systems and Application, Security Outreach and Integration, and Security Test, Validation and Measurement. She explained the functions of each group. She will distribute the mission statement and conceptual plan to the board for their comments. Matt Scholl is temporarily acting as Group Manager until the position is filled. Donna Dodson highlighted a number of draft publications that are open for comments and finalized publications including the 2010 CSD Annual Report has also been issued. She also discussed the status of key programs, initiatives, and a number of upcoming events.

[1] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/Jul13_NIST-updates.pdf

<u>Cloud Security and Privacy</u> (Presentations[2] [3]provided by moderator)
Earl Crane, Director of Cybersecurity Strategy, OCIO, DHS (Moderator)
David Mihalchik, Head of Google Apps, Federal Google
Laura Posey, Senior Security Strategist, Trustworthy Computing, Microsoft
Jim Reavis, Co-Founder and Executive Director, Cloud Security Alliance, and President of Reavis Consulting Group, LLC

Dan Chenok introduced the panel members. He added that there had been a lot of movement in the federal space with Cloud since the last time Earl Crane has spoken to the board.

Earl Crane as the moderator of the panel started the discussion. He participates in Information Security and Identity Management Committee (ISIMC) that helps to define the scope within the CIO Council. The CIO Council had produced a document, *Guidelines for Secure Use of Cloud Computing by Federal Departments and Agencies*. This document will not be released until FedRAMP is official. The framework as described in the document integrates with different programs and addresses different functions. There are six different use cases in this framework. The Federal Cloud Security Top 20 captures fair portions of concerns.

Jim Reavis, CSA, explained his role in the sub-committee, CSA, and his focus on trusted ecosystem. It is challenging to have a complete virtual environment and then to think of how to implement controls. There must be some levels of physical security, design with complete virtual concept, with more robust cryptography and hardware layer. One cannot ignore supply chain issues concerns. He discussed the importance of implementing controls and physical security, and design vs. implementation. It is necessary to design things with a virtual concept, and therefore, resulting in forming trusted systems. Cloud is a new business model with virtualization as an old technology. The issues and concerns with supply chain are part of the big challenge with today's cloud definition.

Laura Posey, Microsoft's Trustworthy Computing group, asserted that they have an incident response team. She emphasized the need for a strong partnership between cloud service providers and federal agencies. The Federal Cloud Security Top 20 is applicable to both private and public cloud.

David Mihalchik, Google, discussed the development of cloud. It is critical to note that if existing systems are not secured cloud cannot be secured on the existing systems. There are concerns on the classification of public and private clouds. A private cloud is not more secure than a public cloud. Moving forward, cloud can be customized in many ways, and public cloud is looking more and more like any private clouds. Any organizations considering cloud should not hesitate because of security concerns. Government agencies should begin to embed in commercial products and services, and most importantly, should move quickly to embrace the cloud. The decision process should be driven by innovation while recognizing security priority. It is noted that public cloud has as much possibilities of failing as private cloud. When focusing on cost, it is important to focus on the model as it cost increases for additional security controls. Continuing monitoring is still critical for any system.

[2] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/Jul13_Cloud-ISIMC-Cloud-Security-ISPAB.pdf
[3] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/Jul13_Cloud-Coordinating-Draft-Guidelines-Secure-Use-Cloud-Computing.pdf

Current Status of the Cyber Legislative Process

Matt Grote, Senate Committee on Homeland Security and Governmental Affairs
Denise Zheng, Senate Committee on Homeland Security and Governmental Affairs

Matt Grote and Denise Zheng are staffers for Senator Lieberman and Senator Collins. Denise Zheng worked as a program manager for CSIS commission prior to her present role as the Cyber Security Lead. Matt Grote replaced Adam Sedwick with his work in GAO with Senator Lieberman.

Matt Grote and Denise Zheng stressed that they are strictly presenting their own opinions and do not represent the views of the senate or their senators. Denise Zheng explained the history of cyber security legislation. She also explained the main elements of the cyber bill reintroduced by Senator Collins this year. It included three different goals: secure Federal government; Critical Infrastructure; and Private Sector. The starting point was to identify actual systems and based risks on the requirements. Facilities with critical structure are to decide on the standards and define response time. DHS had provided some inputs to OMB's process. The bill will provide limited liability protection. There are 7-8 committees with focuses such as cybersecurity, commerce, and judiciary. The performance standards included supply chain risk management, and with broad, high level requirements. The key is to have strong private sector communications, and DHS is evaluating risk assessment with private providers. With a proper legal framework in place, it will be easy and efficient to communicate in the event of an attack or emergency.

In general, companies should be responsible for protecting their systems based on their own risk assessment. But many companies would prefer to work with software without any needs for patching so as they could negate liabilities. Matt Grote and Denise Zheng did not receive any assurance from companies on the reliability and security of software. While it is generally known that semi conductors are seldom made in the US, even if we could have everything manufactured in the US there are other areas of risks, such as the number of foreign hires in the US. The proposal that was delivered by the White House in May has many similar issues. Denise proposed to establish a series of working groups. Presently, the leadership level is working on the next steps.

Matt also touched on the FISMA Reform, and that nothing has been passed since the president took office. The focuses are on formalizing the move from OMB to DHS, Continuous Monitoring and SCAP.

International Standards and Cybersecurity

Chris Painter, Coordinator for Cyber Issues, Office of the Secretary, US Department of State

Chris Painter has previously been invited to the board prior to his new role as the Global Cyber Ambassador at the US State Department. He stated that the State Department is working hard to create a national strategy that would have key impact on technology for the next twenty years. The framework of the national strategy that has been worked on for the past 18 months is layout not only for inter-agencies but also for the rest of the country. It is interoperable and it supports international commerce. There are many principles laid out in the new strategy (*International Strategy For Cyberspace*)[4] that was launched in May. The strategy dealt on a number of policy priorities; Law Enforcement; Internet Freedom, and build consensus of cyberspace. In order to achieve a common goal, it is necessary to engage everyone. He held dialogue with various countries

[4] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

and United Nations on building an international strategy. He had sent the strategy out to every embassy in the world to de-marsh the local governments. The effort has created a great community and everyone has been very happy to participate. Chris Painter will be glad to give an update at another meeting.

