

INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL QUARTERLY MEETING MINUTES

June 28, 2006

Introduction to the New Secretariat

The IT SCC coordination responsibilities are leaving Meridian and moving to the George Mason University (GMU) Critical Infrastructure Protection (CIP) Program's Private Sector Program (PSP). As part of the transition process Meridian is going to be reducing administrative support with the exception of to the Plans Working Group.

Kathryn Condello of GMU introduced the CIP Program, which consists of two parts: One primarily research-oriented, and the other being the Private Sector Program. PSP currently supports seven sectors: Oil and Natural Gas, Commercial Facilities, Food and Agriculture, Dams and Levees, Water, Healthcare, and now Information Technology. Larry Clark will be the IT primary representative and James Creel will be the secondary. Virtually all the meetings that PSP hosts take place at GMU. Additionally, the IT SCC will have full access, through the GMU PSP relationship with PCIS, to virtually every other sector. Although PSP is funded through a DHS contract, SCC minutes and information are not given to DHS, with the exception of noting that a meeting took place, unless the SCC requests PSP to do so.

Report from the Executive Committee and Business

Introduction of David Barron – In accordance with the charter the organization/company that provided an outgoing member may name their substitute to the Executive Committee. David Barron will replace Cristin Goodwin (BellSouth). He was also recently elected as Chairman of the Communications SCC.

New SCC Members – The Executive Committee recommend for membership, subject to approval by the full Membership: Bearing Point (J.R. Reagan with Mark Fabro and Joe Albaugh), TestPros, Inc. (Kevin Murray); System 1, Inc. (Barbara Gorsen with John Abeles and Steven Senz). John Sabo motioned to approve; Ken Watson seconded. The new members were unanimously approved by the Membership.

New IT SCC logo – The motion to accept the new logo was unanimously carried. A question was raised on what to do about trademarking. The Executive Committee will pursue whether to register the logo. Michael Aisenberg will look at trademark registration requirements.

Follow up on CIPAC concerns – The Executive Committee was pleased to receive confirmation that SCC members are not just owners and operators and that the SCC can establish its own requirements for membership. There was also concern that the CIPAC charter was written in a way that was problematic, having a lack of transparency because it was written without consultation with the private sector; it would have been better to have parallel requirements. Currently the SCC cannot grant membership and have new members automatically become members of CIPAC. As it stands, the government gets additional review. Michael Aisenberg related that Carlos Kizzee of DHS's Office of General Counsel, who is assigned to work with the private sector, indicated that DHS will revisit the CIPAC charter.

GAO Request for Feedback – The IT SCC had a second round of questions from the GAO, which were handled through a conference call. The SCC communicated to the GAO the concern that significant groups within DHS that are not familiar with the sector and are making inappropriate requests and approaching people who are not actual representatives of the sector. Both parties felt the all was positive.

Joint SCC/GCC Meeting – The Executive Committee has planned the first joint SCC/GCC meeting and is currently coordinating a number of documents for the meeting.

The Executive Committee provided input on the DHS Preparedness Directorate which has been shared with the membership.

The Nuclear SCC shared its draft SSP with the IT SCC. Members who wish to see it may request it from GMU.

PCIS Exercise Letter – PCIS is drafting a letter to DHS regarding exercises. The letter seeks clarification on DHS’s practices regarding exercise participation, especially who it reaches out to in the private sector and how. (The request for SCC participation in the TOPOFF 4 tabletop exercise was late.)

The SCC raised a concern regarding other exercises being planned in other sections of DHS that members of the private sector may not be aware of.

Pandemic Planning – The SCC has identified a team to work with the National Infrastructure Advisory Council’s (NAIC) Pandemic Planning. Ken Watson is actively engaged within the NIAC for the IT SCC’s effort. The groups most likely to be impacted first by pandemic flu are those with fielded products and services.

Coordination with the Communications SCC – The IT SCC has been engaged with colleagues in the Communications SCC. A quick update on Communications...Last week the Comms SCC elected officers and approved the SCC charter. From a priority standpoint, the task of the Communications SCC is to obtain SCC-wide input on the SSP. It will also review the NIPP to see how that document reflects the input other sectors have given. The Comms SCC already has a private sector draft of the SSP and is on target for meeting the deadline. However, Comms would like to coordinate with the IT SCC. Currently the Comms SCC plans to move from reactive to proactive and is trying to undertake projects that bring value to the sector. It is working on team building exercises similar to the one held in Maryland on issues such as access procedures and credentialing. Another task for the Comms SCC is to secure a broader base from within the communications sector.

Guy Copeland asked the membership if anyone did not want to move forward on planning and conducting a joint meeting annually for the IT SCC, IT GCC, Comms SCC, and Comms GCC. There were no objections.

The SCC previously received a copy of the “Rules of Engagement” from the government regarding GCC/SCC contact.

