



**Information Technology Sector Coordinating Council (IT SCC)
Quarterly Plenary Meeting
January 8, 2008**

Welcome & Introductions

Mr. Guy Copeland introduced himself and thanked everyone for attending the annual meeting for the Information Technology Sector Coordinating Council (IT SCC). Mr. Copeland also welcomed new members to the council, and introduced Mr. Joseph Lauffer, as the new secretariat support from SRA International.

Administrative Items

Mr. Copeland began by taking attendance. Given those participating in person as well as those joining via telephone, Mr. Copeland concluded the council had a quorum.

Mr. Larry Clinton, the ranking Treasurer, was unable to attend and thus could not deliver his quarterly report. In his place, Mr. Copeland informed the council that, at present, it has a comfortable balance of funds, adding that donations are always welcome.

Mr. Copeland shifted the focus of the discussion toward a by-law miscalculation in the election process. He explained that those elected to an officer position do not have their Executive Committee seat automatically extended to coincide with the end of their term as an officer. Mr. Copeland proposed an amendment to the by-laws to correct this issue.

The council then voted to see if any members had any objections to the language or the timeline of notification of the amendment. There was none. Mr. Copeland then read the by-law amendment to the council and asked if there were any objections. Mr. John Sabo did not object, but inquired to the long-term implications of this amendment. Mr. Copeland said they would like to have more continuity, noting this amendment would facilitate continuity by lengthening members' terms. Two members agreed to move the motion, and since there were no further objections, the amendment passed.

Annual Elections

Ms. Tiffany Jones began her discussion regarding the elections with information about open seats for three officer positions and two Executive Committee positions. Under the terms of the recently passed amendment, Michael Aisenberg's ascent to chairman was not up for a vote by the Executive Committee. Current council Secretary, Mr. Robert Dix, was elected Vice

Chairman, putting him in line to become the next Chairman. Ms. Liesyl Franz, will take over for Mr. Dix as the council's next Secretary. Finally, Mr. Larry Clinton will remain Treasurer.

New Chairman Mr. Aisenberg informed council members that next year many positions are going to become available. Many opportunities for members to join the Executive Committee and become officers will then present themselves. The Executive Committee and Officers for the 2008 year is as follows:

- Michael Aisenberg (Chairman). EWA Information and Infrastructure Technologies, Inc. Special Assistant and Councilor to the President
- Robert B. Dix, Jr. (Vice Chairman). Juniper Networks, Inc., Vice President-Government Affairs
- Liesyl Franz (Secretary). Information Technology Association of America Vice President for Information Security Programs and Global Public Policy
- Larry Clinton (Treasurer) Internet Security Alliance, President
- Pete Allor, IBM Internet Security Systems, Program Manager, Intelligence & Vendor Relations & Special Assistant to the GM
- Guy Copeland, IT-ISAC Representative President Emeritus, IT-ISAC Computer Sciences Corporation, Vice President Information Infrastructure Special Assistant to the CEO
- Lynn McNulty, International Systems Security Association
- Paul Nicholas, Microsoft Corporation, Senior Security Strategist
- Andy Purdy, DRA Enterprise. President
- John Sabo, International Security Trust and Privacy Alliance (ISTPA) IT- Information Sharing and Analysis Center (ISAC) Ex officio/VOTING representative to IT SCC
- Ken Watson, Cisco Systems, Inc., Senior Manager, Critical, Infrastructure Assurance Group
- Marcus Sachs, Verizon. Ex Officio, Nonvoting-Representative of Communications Sector

Plans Working Group
(Please see slides for additional information)

Mr. John Lindquist introduced the four current working groups within the IT SCC.