Doctrine for Cybersecurity [5] (Presentation provided)[6]

Fred Schneider, Professor, Cornell University

Dr. Schneider shared his completed work on *Doctrine of Cybersecurity* with the board at his last ISPAB meeting. He explained that he leveraged his position as an ISPAB member to acquired government information. He learned an enormous amount, and affirmed that today's networked systems are not trustworthy. The root of the problem lies in policy and technology. Security has high costs and further compounds the problem. It costs more money to develop a system for increase security. The paper, *Doctrine of Cyber security,* proposes to "view cybersecurity as a public good or to adopt mechanisms inspired by those used for public health". It defines goals, includes the means, and explains resolutions. In his presentation, Dr. Schneider talks about the early doctrine -- doctrine of prevention and doctrine of risk management, while recent doctrine includes a doctrine of accountability, which is to deter attacks through threats of retribution. The New Doctrine describes cybersecurity is a public good, and "public health" is a public good as well. Dr. Schneider followed up with an explanation of the goals and means of the Doctrine of Public Health and how it relates to Public Cybersecurity. While this paper is available publicly, it has not been implemented. Dr. Schneider requested for the board to help him to move forward his paper. The board agreed to study the paper and submit a recommendation to OMB.

NIAP Testing and Assurance

Shaun Gilmore, Lead Validator, NSA
Carol Houck, Director, NIAP, NSA Commercial Solutions Center

Shaun Gilmore stated that NSA has worked closely and effectively with NIST on *National Information Assurance Partnership* (*NIAP*). NIAP was originally put together for unclassified systems. NSA has met with many common criteria international partners as they are looking to expand to commercial usage, and to classified systems. They have evaluated a lot of products and technologies. They have nine US approved Common Criteria testing laboratories. NIAP has been reengineering so as to be more efficient and to improve on processing to the market. The changes will include focus on functional requirement with specified assurance activities; and crypto requirements in the profiles. They have asked vendors for more participation and sought to give a larger role to the industry. Ultimately, they are seeking to regain credibility to the program and are looking for areas where they can increase values. Mr. Gilmore discussed steps taken with Customer Engagement, Policy Updates and Technology Communities and Protection. Fred Schneider, suggested that publishing an article would help to improve visibility.

The meeting recessed at 5:23 P.M., Wednesday, July 13, 2011.

[5] http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf
[6] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/Jul13_Schneider-Lecture-PolNewDoctrine-NIST.pdf

Thursday July 14, 2011

The Chair called the meeting to order at 8:04 A.M. and led the board's review of yesterday meeting.

Board Discussion

The board members discussed the various approaches and presentation from the Cloud panel. The Chair suggested that the board should ask the panel clearly for the information they need. Annie Sokol, NIST, stated that we are waiting for the OMB memo to be finalized and release before inviting any representative from FedRAMP to meet with the board. Ed Roback suggested inviting some of the users who have already used the cloud to discuss their experiences. The board was also interested in having information on the cost of moving to cloud computing, and therefore, it would be good to arrange a future panel consisting of users and especially those who have already implemented cloud.

The board reacted favorably to the discussion on the Status of Cyber Legislation. In general, board members found the Senate Committee representatives to be very forthcoming and aptly shared the information. Phyllis Schneck suggested that the board to provide appropriate, strong recommendations and feedback to them. Ed Roback supported an arrangement to invite them to one meeting every year.

The board also reacted favorably to Dr. Schneider's presentation. Board members were not sure about the elements of common criteria as presented by the NIAP team or of the advantages of the program. There were concerns on safety/security component.

Mississippi Sate Research on SCADA and Mississippi State Research on Wounded Warrior (Presentation provided)[7]

Ray Vaughn, Associate Vice President for Research, Mississippi State University
Dave Dampier, Associate Professor, Mississippi State University

Mississippi State Research on Wounded Warrior

Ray Vaughn and Dave Dampier worked together on a Digital Forensics training program in 2004 for law enforcement. Building on this work, they use this training program to help the wounded warriors returning from active combat to learn a skill. The training program was funded by NSF until 2012. Dave Dampier described the formation of the National Forensics Training Center. Their work included murder cases, identity theft, and child pornography cases. The program is responsible for training for over 1500 police officers in Mississippi, and also conducted training in 34 other states. The training is free and they also offer accommodation and meals to all students.

The curriculum for the program is broken down into three tracks. They would be glad to collaborate/work with other parties. Dave Dampier discussed about some of the lessons learned and that military hospitals are better fit for the program. There are 28 warrior transition units but they do not have funding to go to all of them. The cost for a 3-week training session per person is about $1000. The training represents more than an academic effort for those wounded warriors.

[7] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/Jul14_Vaughn_SCADA-Presentation-2011.pdf

Matt Thomlinson, who is the lead person on forensics training at Microsoft, would be happy to meet them when they next visit Ft. Lewis for exchange of information and further discussion.

Mississippi State Research on SCADA

Ray Vaughn presented his observations and opinions on SCADA Systems. He also discussed his concerns, e.g. increased risks to interconnected systems when SCADA systems are attached to corporate internets. He explained their research at MSU and the relation to the SCADA world. He illustrated the dozens of exploits released for popular SCADA programs and the attacks on the miniature models of systems installed in their SCADA security laboratory. In addition, he provided many other examples of SCADA System Vulnerabilities. There is very little awareness on control system vulnerabilities. He stated that the major concern is the systems are outdated and they would require time and money to rebuild or recreate. He concluded his presentation with a video clip of a real time success hacking. The hacker was convicted and sentenced to nine years in jail.

Medical devices: Security and Privacy Concerns (Presentation provided)[8]

Kevin Fu, Associate Professor, University of Massachusetts, Amherst

Dr. Kevin Fu spoke about the benefits of software in medical device and that many medical treatments could not exist without software. Today's computer technology is furthering the effectiveness of devices. Dr. Fu started his presentation with the history of medical devices and followed with an explanation of the working of an actual pacemaker. The battery occupies nearly half of the device. The device experienced few software issues in the 1980s, but issues doubled between 1999 and 2000. The contributing factors for security and privacy in medical devices were also discussed. But the larger issues are implementation errors, including problems relating to infusion pumps. People tend to be overly confident with software in devices and ignore potential risks. NITRD report stated that there is a "complete lack of regard, in the medical-device software domain, for the specification of requirements. There is no support for expired system and the system is exposed to virus.

He explained some emerging issues from information security and privacy namely, managerial issues – diffusion of responsibility such as maintaining and updating of software, reporting and under reporting of malware updates. He used the example of the Tylenol Scare of 1982 to illustrate some physical safeguard issues with medical devices. There were issues categorized as administrative and technical.