IS SCC Website – Work establishing the website is progressing. The goal of the website is to keep SCC members fully informed of sector issues and events. Members are encouraged to share information with the rest of the membership by the most appropriate means. If information is timely or short-fused, a member may send information out through the membership mail list. If the item is substantial, it should be forwarded to GMU for posting on the website.

Issues to Address in the Future – The IT SCC needs to discuss expanding membership. Guy Copeland has been developing a list of companies and organizations (currently about 190) that are involved in the IT sector. Not all of those on the list are high priority, but some should be represented on the SCC. Some help may be needed to identify those small companies that do not always show up on lists, but play a critical role in the sector. Mr. Copeland will be sharing the list with the Executive Committee and then the general membership. He will also be sharing it with the IT ISAC.

Decided amendments to the Operating Charter need more maturing within the Executive Committee before raising them with the general membership.

The Executive Committee is considering holding an Executive Committee/Working Group Chairs retreat within 30-60 days to focus on what the IT SCC should be doing and bring those ideas back to the general membership.

The IT SCC has been building a strong relationship with the Sector-Specific Agency – DHS’s National Cyber Security Division (NCSA).

Regarding education and outreach, the IT SCC potentially needs to start reaching out to congressional staff, especially those that are taking an interest in cybersecurity, to ensure that they are aware of the SCC’s existence.

Report from the Communications, Nominations, and Membership Working Group

(Jared Mauch and Tiffany Jones, Co-Chairs)

Half of the Executive Committee’s membership coming up for election and the working group will be involved in the elections.

A major task of the group is working on IT SCC communications plan. The plan will cover both internal and external communications. There have been some initial conversations with DHS on how the agency wants to be folded into the communications plan.

The Membership Committee needs some information to give new members. Additionally, the working group needs from all members; first and second point of contact, a public relations point of contact, an operations point of contact, and what working groups the member wants to participate in.

The group discussed a possible “road show” to socialize the draft SSP with sector representatives and to receive direct feedback. A road show might also be a useful tool for recruitment to the IT SCC. It could be coupled with a West Coast SCC meeting. The NOVA tech corridor, Silicon Valley, Austin, and Boston (I-495 Tech Corridor) were also mentioned as potential road show destinations. Other ideas for socializing the SSP included engagement with the FBI’s InfoGuard program and publication in the Federal Register.

Report from the Strategy Work Group and IT SCC Budget Planning (Working Lunch)

GMU will provide space for Executive Committee and full membership meetings, and working lunches for full membership all-day meetings. Costs for food/refreshments for other meetings, working group spaces, etc. would have to be borne by the participants.

The Working Group presented a draft three-year budget (the numbers are all estimates):

Year #1 will cost approximately \$62,000; and

Years #2 and #3 will cost approximately \$49,000 each.

The IT ISAC (through Internet Security Services – ISS) has donated all the time for the development of the website. They are willing to continue to do so, but for a more capable site the SCC may need to pay for some services, features, and capabilities.

The Working Group is proposing an annual sponsorship model with two levels (\$5,000 & \$10,000). Sponsors would be listed as “founding member” on certain materials. In addition, the \$10,000 sponsorship level lets members host meetings to cut down on travel costs. Sponsorship does not get members extra votes; and those members do not get automatic seats on the Executive Committee.

Further discussion centered on the following issues and points:

- Who would sponsor/contributor checks be made out to since the SCC isn't a legal entity?
- The need to clarify the benefits of joining the SCC and for being a sponsor, including underwriting credit on the website.
- Consideration should be given to multiple sponsors for the road show.
- Other SCCs supported by GMU are not pursuing sponsorship concepts at this time.
- Are there opportunities to raise funds at levels less than sponsorship?
- The need for a short document for the membership to look at before adopting a sponsorship model, which could also function as the draft for a general SCC information document.

Mr. Algeier will mail out a revised presentation as support for the sponsorship model, and noting that some work is needed to more fully develop a sponsorship proposal, he asked the Chair if a special meeting could be held to vote on the revised proposal.

Mr. Copeland reminded the SCC that sponsorships would be voluntary. He suggested the Membership give authorization to have the Executive Committee work with the Strategy Work Group on the proposal.

Report from the Plans Working Group

(Paul Kurtz – Co-Chair)

The Working Group would like members to walk through the plan and provide line-by-line corrections, as appropriate.

- Operating Principles – The working group has been working closely with government counterparts on this portion of the plan.
- Sub-Groups and Chairs – For each sub-group a private sector individual and a government representative will work together as do-chairs.
- Outline Highlights – Regarding the context of the IT SSP, with consumers and enterprise security on one side, and national security on the other. The group is trying

to focus where these come together – situational awareness, risk management, emergency response and communications mechanisms, and recovery and reconstitution.