- Plans Working Group
- Critical Functions/Information Sharing Group (CFIS)
- Core Implementation Group (CIG)
- Protective Programs/Research and Development Group (PPRD)

Mr. Lindquist then noted Ms. Liesyl Franz would take over the IT SCC Plans Working Group in 2008. The goal of the Plans Working Group remains to provide awareness of progress and review of products. After presenting a brief summary of each of the working groups, Mr. Lindquist and Ms. Jenny Menna of the Department of Homeland Security (DHS), mentioned that a critical foreign dependencies initiative is becoming a hot topic, one that Assistant Secretary Bob Stephan would like to study more in depth. Mr. Ken Watson agreed that if the council did not focus more attention on the global aspects of information security, the Sector could fall behind. The plenary agreed that, until recently, the Sector has not addressed the international aspects of the National Infrastructure Protection Plan (NIPP) in sufficient detail. Others suggested that the Cross Sector Cyber groups should perhaps be more involved in these dealings.

Critical Functions & Information Sharing Working Group (CFIS)

(Please see slides for additional information)

Mr. Scott Algeier and Mr. Patrick Beggs began their presentation by explaining how the CFIS broke down IT critical functions, risk management, and threat thresholds for the risk assessment pilot. The group has been working diligently to create a pilot project to implement risk assessment. Mr. Algeier and Mr. Beggs presented their methodology that would have the risk assessment pilot validated and operational in late 2008. They asked the plenary for help from subject matter experts who could potentially help the working group accomplish this task.

John Sabo, Information Security Analysis Center (ISAC) and Executive Committee member, asked how and when IT SCC ideas could be better utilized and put into the operational stage. For instance, large companies such as Boeing, which could greatly benefit from a risk assessment of the nature the CFIS has developed, are not participating in the SCC. Mr. Peter Allor speculated that if a real life scenario presented itself, the IT SCC assessments might become operational. Given the experience and knowledge within the IT SCC, operational respect and credibility should become the standard, members agreed. Ms. Menna said the government has increased its information sharing with SCC's, particularly since she and Mr. Robert Dix formed a small working group to help restructure information sharing between the government and industry.

Core Implementation Working Group (CIWG)

(Please see slides for additional information)

Ms. Franz introduced the CIWG, whose members have been focusing on the working group's outreach and awareness plan, as well as Sector-Specific metrics. The outreach and awareness plan has short and long-term goals to focus a proactive approach to Sector-Specific Plan (SSP) implementation.

Ms. Rama Moorthy noted the metrics that the CIWG is working on are developmental rather than operational metrics. The government would like working groups and sectors to provide proof of progress, and members proceeded to discuss what defines security. Specifically, the council addressed the question of whether the council, or even the government, can deter an incident, and if the overall goal of the IT Sector security is fully attainable. Mr. Marcus Sachs said risk assessment is hard to measure without fully understanding and defining risk. Mr. Ken Watson commented that the metrics were impressive, but added that the methodology behind the metrics could improve. Ms. Liesyl Franz recommended starting a sub-working group for Sector-Specific metrics in order to form an adequate strategy. ISAC representative and newly-elected Executive Committee member, John Sabo, ended the session by mentioning that every company and every organization has a different understanding and definition of risk assessment.

Assistant Secretary Greg Garcia Cyber Security and Communications

Assistant Secretary Greg Garcia expressed his gratitude for the invitation to speak and for the ongoing work of the IT SCC. A/S Garcia began by presenting his plans to share the progress from 2007 and the goals for 2008. He then congratulated everyone associated with the Sector-Specific Plan (SSP), labeling it as a one of the IT SCC's great achievements in 2007. A/S Garcia

said he looked forward to the forthcoming pilot in the months to come. Saying that 2008 will be an important year, A/S Garcia reminded the group that Homeland Security Secretary Michael Chertoff has consistently listed cyber security as a priority issue for the Department. He assured the council that despite the difficulties in measuring and seeing actual progress, the IT Sector had indeed enhanced security. The Sector has made great strides, he said, crediting the maturation of relationships between public- and private-sector security partners. A/S Garcia continued highlighting, what he saw as, the great achievements of the IT SCC. With increased participation, would add real value and relevancy to exercises such as Cyber Storm II. He continued by praising the SIN and FIN, which helped alert the industry on incoming threats. A/S Garcia closed his statement by again congratulating the council on its accomplishments. He said he hopes to keep the momentum moving forward in 2008.