In conclusion, devices are vulnerable and very little is being done. In many cases, upgrading of medical devices is complicated and usually required a visit to the doctor's office. Kevin Fu's presentation included a list of considerations and on how NIST can help. Donna Dodson, NIST, agreed that there is a need to have better coordination on S&P standards for medical devices and she would explore ways to remove roadblocks to medical device S&P research.

[8] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/July14_Fu-med.pdf

Enabling Distributed Security in Cyberspace[9]

Kim Johnson, Sr. Cybersecurity Strategist, DHS

Kim Johnson mentioned that the white paper, *Enabling Distributed Security in Cyberspace,* was published in March, 2011, and has five maturity levels. The intent is to reenergize the idea originated around 1980s of how cyber devices work together in real time and in their own defense. It was centered on DHS's five core mission areas: preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; safeguarding and securing cyberspace; ensuring resilience to disasters; and strengthening and maturing the Department. Presently, they have security products that are intended to protect whole communities and to have preventive actions and shared strategies in the future. The three building blocks are automation (speedy response), interoperability (have to communicate with each other in common operations), and authentication (appropriately authenticate, machine to machine authentication).

Building trust is a big issue, but scalability is a huge issue. These issues are not be simple and will evolve over time. It is critical to have collaboration on security and leverage sharing of data. The goal is to start some pilots so as to demonstrate feasibility. Fundamentally, it is how to get to a more secure – cyber ecosystem of the future, in which cyber participants, including cyber devices, are able to work together in near-real time to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state.

Presently, they are seeking to identify additional use cases; what kind of framework needs to be in place; and accountability for attack. A lot of information that they need to be collected has already been collected through continuous monitoring. In approaching diversity, they have been talking to academia, private and public sectors. Simultaneously, they are working with other agencies to start more pilots and conduct demonstrations. The plan is to publish three papers from the information they are gathering. Joe Guirreri expressed his concern on the classification of information and dissemination of information.

DHS had released cybersecurity strategy for interagency review and feedbacks are to be submitted to cyberfeedback@dhs.gov. Kim Johnson would welcome feedbacks from board members. Dan Chenok, Chair, suggested that Kim Johnson to review Fred Schneider's paper, Doctrine of Cybersecurity. The subsequent discussion touched on DHS's role in DOD's first unclassified strategy, [10]Department of Defense Strategy for Operating in Cyberspace. It was suggested to arrange a session discussion on the different strategies and Dr. Schneider's doctrine. The presenters should include representatives from various agencies including DOD. This is to look for any similarities among the strategies and assemble examples for moving forward.

[9] http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf
[10] http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Beyond FISMA- A Policy Framework for an Interconnected World (Presentation provided)[11]

Julie Boughn, Deputy Director for Operations, Center for Medicare & Medicaid Innovation, DHHS/CMS
Ryan Brewer, Senior Manager, Deloitte & Touche, LLP
Ashley Corbin, Director, Division of Research, Innovation and Standards, Centers for Medicare & Medicaid
Henry Chao, Deputy CIO, Centers for Medicare & Medicaid

Julie Boughn as the moderator for the panel began the discussion with description on government's focus. Government healthcare consumes over 30% of government budget. Almost everyday for the past five years she had to review and validate an enormous amount of FISMA report. While FISMA has done a lot of good, but as we move forward FISMA needs to adapt to the future.

Ryan Brewer began working at CMS on the Legacy Information Security Program three years ago. A lot of work was focused on continuous monitoring at that time. The data center in Baltimore is the only one with federal presence but almost everything is outsourced to contractors. Ed Roback mentioned that the definition of system has changed since FISMA started. Initially, it was difficult to get data owners to cooperate and to follow the FISMA regulations because they cannot justify the spending and quantify the benefits, and therefore, they do not care. They did not know what they were protecting or were they able to do anything about threats. They simply monitored vulnerabilities and risks. The present reporting allows connected/relying owners to be concerned about security. They were able to get agreement with required employers, private sectors, federal contractors, and other stakeholders to work with them. It is now consumer driven.

Ashley Corbin continued the presentation on Health Care environment drivers and Health information exchange/interconnectivity. They are constantly confronted to find ways of keep data classified and secured, and also to achieve these fronts in a cost effective way. A data use agreement must be in place before they can send/share the data.

FISMA is interpreted differently by agencies as noted by Henry Chao. There is no clear definition of functionalities and requirements. While FISMA compliance is mandated by OMB, application varied among agencies. He suggested that the future generations will benefit from some sort of training/education on FISMA. Henry Chao went on to describe the challenges with the Health Insurance Exchange Program including governance and authority; numerous securities, frameworks, audits and certifications; and resource demands. The suggested approach would be a pragmatic approach to have a harmonized security and privacy framework. He also described the Key Topics in the draft supplement which include System and Data Classification; Security Controls; Identity, Credential and Access Management; Secure Infrastructure and Could Computing; Data Encryption; Auditing; Continuity of Operations and Disaster Recovery; Compliance Oversight; and Privacy Consideration. Following the panel presentation, the board responded with comments and suggestions.

[11] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/July14_Boughn_Beyond-FISMA.pdf

A Study on Economic Incentives and Cyber (Presentations provided) [12]

Herb Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies

Herb Lin introduced his discussion as a potential new project that derives from his personal concept. He laid out the present problems. The private sector is doing just the minimal necessary for security. This is not to bear any unnecessary costs because spending on security is consistently increasing but does not result in higher return. While there are many solutions, there is no consensus or unified approach. Cybersecurity does not simply involve having good technology but measures must be deployed and used on a scale commensurate with plausible attacks, and economic and regulatory issues will have influence over deployment and use. Some possible solutions would be liability, mandated reporting and ISO certification. The question is: is this an economic issue or regulatory/policy issue where economic model leads to monopoly and regulations leads to a negative incentive. He is planning a possible NRC study that would look at the nature and extent of market failure, make an assessment of mechanisms, and provide workable recommendations. Board members suggested reviewing a study by Federal Energy Regulatory Administration on awareness failure. Dr. Lin appreciated the discussion and will provide a draft to the board for review.

