

# Information Technology SCC Meeting Minutes

## Attendees

---

**Michael Aisenberg** – VeriSign

**Scott Algeier** – IT-ISAC

**Larry Clinton** – Internet Security Alliance

**Guy Copeland** – CSC

**Robert Dix** – Juniper Networks

**Liz Gasster** – Cyber Security Industry Alliance

**Eric Hanson** – SRA International

**John Hopkinson** – International Systems Security Engineering Association

**Tiffany Jones** – Symantec

**Franck Journoud** – Business Software Alliance

**Clint Kreitner** – Center for Internet Security

**John Lindquist** – EWA - IIT

**Dan Matthews** – Lockheed Martin

**Lynn McNulty** – Information Systems Security Association

**Julie Mehan** – Hatha Systems

**Angela Morgan** – EWA – IIT

**Kevin Murray** – TestPros, Inc.

**Paul Nicholas** – Microsoft

**Andy Purdy**

**Phil Reitinger** – Microsoft

**Doug Sabo** – McAfee

**John Sabo** – Computer Associates

**David Sanders** – BearingPoint

**Howard Schmidt** – R&H Security Consulting

**Joe Tasker** – Information

Technology Association of America

**Bryant Tow** – Unisys

**Ken Watson** – Cisco

## Partial day attendees:

---

**Marcia Fagan** – BAH/DHS

**Greg Garcia** – DHS

**Nancy Limauro** – SRA International

**Cheri McGuire** – DHS

**Emily Miller** – SRA International

**Jon Noetzel** – BAH/DHS

**Robert Stephan** – DHS

**Chris Watson** – DHS

**Jeff Wright** – DHS

## Introductions

---

Guy Copeland, IT SCC Chair, welcomed the group and thanked everyone for attending. Mr. Copeland expressed particular thanks to all of those who took part in the great deal of work involved in drafting the Sector Specific Plan. He stressed that while an incredible amount of work had gone into the plan, much work remained to be done in the coming year. The next step would be to gather commitments from companies to follow the recommendations laid out in the SSP. Mr. Copeland stated that for the most part these commitments consist of activities that organizations are already undertaking, with the bulk of the

recommendations calling for renewed cooperation at policy and leadership levels.

Mr. Copeland also notified the group of several organizational changes occurring within DHS (this was confirmed later in the day by Assistant Secretary Garcia). Specifically, the National Communications System (NCS) and the National Cyber Security Division (NCSD) have had substantial reorganization in their ranks:

- **Pete Fonash**, director of NCS, has moved to Chief Technical Officer of the Cyber Security and Telecommunications division and will be reporting directly to Greg
- **Colonel Victoria Velez** will be taking over the Office of Emergency Communications, which was established as a provision of the recent Homeland Security Appropriations bill
- **Sallie McDonald** will be taking over as director of NCS
- **Bruce Landis** will be named as the Deputy Assistant Secretary for Cyber Security and Telecommunications
- **Jerry Dixon** will be taking over the role of Director of NCSD
- **Cheri McGuire** will be the Deputy Director of NCSD
- **Jeff Wright** will be moving up to replace Cheri as the Deputy Director for Strategic Initiatives Exercises, focused on control system security, training, education, and other duties
- **Hun Kim** will be AS Garcia's chief of staff

### **Proposed waiving of Charter notification rules**

Mr. Aisenberg also welcomed the group and expressed his thanks to everyone for their commitment and effort. Mr. Aisenberg recognized that for some members their job is government relations, but for many members they have to carve out valuable time from their regular jobs to participate in the IT SCC, and wished to express his sincere thanks to everyone for participating.

Mr. Aisenberg stated that the group had done an excellent job on behalf of the sector, but many of the estimates made in setting the foundation for the group a year ago were not as accurate as they could be. As such, many of the items for discussion later in the meeting would require advanced notification and a waiting period before the group could approve them. The proposed motion waived these notification requirements and allowed the group to vote on any matters chosen for discussion and voting without risking violation of certain notification rules set forth in our charter.

Proposed motion: *"The Membership of the IT SCC, upon recommendation of the EC, waives any and all provisions of the Existing IT SCC charter regarding notice of agenda, quorum and prior action of the EC for the meeting of January 9, 2007, for the purpose of permitting the reorganization and legal entity proposals separately considered to be conducted as business matters of the IT SCC."*

The motion was approved unanimously.