Mr. Marcus Sachs asked A/S Garcia about metrics as they relate to cyber security. A/S Garcia said the Department is working on requirements for agencies to recognize their level of security, but first, he added, they need to enhance their assessment capabilities. Mr. Andy Purdy agreed that milestones should be made, but he added the Sector would like to communicate better and more frequently with government and with A/S Garcia himself. A/S Garcia agreed to improve opportunities for engagement between the SCC and DHS. Mr. Copeland thanked A/S Garcia for coming, and said he looked forward to the January 25 meeting with him, so the IT SCC can begin the year working together with its government partners.

Protective Programs Research & Development Working Group (PPRD)
(Please see slides for additional information)

Mr. Larry Kettlewell of the IT Government Coordinating Council (GCC) presented the PPRD Working Group updates. The trust building exercise remains tentatively scheduled for January 21. He said he would provide more information on the exercise shortly. In the near future, the PPRD will determine needed capabilities from the SSP, and then reach out to subject matter experts in February.

Strategy Working Group

The Strategy Working Group began for mostly budget strategizing, but are now able to look toward the future. Mr. Watson said they were working with new Chairman Mr. Michael Aisenberg, constructing goals and visions for the future of the IT SCC. Mr. Watson, chair of the Working Group, detailed strategy items the group felt were most important. Communication and information sharing between Private and Government is something they must continue to advance. Collaborations between different aspects of the IT cyber security community will improve efficiency, and therefore increases the probability of achieving its goals. Mr. Watson explained that expanding membership is a good thing, as the power of the council's voice will become stronger.

Partnership for Critical Infrastructure Security (PCIS)
(Please see slides for additional information)

Mr. Watson remained at the podium to update the council on the Partnership for Critical Infrastructure Security (PCIS). The PCIS will hold its quarterly meeting on January 17, and

topics will include private industry interaction and discussion with DHS, ISACs, and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). In addition to those listed above, the PCIS will continue its Pandemic Influenza preparedness work. Mr. Watson reminded the council the IT SCC has a strong voice in PCIS matters, noting that the council speaks directly to the government on all of these issues listed, including the upcoming handbook.

The PCIS, Mr. Watson said, wants to add value to the sectors by promoting risk assessment models, and looking into information sharing mechanisms. The PCIS agenda is made from the SCC's, so Mr. Watson ends by telling people to inform him what battles to fight for and he can do so through the PCIS.

Mr. Watson also discussed the recent successes off the Cross Sector Cyber Security Working Groups, and that more than 90 members attended the Working Group's last meeting. The talks of cross sector returned the conversation back to a discussion about how best strategies for measuring security. Mr. Copeland said he felt there is no such thing as absolute security, and that security is difficult to measure. Mr. Sachs disagreed, noting that he felt security is measurable, or else they would not be there. Mr. Robert Dix said he believes the current model is working. He said Cross Sector Cyber Security in general is working, and is activating more participation.

IT-Information Sharing Analysis Center

Mr. John Sabo, a newly elected Executive Committee member and representative from the IT ISAC, introduced himself and said he would be taking over for Mr. Phil Retinger. The IT ISAC is currently examining how to maintain communication if there are disruptions to the Internet, in addition to working on the upcoming Cyber Storm II exercise.