Continued CIP Report and Industrial Control Systems Security [13](Presentation provided)[14]

Phyllis Schneck, McAfee (Moderator)
Stewart Baker, Steptoe & Johnson LLP
Kevin Gronberg, US House of Representatives
Michael Peters, FERC

Threats are growing faster than the application of security measures. The people’s perception of the threat has grown. People in general consider the internet as a good means to communicate with their homes’ energy controls with any measure of security. People do not realize that adopting some special security measures do not necessarily mean that the controls are secured or the measures are appropriate. Phyllis Schneck referred to a chart with a comparison of 2009 to 2010 threats and vulnerabilities. Government has not funded research on security and NIST approach on security was based on general consensus which does not provide any leadership on security. Dr. Schneck also touched on Smart Grid and the pros and cons of using Smart Grid. There are no common themes as to what are considered security in designing the smart grid. She said that security is not a primary concern for Smart Grid designers with reference to NIST IR 7628[15]. The paper explains the “how to” but did not explain what best for the individual. The last section of the presentation was on “Growing Divergence in how Countries Respond”, and it includes a list of recommendation as to the role of the Government. The panel proceeded to explain the various sections and elements of the CIP report,

The meeting recessed at 5:44 P.M., Thursday, July 14, 2011.

[12] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/Jul14_LIN-H_market-incentives-for-cybersecurity.pdf

[13] http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[14] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/Jul14_CIP-CSIS-2011-ISPAB.pdf

[15] http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

Friday, July, 15, 2011

The meeting was to order by the Chair at 8:20 A.M.

Board Discussion

The board reviewed the presentations and discussions from the previous day. Board Members were enthusiastic and appreciative of the presentations by Ray Vaughn and Dave Dampier, and the panels moderated by Julie Boughn and Phyllis Schneck. They agreed that to review more information from Dr. Herb Lin's concept. The presentation is very much in its formative stage. The board agreed to continue interaction/contact with the congressional staffers. On cloud computing discussion, the panel presented four different opinions, and board members would like to have a structured discussion. The board would like to have a follow-up discussion on NIAP next year. The board agreed to send a recommendation letter about Fred Schneider's paper to NIST Director and/or OMB. A motion was proposed by Brian Gouker and seconded by Peter Weinberger. The motion was approved.

As the Chair for ISPAB, he stated that it was an honor to work with Dr. Fred Schneider. He further proposed to include references and/or pictures of ISPAB past members on the website.

Public Participation

A letter (see Appendix B) was submitted by Ken Morgan regarding non-invasive threat issue relating to FIPS 140-3. The Chair had discussed the letter with Donna Dodson. Donna Dodson agrees that it is a very important question and will review FIPS 140 as a whole. There are concerns in this area from the users and vendor community. Matt Scholl stated that NIST is meeting CRI to discuss their concerns as well. A new draft is being considered but no definite plan has been decided. Donna Dodson asked whether the board is interested in reviewing the comments. It was suggested to review this topic at a next year meeting. The board agreed to post the letter on the website after NIST has cleared it with NIST legal counsel.

NICE and Cybersecurity Awareness Month

Ernest McDuffie, Leader of NICE, NIST
Kristina Dorville, Director, National Cybersecurity Education Strategy, DHS

Ernest McDuffie talked about the primary concern on the National Initiative for Cybersecurity Education (NICE) draft strategic plan[16]. (The draft was released for public comments. The comment period has been extended to October 3, 2011.) He stated that they had collected some comments that led to a redraft. The draft will be released to public in August. They hope to announce the final document during the workshop, September 2011 when NICE is organizing the second annual workshop, *Engaging Americans in Securing Cyberspace*[17], at NIST, September 20-22, 2011. At last year's workshop, there was a nice mix of academic private and public sector people. For the September workshop, they have a longer preparation time, a bigger budget, and they have started planning many activities. They have received a lot of enquiries on the workshop and have heard from many vendors.

[16] http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf

[17] http://csrc.nist.gov/nice/Sept2011-workshop/index.html?https://www.fbcinc.com/nist_Cyber/atreg1.aspx

NICE is still in a growing phase. They have changed the term 'Tracks' to 'Components'. The next step is to define gaps and new resources, and analyze on new structures and new activities that can be proposed for a 2-year cycle. They would like to make sure that the initiative stays relevant and fresh. Apart from funding and the amount of available information available, the biggest challenge that the team faced are that there are so many competing focuses and emphasis. They found that in the public mind there is no difference between safety and security. They found many closely related/parallel programs such as those organized by Department of Education. They need to work closely on cybersecurity education with other states and organizations.

Kristina Dorville from DHS is working on Component Area 1 and National Cybersecurity Awareness Month[18]. She has been with DHS since 2003 and she works closely with National Cyber Security Alliance. The National Cybersecurity Awareness month has always been run by their office. In October 2010, the National Cyber Security Awareness Campaign launched a new catchphrase: *Stop. Think. Connect*. The goals of the campaign are namely, to elevate the nation's awareness on cyber security, and generate approaches and strategies.

Some of her objectives are to shift the perception when working on getting the younger generation to understand. Some of their focus areas this year are: identity theft, fraud and phishing, cyber bullying, and cyber predator. She talked about the huge MTV campaign going on for Cyber Bullying. The Cyber Citizens Forums in which 17 forums have been presented. The National Cyber Security Month is in October every year. Kristina Dorville's goal is to reach out to all fifty states and they are looking for more volunteers. The metric for success is reaching out to as many people as possible -- attracting more people to download information from the website, and getting people to attend the events. They have a list of organizations that have signed up for the program, e.g., boys and girls club, 4-h, and boys and girl scouts.

NSTIC Governance

Jeremy Grant, Senior Executive Advisor for Identity Management, NIST

The board invited Jeremy Grant to return to provide an update on the program. He reported on a great launch with relatively positive press. The challenge is to maintaining interest in NSTIC. This year's primary focus is namely on governance structure. The comment period for Notice of Inquiry (NOI) for NSTIC Governance closed on July 22, 2011. The second focus is on organizing and funding for pilots. The Challenge.gov[19] program is a perfect candidate for a pilot. NSTIC is not a well-funded program, so they have been working with other agencies to gain a better understanding what they are doing with their pilots.