### **Plenary Voting – Membership Applications**

---

The group voted unanimously to approve Juniper Networks, Business Software Alliance, and Hatha Systems as IT SCC members

### **Plenary Voting – Secretary Nomination**

---

The Executive Committee issued a call for nominations for Secretary shortly after Greg Garcia announced his departure. The EC talked with several interested organizations, and Bob Dix was ceded the position by all involved. The IT SCC unanimously voted to confirm Bob Dix as Secretary.

### **Bylaws Revision and Updates**

---

Hugh Webster, a local attorney, drew up documents in consultation with Mr. Aisenberg to transform the IT SCC into a legal entity, registered in the District of Columbia. This followed discussions and suggestions made by the IT SCC earlier in the year to form a legal, non-profit entity. Mr. Webster examined the structure and scope of the organization and recommended that the group incorporate as a 501 c(3) in D.C.

The bylaws proposed at the meeting contained three sections that had been altered significantly.

- A statement of purpose was inserted into the front of the document in order to comply with listing requirements.
- Many of the notification time periods were shortened, particularly in respect to new membership applications. This was done in order to speed up the process of reviewing new member applications. The idea was to get interested organizations involved more quickly, rather than forcing them to wait an entire quarter to get involved.

- A change to the cycling of Executive Committee members was proposed. By the original charter, half of the Executive Committee would be replaced at this meeting. The Executive Committee felt that this would be cutting off a base of expertise and experience of many people at a critical junction in the evolution of the organization. With this proposed change, the Executive Committee elections would be postponed until January 2008, when half of the EC seats would be up for election. Additionally, Guy Copeland would continue to hold his seat as Chair until January 2008

**Questions:**

**Q: *Is a 501 c(3) allowed to lobby?***

**A:** There is no specific prohibition from lobbying as a 501 c(3). Instead, the rules specify that no more than 10% of the funds of the 501 c(3) can be spent on lobbying, and the lobbying cannot be on specific policy recommendations. The 501 c(3) is not recognized as an association that represents its members in a manner similar to lobbying organizations.

**Q: *Are funding mechanisms directly addressed by the bylaws?***

**A:** The only conversation held about this topic at the moment is that the IT SCC would like to be self-sustaining. There are no requirements for the bylaws to include funding mechanisms, and Mr. Webster recommended that the group try to keep the documents as lean and flexible as possible. Once the bills and total costs are aggregated, the Executive Committee will look at the final costs and likely present several options to the IT SCC as a whole.

**Q: *How does the automatic succession of officers work?***

**A:** The automatic succession of the Vice Chair to the Chair position was agreed upon for a variety of reasons. Part of the concern was ensuring that the IT SCC has a consistent face in meeting with government individuals. If a Vice Chair takes over as Chair that person already has an established relationship with many key individuals and is a familiar face. This becomes increasingly important as there is turnover in government, particularly on the Hill. Additionally it offers a benefit internal to the organization with predictability in knowing that there will be continuity and work will go forward even with a new Chair.

The group unanimously passed the bylaws revisions.

The group unanimously passed the motion to proceed with filing the IT SCC as a legal entity.

## **Report on PCIS Activities**

---

Mr. Stuart Brindley joined the group via teleconference to talk about recent Partnership for Critical Infrastructure Security (PCIS) issues. Mr. Brindley informed the group that in addition to being a defining moment for the Sector Coordinating Councils, this was also proving to be a critical moment for PCIS. Now that PCIS has officially been recognized as the place to bring together representatives from all of the SCCs they are working to develop a business plan for 2007 to determine what task areas they wish to focus on. The PCIS held a meeting on January 10 to discuss their business plan, and anticipate moving forward on the recommendations coming out of that meeting shortly.

PCIS does not wish to duplicate any of the efforts of the individual SCCs, but there are areas in which Mr. Brindley suggested PCIS could play a role:

- Partnership leadership: PCIS can offer leadership on CIP issues from a policy perspective, and act as a coordinated point of contact for DHS on policy recommendations from the combined SCCs.
- Cross-sector leadership: PCIS can work on providing a venue for sectors to work together on cross-sector interdependencies.