Mr. Sabo thanked Ms. Franz and ITAA for all their help and assistance. He then agreed with the earlier discussion that the information compiled from the private sector and the IT SCC need to end up in the hands of decision makers on Capitol Hill. Mr. Sabo mentioned PCIS has been opening up its meetings to ISAC, which has been helpful for communication. He credited Mr. Robert Dix for working hard toward collaboration in the ad-hoc relationships, and for what the role of ISAC is in incident response. Mr. Dix stated he wanted to create better methods to communicate security information, to put them into writing and institutionalize them. Expanding the Steering Committee was another idea that could help make the private sectors input become operational because of the better representation, Mr. Dix said. Mr. Ken Watson suggested that when the ISAC calculates its first incident management results, it should send the results to him so he can insert them into the PCIS handbook. Mr. Watson ended by noting that the Critical Infrastructure Warning Information Network (CWIN) wanted to have increased communication role within the overall Critical Infrastructure Protection environment.

Communications Sector

(Please see slides for additional information)

Mr. Marcus Sachs, the liaison from the communications sector, updated the activities of the Communications Sector Coordinating Council (CSCC) to the IT SCC. The CSCC shares many

of the same interests as the IT SCC. The group's next quarterly meeting has been scheduled for February 14. There are currently 35 organizations in the CSCC, and most of the members have international interests within their organizations.

Mr. Sachs broke down the three core components of the communication sector. The first of which was voice, which consists of phone, radio and air traffic control sections of communication. The second core service is video, which ranges from live and on-demand entertainment to overall news and information. The third, and likely fastest growing, core service is Data, which covers the Internet, e-mail, GPS navigation, and remote file access. An IT SCC member suggested reaching out to satellite radio companies, such as XM and Sirius, to ensure that their growing field is represented adequately as well. Mr. Sachs agreed with the suggestion and said he would bring up the matter with the CSCC.

The CSCC reported that its studies suggest that it would require more than a single location would have to fail for the overall communications national infrastructure to collapse. They have been in discussions about locating one particular spot that can present significant risk to national communication and the core network and infrastructure, but no such single place exists. In conclusion, the CSCC is beginning to communicate more regularly. With elections scheduled at their next quarterly meeting, the CSCC is set to elect a new Chairman and Vice Chairman.

Center for Strategic & International Studies Cyber Security Commission

(Please see slides for additional information)

Mr. Sachs explained that the goal of the CSIS commission on cyber security is to develop actionable recommendations for the incoming administration to improve U.S. Cyber Security. Essentially, he said, it is a think tank for the next president. In addition, the commission has established five working groups from plenary sessions in 2007: 1) Horizon Review; 2) Threats; 3) Complexities; 4) Key Actors; and 5) Infrastructure. The upcoming phase will establish where the commission stands, and it will allow members to review what is out there. Mr. Sachs ended by noting in the next year there will be brainstorming on all levels of the cyber community, until the report is due in December 2008.

Cyber Storm II

(Please see slides for additional information)

Cyber Storm II will be the largest government sponsored cyber security exercise ever. It involves four of the seventeen Critical Infrastructure/Key Resource (CIKR) sectors: Information Technology (IT), Communications, Chemical, and Transportation (rail and pipeline). These exercises will be publicized in a more comprehensive manner than the first Cyber Storm conducted in February 2006. The original exercise was quiet while this exercise will likely receive media attention. The exercises are to take place March 10-14, but pre-start exercises are going to begin two to four weeks prior. A master scenario is coming soon. The goal of Cyber Storm II is to execute a national cyber exercise to exam the process in response to a multi-sector coordinated attack on global cyber security.

National Level Exercise (2) 08 (NLE)

Ms. Casey Ateah, from the Office of Infrastructure Protection (IP), discussed different exercises such as TOPOFF 4, now called NLE. These particular exercises are incident management activities, which will take place the first week of May 2008. She added for continuity and cooperation, many exercises in addition to Cyber Storm II and NLE will present themselves in 2008. Mr. Watson proposed the government should ask for subject matter experts from the private sector to help assist in exercises. This would benefit both industry and government while strengthening collaboration between the two.