Jeremy Grant is working on putting together a report on how the group should be created and then to release it for comments by fall. He mentioned of his presentation at the recent NSTIC Privacy Workshop, and of the benefits of gathering a number of larger stakeholders in the same room. Generally, people were energized, enthusiastic, and ready to get involved. At the same time, there were also lots of nervousness and skepticism, and they need to keep reaching out to people and to maintain engagement. He would like to set aside work on implementation plan because there were more activities than necessary and the activities did not prioritize in the best interest of NSTIC. It is

[18] http://www.dhs.gov/files/programs/gc_1158611596104.shtm
[19] http://challenge.gov/

necessary to define what are achievable in the short terms and how best to leverage on the momentum. One of the biggest issues is relying parties and how to get more of their members engaged. In response to Ed Roback's question on IRS interaction, Jeremy Grant states that they have only had preliminary discussion.

For the next workshop – a technology workshop -- they had received a few offers to host the workshop, e.g. OASIS, OIX, BioPharma, DoC, and TechAmerica. Cybersecurity should be front and center of the technology workshop. Jeremy Grant talked about the possibilities of holding longer sessions such as a special ISPAB meeting for discussing NSTIC steering group. ISPAB could function as an advisory role to steering group.

Jeremy Grant stated that they are beginning to get some staff working together, but they did not have room to accommodate everyone. They are working to a renovated space on the second floor of the Commerce Department that will accommodate about fourteen people.

Jeremy Grant reported receiving three general questions from people: 1) How to get participation in NSTIC? 2) While the principles are great, but how do translate them into a set of rules? 3) How is NSTIC going to address the many privacy issues over the history?

The board is open to doing a half day or whole day focused on NSTIC at one of the next meetings.

Health IT Policy Committee
Tiger Team Recommendations on Security and Integrity of ePHI (Presentation provided)[20]

Deven McGraw, Director of the Health Privacy Project, CDT

Deven McGraw explained functions and activities of the Tiger Team. The Team was initially assembled in June 2010 to address some specific questions from Office of the National Coordinator (ONC). The recommendations were submitted to ONC through Health IT Policy Committee. The team is still meeting on privacy and security issues about 2-3 times a month. The ONC makes all of the decisions and rules. The focus is to recommend what policy levers to enforce and this is build on the HIPAA laws and not to change it.

The Health IT Standards Committee establishes standards and technical requirements for certified EHRs. The committee was a pioneer with security functionalities required for certified EHRs for Stage 1. The Policy Committee recommended matching patients with their information specifically using a Unique Patient Identifier. The Tiger Team supported meaningful use efforts to provide patients with greater access to their data to flag potential errors. The other recommendations include exchange requirements for entities, identification and authentication for provider EHR users, and patient portals. The presentation also covered security risk assessment for meaningful Use Stage 2 and amendments/corrections to health data.

[20] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/July15_McGrawTigerTeamrecs.pdf

Legislation and Related Activities in Cybersecurity and Privacy

Danny Weitzner, Office of Science and Technology Policy (OSTP)

Danny Weitzner's work with the administration is focused on consumers and commercial data privacy. He talked about the environment that we try to influence, with particular interest and approach to internet privacy which is a special interest of the President. He stated that we had entered a new phase on internet policy. The initial approach was to let the internet develops and to allow it to work its way. This is no longer the case with the government. There is a new market, new technology, and multi stakeholders, and it is necessary to look carefully for ways to collaborate and interact especially on PII. Companies should be able to comply with a code of conduct for sharing information, and a clear set of baseline privacy protection.

The government needs to fill in the gap in commercial interactions. In his view, the congress should take action and not react in a panic. The action should include a key part of the global internet scale. Danny Weitzner mentioned the discussion on the privacy with colleagues in Europe and Asia in particular to data protection and data retention. He would look forward to return to the board especially to discuss the privacy act.

Board Discussion

Brian Gouker motioned to approve minutes, Matt Thomlinson seconded the motion. The board approved the meeting minutes for the April 2011 meeting.

The following are proposed agenda items for the next meeting:

- Global Supply Chain – to include supply chain framework and common vocabulary
- DHS Follow-up on the strategy – possibly a follow-up session with Kim Johnson to discuss the strategy
- Baseline FISMA, group together a set of healthcare relating subjects, e.g. intersection privacy, cryptography, health IT, medical devices, FISMA and health data
- RSA -Privacy Identity management and Crypto. Workshop this fall.
- Cyber Awareness Month
- Data storage issue
- Lisa Schlosser
- Phil Reitinger
- FedRAMP – a follow-up with Dave McClure re. costs, experiences, FISMA ROI
- NSTIC – a follow-up with Jeremy Grant on NOI and Technology Workshop
- SmartGrid – the motivation and influence
- SCADA, National Border Database (NVD)
- Revisiting privacy work with consumer emphasis. Consumer Privacy
- Updates - Tommy Ross
- DOD Cybersecurity paper
- SP 800-53 Appendix on privacy
- Howard Schmidt / Bruce McConnell – status updates, oversight, leadership on cybersecurity, impending budget cut on the impact of security
- FCC and technology – FCC CIO
- OMB re. auditing
- Tony Sager, NSA

- Securing network sites, SLA, Cloud
- NIST Updates (including FIPS 140-3)

The next meeting was moved back a week to October 26-28, 2011, due to schedule conflicts with two board members.

Meeting adjourned at 12:57 P.M., Friday, July 15, 2011.