Mr. Brindley reiterated that DHS looks to PCIS for recommendations and input from the private sector, as a venue where all of the SCC inputs can be compiled. As such, in 2007 PCIS will strive to ensure the survival of the partnership framework, including putting emphasis that everything being done is being done in a voluntary manner, and any imposition of a regulatory framework will inevitably damage the partnership and set back much of the progress that has already been made.

### **Questions**

**Q:** *What is your assessment of other sector's approach to IT security, and do you feel that it is a point that has been acknowledged in other sectors.*

**A:** None of the PCIS members have had a chance to look at all of the different sector SSPs, only DHS has had that ability, so Mr. Brindley could not speak to the IT component of each of the SSPs. However, the offer was made by the IT SCC to review the Cyber sections of other plans, and some sector plans were reviewed by a group from the IT SCC.

**Q:** *Does PCIS intend on looking at cyber risk assessment as part of a cross-sector risk assessment activity?*

**A:** Mr. Brindley indicated that this is such a big area that PCIS is still tackling the issue of how to organize it. He informed the group that he anticipated the development of a working group for PCIS on the cross-sector risk assessment issue would be a part of the 2007 business plan.

**Q:** *Have you had any expressed interest from the Canadian government?*

**A:** Mr. Brindley stated that there hasn't been much interest at all from Canada. On an informal basis the PCIS has been working to get a greater participation, but most of the motivation has come from the private sector, not the Canadian government.

## **Working Group Reports**

---

### **SSP Working Group** *(slides distributed via e-mail)*

Mr. John Lindquist informed the group that the IT SSP was a collaborative effort between members of the IT SCC and the IT GCC, notably Cheri McGuire, DHS. The document was submitted to the Homeland Security Council Policy Coordination Council (PCC). The PCC returned some comments that focused on government pieces of the document and contained no substantive concerns. It is now at the Homeland Security Council for review, and should be approved within a few weeks. (The latest version was distributed to the group via e-mail following the meeting)

Mr. Lindquist encouraged all interested members to attend the next meeting of the Working Group, including new members, to be held on January 31, 2007. (Meeting information distributed via e-mail)

### **Strategy Working Group** *(slides distributed via e-mail)*

Mr. Scott Algeier informed the SCC that the Strategy working group met twice in the fall and were working on coming up with a financial plan for making the SCC self-sustaining. Currently the group is examining how much the operating costs will run. Once that is determined the group will determine what funding mechanisms are appropriate and present options to the full SCC membership.

### **Communications and Membership Working Group**

*(slides distributed via e-mail)*

Ms. Tiffany Jones informed the group that the Communications and Membership working group had suggested inputs into the bylaws to allow new member

organizations to become involved more quickly. These measures were passed earlier in the meeting.

Following the background introduction given by Ms. Jones, the group had a discussion on membership provisions and proposed changes to the bylaws. Among the topics addressed in this discussion:

- Member vetting process, and whether there was a need for a Membership Committee, or whether the Executive Committee should be sufficient to handle the membership applications
- Permission of electronic voting, so that vote on membership approval does not have to wait until a quarterly business meeting
- Proposal that if the Executive Committee chooses to reject an application that the SCC should be given an opportunity to review and vote on the application
- Currently, the only reason a company would be refused membership is if they do not meet the criteria as defined in the bylaws. One member of the group indicated that they wanted to ensure that whatever vetting process is decided upon that there isn't the possibility for a company who clearly does not meet the criteria for membership to be admitted as a member

Following this discussion, Ms. Jones touched briefly on the proposed nominations process for Executive Committee elections. Ms. Jones informed the group that there had been some concern expressed to her from the general membership regarding the slate process and a desire for more transparency. As the group was running short on time, it was agreed that members would review the "Membership and Communications" PowerPoint slides (distributed via e-mail following the meeting) and send all comments to Ms. Jones, who would anonymize them and share all comments with the Executive Committee.

### **Discussion with Assistant Secretaries Stephan and Garcia**

---

#### **Assistant Secretary Stephan**

Assistant Secretary Stephan thanked the group for inviting him to speak and expressed his appreciation for the efforts of all involved in the IT SCC. He informed the group that DHS recently completed the National Infrastructure Protection Plan (NIPP) requirement to submit all SSPs for approval by the end of 2006. All of the documents are currently at the Homeland Security Council for review, and AS Stephan indicated that he did not predict any substantive comments that would cause any controversy.