National Cyber Response Coordination (NCRCG)

Ms. Cherri McGuire informed the council that the NCRCG is currently updating its charter, concept of operations (CONOPS), and standards of procedures (SOPs). The group is also coordinating information sharing with the DHS Office of Operations Coordination. New additions to the NCRCG are as follows: public affairs, private sector coordination, international coordination, and a crisis action team (CAT). Ms. McGuire mentioned that the NCRCG are holding a tabletop style workshop in early February to determine a variety of things involving responsibilities in incident management. Members of the IT SCC want to make sure NCRCG is working with ISAC on their CONOPS. They also found out the intent of the CAT team was to generate real, not simply theoretical, recommendations up the ladder. Ms. McGuire volunteered to host a meeting to discuss NCRCG in more detail.

Internet Disruption Working Group (IDWG)

(Please see slides for additional information)

The Internet Disruption Working Group (IDWG) was established to address the resilience and recovery of Internet functions. Ms. Jenny Menna began running down the recent accomplishments of the IDWG, such as conducting the information sharing assessment study in order to understand the sharing environment relationships for addressing Internet incidents. Mr. Jared Mauch asked whether the Internet falls under the domain of the Communications or IT Sector. This is an area for another possible working group to further map sectors actions. Mr. Sachs felt both sectors should continue operating under the assumption that the Internet falls under both sectors to ensure one sector was not assuming the other one was covering it.

SCADA Security Initiatives

SCADA security initiatives intend to reduce risk of control systems. They also provide guidance, develop partnerships, prepare and respond. A self-assessment tool for risk reduction is currently under development.

Strategic Homeland Intelligence Risk Assessment (SHIRA)

For the first time, the IT SCC had the chance to drive the SHIRA model this year. DHS HITRAC will soon analyze the IT SHIRA document and HITRAC will also rank and analyze the sector's risk.

Pandemic Influenza Working Group

(Please see slides for additional information)

Mr. Watson briefly explained the strategic assessment of the IT Sector's ad hoc Pandemic Influenza Working Group. The assessment is based on the following six high-level questions:

- Can your sector continue to provide your critical services if 40 percent of your staff are unavailable for work for a peak period of 1 week, and 20 percent for the remaining seven weeks of a pandemic wave?
- Further to Question above: What qualifying statements do you need to make, if any.
- Further to Question above: If not, what disruptions do you anticipate and for how long?
- Which other critical infrastructure sectors do you rely upon in order to be able to continue providing your critical services?
- What unresolved issues need to be addressed in order for you to be able to continue providing your critical services?
- Has your sector identified regulatory requirements that, if relaxed, would substantially enhance your sector's ability to continue providing critical services?

Mr. Watson said the group plans to complete its IT sector survey and finish its final sector report. The working group plans to present the Pandemic Influenza report during the PCIS quarterly meeting January 17.

Conclusion

Mr. Copeland began his closing statements after two years of chairing the IT SCC. Mr. Copeland spoke about how long ago it was when there were just a few of them starting the IT SCC. He gave an award to Mr. Robert Dix, for all of his help and effort over the years. He thanked everyone for all of their assistance and support, and handed over the microphone to the new chair Mr. Michael Aisenberg to a standing ovation. Mr. Aisenberg and Mr. Dix stood in front of the podium, and honored their former Chairman Mr. Guy Copeland by giving him an award for all he has done for the IT SCC over the years.

Mr. Aisenberg took over and noted three areas are within scope of emphasis for the new year: Sector-Specific commitments, IT SCC growth, and expanded horizons. He asked the members to trust him as their representative, and told them to not hesitate to come to him with comments and help. Below is his statement.