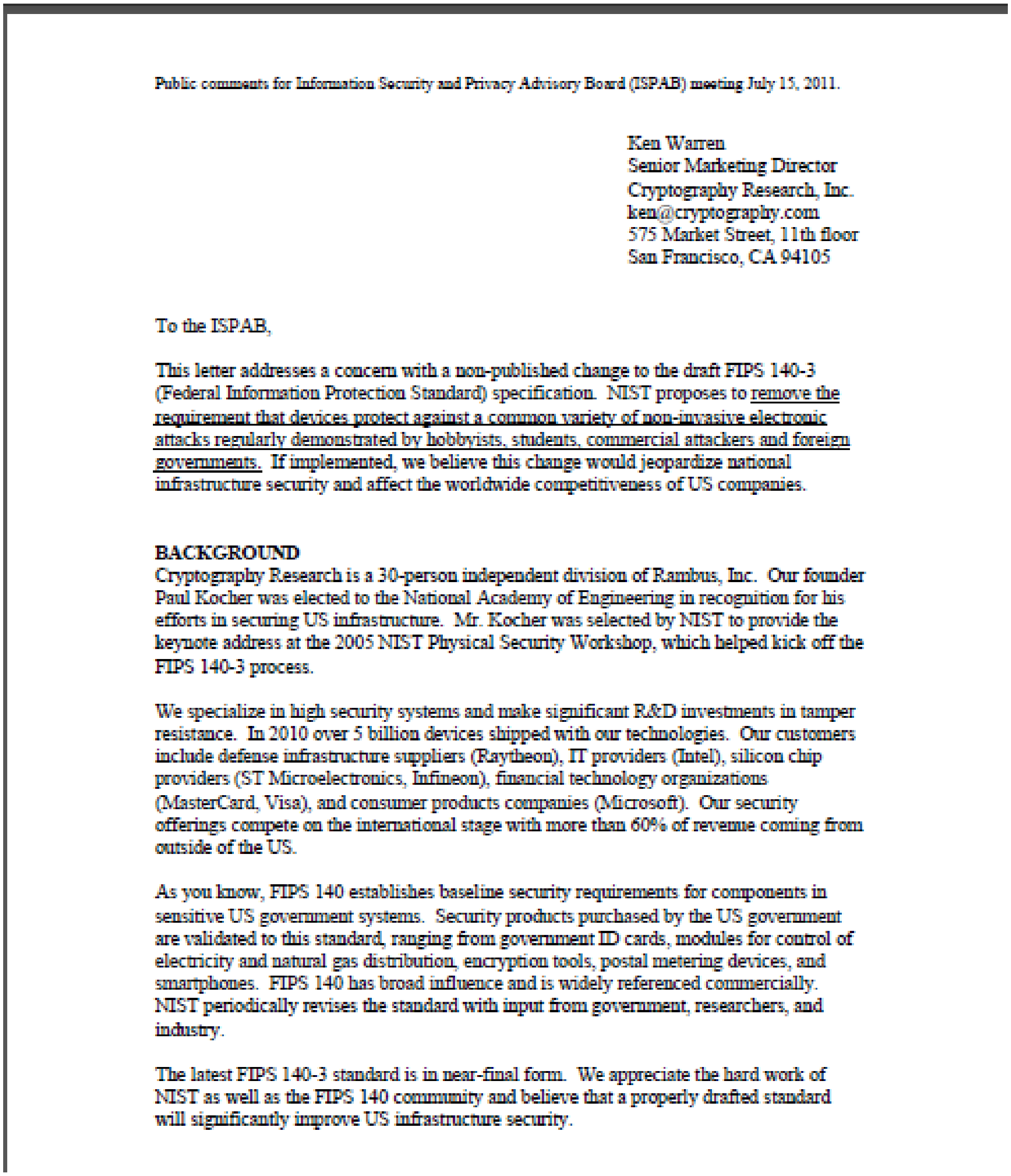
ANNEX A

LAST	FIRST	AFFILIATION	ROLE
Baker	Stewart	Steptoe & Johnson LLP	Presenter
Brewer	Ryan	Deloitte & Touche, LLP	Presenter
Bruggeman	David	ACM	Visitor
Camm	Larry	SEL, Inc.	Visitor
Chao	Henry	CMS	Presenter
Comley	Sarah H.	NA Independent Researcher	Visitor
Corbin	Ashley	CMS	Presenter
Cording	Kristina	CMS	Visitor
Crane	Earl	DHS	Panelist
Cummins	Keren W.	nCircle	Visitor
Curran	John	Telecom Reports	Visitor/Media
Dampier	Dave	Mississippi State University	Presenter
Davis	John C.	Teknoworks Inc.	Visitor
Dorville	Kristina V.	DHS	Presenter
Fu	Kevin	University of Massachusetts Amherst (UMASS)	Presenter
Gilmore	Shaun	NSA	Presenter
Grant	Jeremy	NIST	Presenter
Gronberg	Kevin	US House of Representatives	Presenter
Grote	Matt	Senate Committee on Homeland Security & Governmental Affairs	Presenter
Hennandez	Jessica	Department of Treasury	Visitor
Houck	Carol	NSA	Presenter
Jaffe	Roger	FRIIPWR USA Limited	Visitor
Johnson	Kim	DHS	Presenter
Kerben	Jason	Department of State	Visitor
LeDuc	David	Software & Info Industry Assoc	Visitor
Lightman	Suzanne	NIST	Visitor
Lin	Herb	National Academies	Presenter
McGraw	Deven	CDT	Presenter
McKay	Angela	Microsoft	Visitor
Mihalchik	David	Google	Panelist
Morgan	John	MITRE Corp	Visitor
Ozment	Andy	White House, National Security Staff	Visitor
Painter	Chris	Department of State	Presenter
Pfleeger	Shari Lawrence	Dartmouth College - I3P	Visitor
Posey	Laura	Microsoft	Panelist
Reavis	Jim	CSA	Panelist
Stine	Kevin	NIST	Visitor
Suh	Paul	Booz Allen Hamilton	Visitor
Vaughn	Ray	Mississippi State University	Presenter
Weinreb	Carly	The Constitution Project	Visitor
Weitzner	Danny	OSTP	Presenter
Wilson	David	Telos Corporation	Visitor
Zheng	Denise	Senate Committee on Homeland Security & Governmental Affairs	Presenter

ANNEX B

Public comments for Information Security and Privacy Advisory Board (ISPAB) meeting July 15, 2011.

Ken Warren
Senior Marketing Director
Cryptography Research, Inc.
ken@cryptography.com
575 Market Street, 11th floor
San Francisco, CA 94105



Public comments for Information Security and Privacy Advisory Board (ISPAB) meeting July 15, 2011.