AS Stephan congratulated the group on their accomplishment and thanked the IT sector and Cheri McGuire for agreeing to take a look at not only the IT SSP, but other sector SSPs to ensure that cyber was taken into account in all of them.

AS Stephan informed the group that with the completion of the plans he now has the strategies set forth in those documents and can take them as evidence of how the partnership framework is working when asked to speak before the press or individuals on the Hill. The next step is to go inside each of the plans and determine what we have all committed to doing and get to the implementation of those items. AS Stephan requested that the group inform he and Assistant Secretary Garcia of anything that they can do to be of help in the coming year in regards to this implementation.

Regarding the distribution of intelligence documents, AS Stephan informed the group that DHS was working on pooling resources and ideas to determine how best they can provide relevant threat and risk assessment products, and how sector expertise and threats can be folded into this structure. AS Stephan assured the group that he recognized that the IT Sector was almost exclusively a private sector dominated industry, and DHS should not and would not release documents that do not have “private sector fingerprints all over them”. He also informed the group that the Homeland Infrastructure Threat and Risk Assessment Center (HITRAC) has a program in place now to imbed full-time private sector analysts into the intelligence shop.

AS Stephan announced that DHS was now embarking upon becoming a regulatory agency for the Chemical sector. He assured the group that DHS seeks to be a “modern” regulator, and is looking to balance the regulation in such a way that the industry is safe, yet still able to function in a competitive and economically feasible way. As such, DHS is approaching the issues from a purely risk-based approach, and will be breaking the chemical sector up into several tiers of risk, with different security measures needed for each.

Assistant Secretary Stephan also informed the group that DHS has put out a call for private sector input on the National Response Plan (NRP) re-write. The Assistant Secretary told the group that of particular interest would be the Critical Infrastructure/Key Resources annex, and he is seeking private sector assistance in coordinating and vetting the development of that annex.

In regards to the Annual Report process laid out in the NIPP, AS Stephan informed the group that the Department seeks to ensure that more private sector input is gathered this year. 2006 was the first year the reports were developed, and due to a compressed completion schedule, they were not as robust as they ideally should be. AS Stephan remarked that this year the Department was focusing on ensuring the GCCs and SCCs worked together to develop priorities on several issues, including:

- Research and technology solutions
- Modeling, simulation, and analysis capabilities
- Federal information sharing
- Risk assessment methodology

### **Questions**

***Q: How do you see linkages between operational commitments laid out in the SSPs and actual management of the programs. For instance, linkages between a program like CWIN or HSIN or other information sharing platforms.***

**A:** AS Stephan indicated that DHS is currently committed to a partnership with the ISAC Council and ensuring we work out information sharing mechanisms that work for all involved parties. He continued that the information sharing issue is a very big puzzle that they are working on sorting out, and will be looking to PCIS and the ISAC Council for assistance on building those relationships. AS Stephan also notified the group that he had recently met with Ambassador McNamara at the House Intelligence Committee and came out of that meeting with the responsibility to work on the development of regional and local municipality level intelligence “fusion” centers across the country.

***Q: How did the regulation of the Chemical sector come about; what were the driving forces behind it? Additionally, do you see this as a model for future DHS interactions with other sectors?***

**A:** AS Stephan indicated that the second question was up in the air, but DHS is not actively pushing for regulatory authority in any sector. If additional regulatory duties do surface down the line, DHS will approach the situation in the same way they are approaching the Chemical sector: risk-based analysis and approach. As far as why the Chemical sector was chosen, AS Stephan indicated that it was a number of factors, including political machinations, threats, current efforts, as well as countless other reasons. AS Stephan indicated that his own personal view is that roughly 80% of the operational capacity that DHS thinks is at risk is signed up for a voluntary responsible care code. However, within this 80% there are a large companies that are not getting the most efficient policies for their money. Many lower-risk facilities are spending more than they need to on security, while many higher-risk facilities are not spending enough money on

security. DHS will be looking to resolve these issues and provide a good baseline through the risk tiers it is developing. AS Stephan stressed that DHS has an established relationship with the Chemical sector through the SCC framework and will be working hand-in-hand with them on developing this regulatory framework.