Chairman Michael Aisenberg's IT SCC Vision Statement

Opening

- Recognition and gratitude to Guy Copeland
- Recognize contributions of Bob Dix, Scott Algeier, and Ken Watson
 - Cross-Sector Cyber Security Working Group (Guy co-chair)
 - TOPOFF 4
 - Cyber Storm II
 - Drafting of comments on a continuing stream of documents coming from DHS (SAR, NRF and annexes, after-action reports and hot-washes)

Looking ahead: Three areas provide a framework for our objectives

1. Acting on Sector-Specific Plan commitments
2. Continuing to grow the IT Sector Coordinating Council
3. Expanding our horizons

Sector-Specific Plan commitments

- Continue work toward a baseline risk assessment
- Conduct evaluations of our own sector vulnerabilities and those of other interdependent sectors, through appropriate cross-sector channels
- Build on existing engagements to further develop reliable processes for sharing sensitive information, toward the goal of enhanced national situational awareness and coordinated incident response through a Common Operational Picture (COP)
 - Notable improvements to date:
 - IT-ISAC—(tech calls, company reps augmenting advisories, quick analyses during and post incidents)
 - ISAC Council—(regular updates, cross-sector operational awareness, pre-incident relationship management)
 - Information Sharing Policy and Strategy Working Group (ISPSWG)—Ken Watson, co-chair—direct inputs to Guideline 3 document to eliminate confusing, agency-specific Sensitive But Unclassified (SBU) markings and handling
 - Areas still needing work:
 - Joint Ops Center (US-CERT/NCC)
 - NCRCG or its successor
 - Coordination with the Intelligence Community

IT SCC growth

- Expand membership, at company and association levels
- Institutionalize private sector into national incident response
 - Exercises represent one vehicle toward this goal
 - Building private-sector mechanisms into National Response Framework is another
- Continue aggressive engagement with Communications sector, working toward:
 - Completing the collocation of the US Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center (NCC) for Telecommunications begun in October 2007;
 - Including IT-ISAC representation in the new collocated facility, evolving to a joint Operations Center;
 - Setting the goal of a combined, integrated Operations Center by October 2008; and
 - Inviting other Critical Infrastructure/Key Resources sectors to join the Operations Center by 2010
- Complete comprehensive communications plan, including
 - Promoting visibility of EC members as legitimate spokespersons for IT SCC
 - Investigating possible use of donated PR support

Expanding horizons

- Continue in established role to coordinate network security policy and strategy within the sector, across sectors, and with government agencies as appropriate, through the consistent, preferred partnership model.

Closing

- Commitment is to “steady as she goes”
- I look to you, my colleagues, for advice, direction and support in improving and refining this list of objectives and in undertaking their execution.
- Guy leaves a very big pair of shoes to fill--particularly grateful to him for his willingness to maintain a leading role in the SCC
- Immediate task: Draft annual report and forecast letter to prepare for January 25 meeting between the EC and Assistant Secretaries Garcia and Stephan ASAP

Attendees:

Michael Aisenberg - EWA IIT
Scott Algeier - SAIC
Peter Allor - IBM
Casey Ateah -
Patrick Beggs - DHS
Guy Copeland - CSC
Robert Dix Jr. - Juniper Networks
John Dragseth - SRA International, Inc.
Barry Foer - Internet Security Alliance
Liesyl Franz - ITAA
Greg Garcia - Assistant Secretary DHS
Stephen Haynes - Raytheon
John Hopkinson - ISSEA
Tiffany Jones - Symantec
Larry Kettlewell -
Clint Kreitner - The Center for Internet Security
Joey Lauffer - SRA International, Inc.
John Lindquist - EWA IIT
Jared Mauch - NTT USA
Cheri McGuire - R&H Security Consulting, LLC
Angela McKay - Booz Allen Hamilton
Lynn McNulty - ISSA
Jenny Menna - DHS/NCSD
Rama Moorthy - Hatha Systems LLC
Angela Morgan - EWA IIT
Nicholas Murray - SRA International, Inc.
Jon Noetzel -
Andy Purdy - DRA Enterprises Inc.
John Sabo - ISTPA Inc.
Marcus Sachs - Verizon
Howard Schmitt - R&H Security Consulting, LLC
Phyllis Schneck - Secure Computing
Bryant Tow - Unisys
Chris Turner - CompTIA
Ryan Walters - Northrop Grumman
Ken Watson - Cisco Systems
Edward White - McAfee
Brian Willis - Intel