Ken Warren
Senior Marketing Director
Cryptography Research, Inc.
ken@cryptography.com
575 Market Street, 11th floor
San Francisco, CA 94105

To the ISPAB,

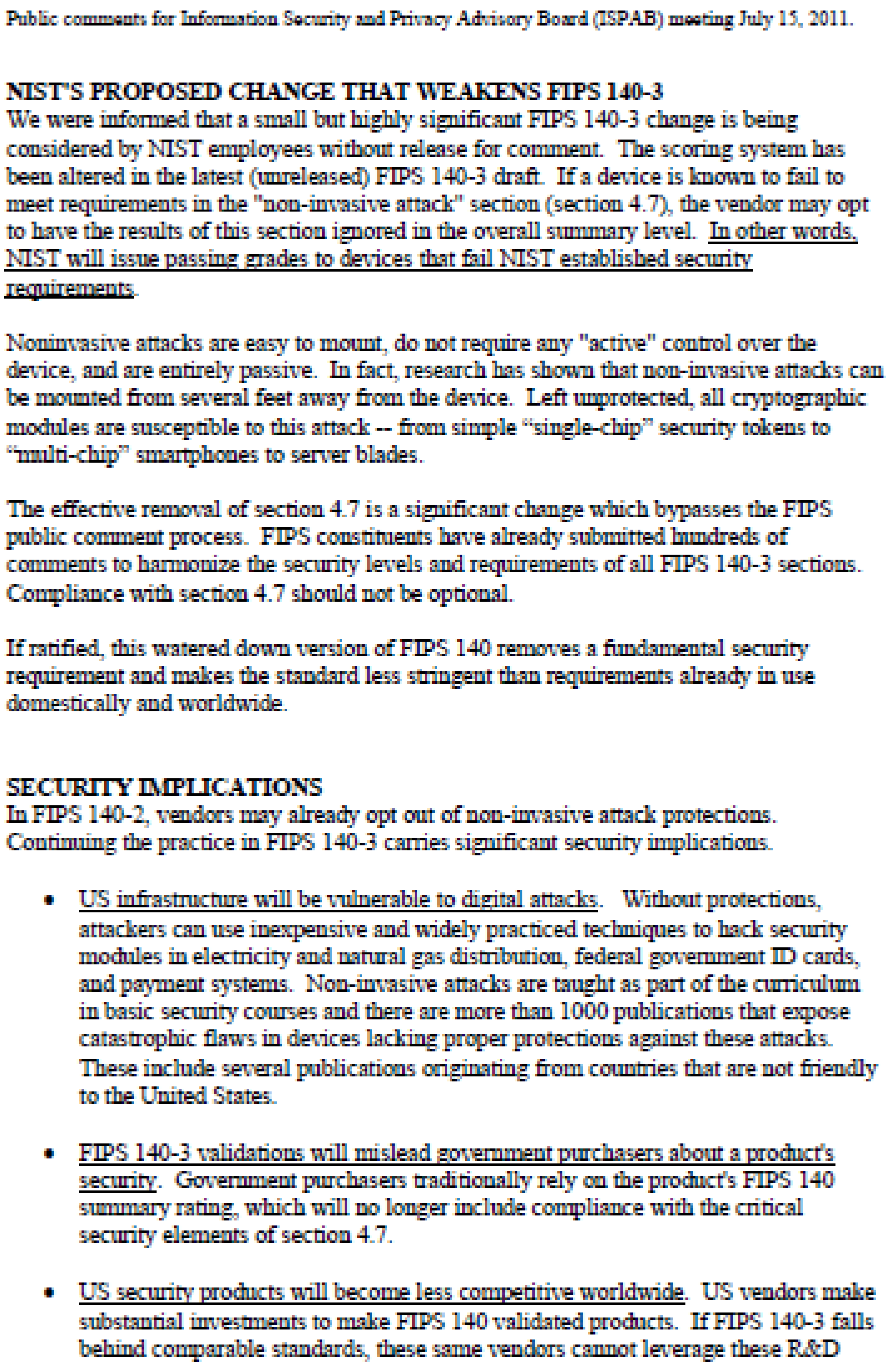
This letter addresses a concern with a non-published change to the draft FIPS 140-3 (Federal Information Protection Standard) specification. NIST proposes to remove the requirement that devices protect against a common variety of non-invasive electronic attacks regularly demonstrated by hobbyists, students, commercial attackers and foreign governments. If implemented, we believe this change would jeopardize national infrastructure security and affect the worldwide competitiveness of US companies.

BACKGROUND
Cryptography Research is a 30-person independent division of Rambus, Inc. Our founder Paul Kocher was elected to the National Academy of Engineering in recognition for his efforts in securing US infrastructure. Mr. Kocher was selected by NIST to provide the keynote address at the 2005 NIST Physical Security Workshop, which helped kick off the FIPS 140-3 process.

We specialize in high security systems and make significant R&D investments in tamper resistance. In 2010 over 5 billion devices shipped with our technologies. Our customers include defense infrastructure suppliers (Raytheon), IT providers (Intel), silicon chip providers (ST Microelectronics, Infineon), financial technology organizations (MasterCard, Visa), and consumer products companies (Microsoft). Our security offerings compete on the international stage with more than 60% of revenue coming from outside of the US.

As you know, FIPS 140 establishes baseline security requirements for components in sensitive US government systems. Security products purchased by the US government are validated to this standard, ranging from government ID cards, modules for control of electricity and natural gas distribution, encryption tools, postal metering devices, and smartphones. FIPS 140 has broad influence and is widely referenced commercially. NIST periodically revises the standard with input from government, researchers, and industry.

The latest FIPS 140-3 standard is in near-final form. We appreciate the hard work of NIST as well as the FIPS 140 community and believe that a properly drafted standard will significantly improve US infrastructure security.



Public comments for Information Security and Privacy Advisory Board (ISPAB) meeting July 15, 2011.

NIST'S PROPOSED CHANGE THAT WEAKENS FIPS 140-3
We were informed that a small but highly significant FIPS 140-3 change is being considered by NIST employees without release for comment. The scoring system has been altered in the latest (unreleased) FIPS 140-3 draft. If a device is known to fail to meet requirements in the "non-invasive attack" section (section 4.7), the vendor may opt to have the results of this section ignored in the overall summary level. In other words, NIST will issue passing grades to devices that fail NIST established security requirements.

Noninvasive attacks are easy to mount, do not require any "active" control over the device, and are entirely passive. In fact, research has shown that non-invasive attacks can be mounted from several feet away from the device. Left unprotected, all cryptographic modules are susceptible to this attack -- from simple "single-chip" security tokens to "multi-chip" smartphones to server blades.

The effective removal of section 4.7 is a significant change which bypasses the FIPS public comment process. FIPS constituents have already submitted hundreds of comments to harmonize the security levels and requirements of all FIPS 140-3 sections. Compliance with section 4.7 should not be optional.