**Q:** *In December, the IT SCC transmitted a priorities letter to you. Do you have any responses to any of the issues outlined in that letter?*

**A:** AS Stephan stated that he had received the letter, and in fact had met with the IT SCC Executive Committee on December 20 and was sure that all of the issues in the letter were either ongoing efforts within DHS or issues that DHS was willing to take on.

### **Assistant Secretary Greg Garcia**

Assistant Secretary Garcia informed the group that he and Assistant Secretary Stephan are working closely together and meet on a biweekly basis to coordinate and share information. He noted that they are currently drafting a point-by-point response to the priorities letter and should have that sent out before too long.

AS Garcia then made announcements regarding the change of staff under his command as mentioned by Guy Copeland during his introduction (see notes under Introduction section).

AS Garcia informed the group that he has briefed Secretary Chertoff on the mission and objectives of the Cyber Security and Telecommunications Division, and that the Secretary has made it a personal mission of his to be informed on Communications and IT initiatives, not just physical security. AS Garcia stated that Secretary Chertoff is tentatively scheduled to address the RSA conference in February, and is also interested in having a roundtable discussion with CEOs to talk about what initiatives really need to be accomplished. The roundtable discussion is still in development, but AS Garcia notified the group that he will be working with the SCC to put this together when appropriate.

AS Garcia next laid out the mission for the Cyber Security and Telecommunications Division (CS&T):

- Prepare and deter: The NIPP and particularly the SSP are part of this process of looking at vulnerabilities, assessing what the status is, and ensuring the sector is prepared.

- Respond: Not just in terms of IT/Communications sectors, but also more robust national capacity. CS&T will be looking to ISACs for operational intelligence and information sharing across all sectors.
- Build awareness: CS&T will have a presence at the RSA conference, and is interested in any other opportunities to reach out to large, medium, and small enterprises to work together with stakeholders to strengthen security posture.

AS Garcia indicated that one of CS&T's immediate priorities is developing a continuity of operations for incident response in the event of a Cyber Incident of National Significance (CINS). AS Garcia acknowledged that a CINS definition still needs to be put into place and that there is significant discussion around the topic, but assured the group that it remained one of his top priorities in the coming months.

AS Garcia also informed the group that one of his highest priorities was to work with the Office of Management and Budget (OMB) to develop a suite of best practices for all federal agencies regarding the ever evolving world of cyber security. He stated that CS&T would be reaching out to the sector for valued input and experience in these matters when the activity is spun up.

### **Questions**

***Q: Some of the comments we have heard from the Hill are that they want to work closely with you, developing a communications link that previously has not been there, can you speak on these efforts?***

**A:** AS Garcia noted that CS&T would be hiring a contractor for outreach and coordination who has a background in staffing on the Hill. Additionally, AS Garcia mentioned that he has made it clear to the Office of Legislative Affairs within DHS that he wants to create a proactive and assertive Congressional affairs posture. It is his intention to keep Congress well-informed with regular briefings, and he informed the group that he may be calling upon them for support when appropriate in these meetings.

***Q: There hasn't been a great deal of coordination between the Science and Technology (S&T) division at DHS and other divisions in the past. I was wondering what plans you have for addressing this issue.***

**A:** AS Garcia noted that there is a new Science and Technology Integrated Product Team (IPT) which will be a new process for S&T to reach out to stakeholders within DHS. He stated that this would be a good process for leading the prioritization of cyber elements into the larger framework of DHS, specifically Research and Development (R&D). AS Garcia assured the group that

when the times comes for distributing the funds available the IPT will work to get the top priorities plugged into that process.

*Q: One of the emerging issue areas we on the industry side have been concerned with is the international nature of the network threat and what kinds of partnerships are required to address these issues. DHS seems to have a substantially domestic focus, but I was wondering what you feel the attitude is on this within DHS.*

**A:** AS Garcia mentioned that he was just out in London with the Deputy Secretary attending a joint contact group for a homeland security partnership between the UK and US. DHS, TSA, and the UK equivalents were all present, and cyber was a topic on the agenda. AS Garcia noted that there is widespread recognition that everyone has cyber vulnerabilities in one way or another and it is a concern. AS Garcia did stress, however, that much work remained to be done and he would be reaching out to the group to work with them on how to manage the global threats.