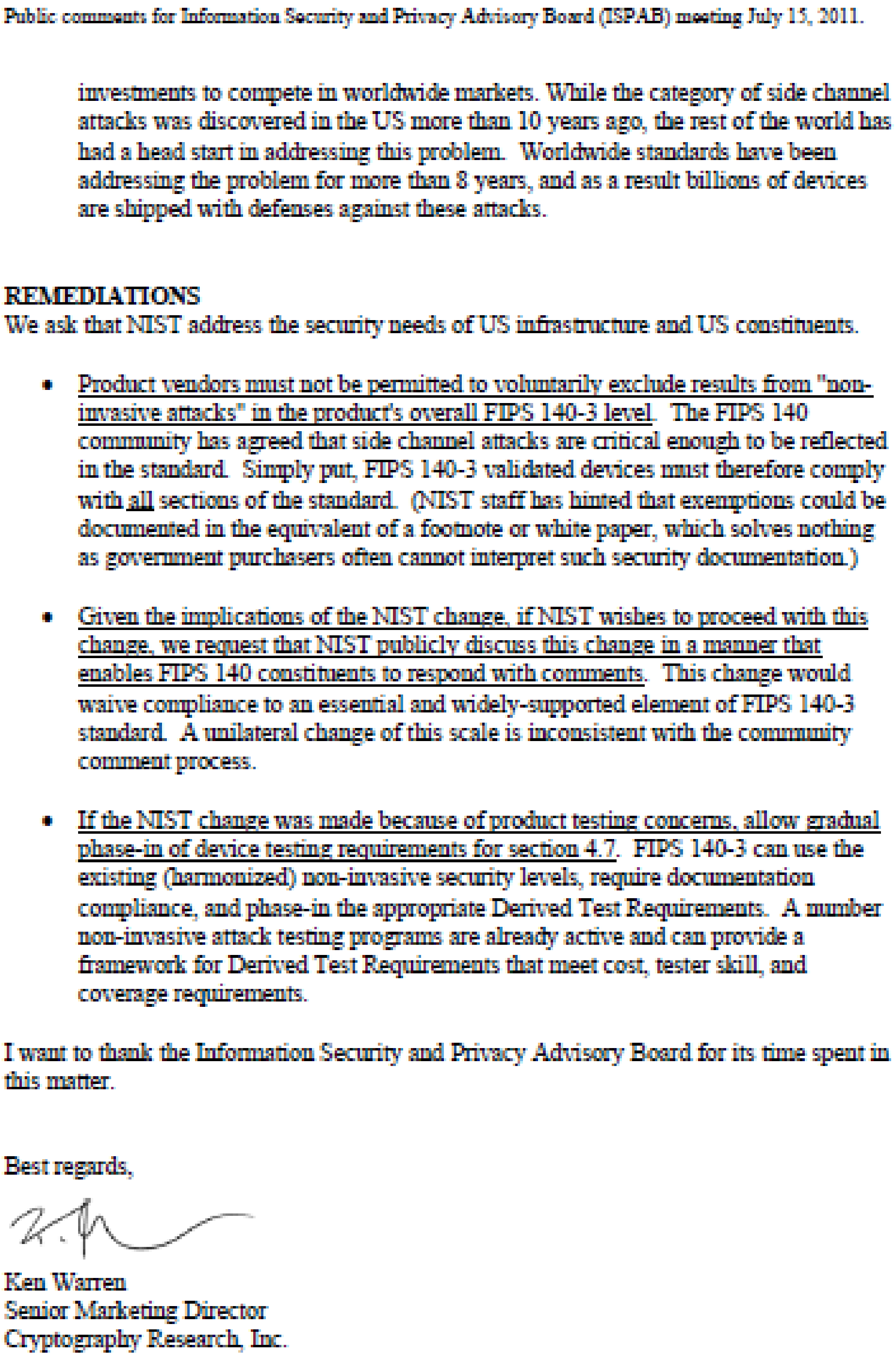
If ratified, this watered down version of FIPS 140 removes a fundamental security requirement and makes the standard less stringent than requirements already in use domestically and worldwide.

SECURITY IMPLICATIONS
In FIPS 140-2, vendors may already opt out of non-invasive attack protections. Continuing the practice in FIPS 140-3 carries significant security implications.

- US infrastructure will be vulnerable to digital attacks. Without protections, attackers can use inexpensive and widely practiced techniques to hack security modules in electricity and natural gas distribution, federal government ID cards, and payment systems. Non-invasive attacks are taught as part of the curriculum in basic security courses and there are more than 1000 publications that expose catastrophic flaws in devices lacking proper protections against these attacks. These include several publications originating from countries that are not friendly to the United States.

- FIPS 140-3 validations will mislead government purchasers about a product's security. Government purchasers traditionally rely on the product's FIPS 140 summary rating, which will no longer include compliance with the critical security elements of section 4.7.

- US security products will become less competitive worldwide. US vendors make substantial investments to make FIPS 140 validated products. If FIPS 140-3 falls behind comparable standards, these same vendors cannot leverage these R&D



Public comments for Information Security and Privacy Advisory Board (ISPAB) meeting July 15, 2011.

investments to compete in worldwide markets. While the category of side channel attacks was discovered in the US more than 10 years ago, the rest of the world has had a head start in addressing this problem. Worldwide standards have been addressing the problem for more than 8 years, and as a result billions of devices are shipped with defenses against these attacks.

REMEDIATIONS

We ask that NIST address the security needs of US infrastructure and US constituents.

- Product vendors must not be permitted to voluntarily exclude results from "non-invasive attacks" in the product's overall FIPS 140-3 level. The FIPS 140 community has agreed that side channel attacks are critical enough to be reflected in the standard. Simply put, FIPS 140-3 validated devices must therefore comply with all sections of the standard. (NIST staff has hinted that exemptions could be documented in the equivalent of a footnote or white paper, which solves nothing as government purchasers often cannot interpret such security documentation.)

- Given the implications of the NIST change, if NIST wishes to proceed with this change, we request that NIST publicly discuss this change in a manner that enables FIPS 140 constituents to respond with comments. This change would waive compliance to an essential and widely-supported element of FIPS 140-3 standard. A unilateral change of this scale is inconsistent with the community comment process.

- If the NIST change was made because of product testing concerns, allow gradual phase-in of device testing requirements for section 4.7. FIPS 140-3 can use the existing (harmonized) non-invasive security levels, require documentation compliance, and phase-in the appropriate Derived Test Requirements. A number non-invasive attack testing programs are already active and can provide a framework for Derived Test Requirements that meet cost, tester skill, and coverage requirements.

I want to thank the Information Security and Privacy Advisory Board for its time spent in this matter.

Best regards,

Ken Warren
Senior Marketing Director
Cryptography Research, Inc.