*Q: How do you see the notion of using government and private sector procurement to raise ambient security without the use of regulation?*

**A:** AS Garcia replied that this is part of CS&T's package of security actions they are trying to develop with OMB on how agencies should protect themselves (including acquisition, 24/7 watch, and procurement) AS Garcia noted that he realized it is an ongoing effort that deserves his attention.

*Q: Have you had a chance to think about how we can work together to get a better handle on how to define an Incident of National Significance (INS), and how we can combine physical/cyber interdependencies?*

**A:** AS Garcia noted that there has been a great deal of discussion on a definition of an INS, and it is an effort that is still being worked on.

## **NCSD Activities Report**

---

### **TOPOFF 4 FSE (please see slides distributed via e-mail)**

Mr. Jeff Wright gave a presentation to the group on the upcoming Top Officials (TOPOFF) 4 Full Scale Exercise (FSE). Mr. Wright indicated that most of the officials involved in TOPOFF 4 are first responders and don't know a great deal about cyber, so it has been a major challenge for NCSD trying to plug into that effort. There was significant discussion on how best to insert cyber concerns into TOPOFF, and why previous iterations of the exercise did little-to-nothing to consider the impact of cyber and communications failures. Mr. Wright assured the group that NCSD definitely understood the valid complaints of the IT SCC, and was working to resolve these issues and get cyber concerns involved with the exercise.

### **Cyber Storm II (*please see slides distributed via e-mail*)**

Mr. Wright informed the group that Cyberstorm II would be significantly different from Cyberstorm I in regards to the recovery phase. He also stressed to the group that they should put time into providing objectives, as this time around the objectives provided by the private sector would be driving the exercise in order to maximize the benefit to the organizations involved.

### **National Response Plan Rewrite**

---

The National Response Plan (NRP) is currently undergoing a rewriting period and is soliciting input from the private sector through the SCCs. Representatives from the IT SCC leadership are involved in the process and will keep the group informed of the discussions surrounding the development process.

### **Communications Sector Report**

---

Mr. Guy Copeland informed the group that the Communications SCC (CSCC) has submitted its SSP and is undergoing the same review process as the IT SCC. The CSCC cosigned the priorities letter delivered to the Department in December. Finally, Mr. Copeland informed the group that efforts are continuing on the possible convergence of the Communications and IT groups, beginning at the operational level in dealing with the Communications and IT ISACs.

### **IT ISAC Report**

---

Mr. John Sabo encouraged all members to participate in the IT ISAC if they have not joined already. Mr. Sabo mentioned that the IT ISAC started discussions on convergence with the Communications ISAC and anticipates having a plan within 90 days. Additionally, the ISAC is hard at work developing relationships with other ISACs. Finally, the IT ISAC is working on a new concept of operations that will attempt to harmonize our activities with USCERT and develop a conops document that will clarify roles and responsibilities, information sharing, policies, controls, response, threat levels, collaborative analysis, emergency procedures, support for exercises, as well as other important operational concerns.

### **ISAC Council Report**

---

Mr. John Sabo informed the group that the IT ISAC has been a leader in working on the ISAC Council, and has been working with Assistant Secretary Stephan to foster a close relationship with DHS. The ISAC Council is developing a proposed information sharing framework for operational information

intelligence, which is being endorsed by PCIS. The framework is still in an early stage, but is developing nicely.

### **Workplan for 2007**

---

Mr. Guy Copeland informed the group that there would be many tasks ahead of the IT SCC in 2007, and laid out several areas that would require work:

- Commitments laid out in the Sector Specific Plan
- Commitments laid out in the National Infrastructure Protection Plan, including the Annual Report process
- A variety of internal IT SCC matters, including: new membership; bylaws revision; establishment as a legal entity; budget concerns; and others
- Education efforts on the Hill
- Convergence of IT and Communications communities
- Development of a communications strategy
- Development of a membership recruitment plan for 2007 on how to broaden the foundation of the organization

Mr. Copeland requested that the group please notify Secretary Bob Dix or Secretariat Eric Hanson or any other issues that they feel should be considered for inclusion in a business plan for 2007.

### **Conclusion**

---