- The group’s mission is to look at the availability of the information structure overall -- not trying to get into those discrete national security spaces.
- The IT Sector Definition should not be new to anyone as it is more or less taken from IT SCC Charter.
- The internet definition was drafted to acknowledge the IT Sector has very close relationship with the Communications Sector.
- Risk Management will describe a top down process. The group is taking more of a functionality approach than an asset approach. The plan is focused on what are perceived as sector security goals and takes a qualitative as opposed to quantitative risk assessment approach. The high-level goal of the plan is to advocate risk management technologies. The Plans Working Group is also planning to put a survey on the website for the SCC membership in order to collect information on methodologies that are in use. The plan is to put a questionnaire on the website for members to fill out. This should allow identification of current methodologies, their common points, and differences
- The Protective Programs section includes situational awareness, emergency response, reconstituting cyber assets, etc. This is an important area for the GCC partners.
- Information sharing and protection is a description of mechanisms and processes.
- The Research and Development section is almost in final draft form.
- The Managing and Coordinating Responsibilities section describes the overall approach to coordinating IT Sector responsibilities.
- There will be appendices on authorities and the decision-making process.
- A working group cyber incidents of national significance (CINS) has formed.

The number one priority is that the SSP be an unclassified document, although there may be plan elements that require more protection.

The SSP will be reviewed once a year to determine if updates are needed. The SSP is not meant to be static; it is meant to be a useful working document and should have an on-going life that reflects the practical needs of the sector.

When the plan is promulgated it can be included in relevant portions of government guidance and other documents.

Development Timeline

- July 14: Comments on the annotated outline are due.
- August 11: Circulate first draft of the SSP
- September 21: Circulate second draft of the SSP.
- November 2: Circulate final draft of the SSP
- November 22: Finalized SSP.

Introduction to the IT SCC Website

The original plan was for the SCC to develop a public website. However, the site, in its present form, stems from the short-term need to support SSP development. The site shown to the membership is a hybrid and will grow to accommodate more than the SSP.

Since the last discussion was in April, the IT ISAC went ahead and purchased the domain names for the SCC. The site is using the ISAC certificates.

GMU will validate the authentication of users for the site (Meridian has validated work group members). The site managers would like GMU to gather the requirements for the site, and keep the site development on track.

The IT ISAC site has four public areas: General Member, Tech Member, IT SCC Member, and IT GCC Member. Users need a certificate to log onto the appropriate areas of the site and to access documents.

The annotated SSP outline is a flat file type page and shows latest outline. In the future there will be a separate page to allow comments for specific sections (change, delete, add, and reason). Adjudication of comments will be done by the core writing team, but no comments will post to the site until adjudicated.

The site will also have a calendar view with meetings. Users will be able to filter calendar views according to their needs. Currently a static SSP calendar is posted.

Follow-up on Issues Raised at the May 12 Joint SCC/GCC Meeting

Access to classified information. HITRAC (Homeland Infrastructure Threat and Risk Analysis Center) is beginning to invite private sector participation. This might open up the possibility for credible analysis that can be shared and which requires only a “For Official Use Only” designation. Other comments and questions included:

- Will there be regular threat briefings for industry?
- There are two separate issues concerning sharing of threat information. The first is getting clearances for the people who need them. (Chris Watson is the person to talk to.) The second issue is having classified briefings on sector-appropriate subjects.
- A participant commented he would hope that sometime in the future DHS would include sector representatives in after-action briefings and discussions.
- There is still confusion over handling requirements for “Sensitive But Unclassified” (SBU) and “For Official Use Only” (FOUO) information. The private sector should really think of it more as a mark indicating handling restrictions, but which offers no intrinsic protection whatsoever. As soon as one of these documents is sent outside the government those SBU categorizations becomes unenforceable.
- Is there value in the SCC helping to develop time/content of Essential Elements of Information (EEI) – perhaps situationally based too?

Other comments on the May 12 meeting include:

- Coordination of the NIPP roll-out depends on release of the NIPP.
- The government has shared the GCC rules of engagement. At the joint meeting the GCC asked for suggestions of other government agencies that should join the group.

- The Treasury Department requested the IT SCC review the Financial and Banking Sector’s research and development agenda. GMU will send a reminder to membership to review the document.
- Currently the research and development group is focusing on the SSP, but are recommending a group be established that lives beyond the SSP.
- There is a need to share information on government protective programs regarding IT.

Next Joint Meeting – The SCC wants to plan a combined IT SCC, IT GCC, Communications SCC, Communications GCC meeting. A possibility is January in Tampa when IT ISAC has its annual meeting.

The joint meeting will be pursued further in the Executive Committee.

Should the next meeting focus cyber or physical threats to the IT sector?

- There was a comment that we are already embedding a lot of physical information. The participant thinks the SSP is an all-risk approach.

Action Items

20060628-01: Determine if the IT SCC should register the logo. Assigned to the Executive Committee.

20060628-02: Investigate trademark requirements for registering IT SCC logo. Assigned to Michael Aisenberg.

20060628-03: Regarding the PCIS letter to DHS dealing with exercise coordination – To which level at DHS should the letter be addressed to? Assigned to Guy Copeland and Michael Aisenberg.

20060628-04: Establish the appropriate way to approach George Foresman regarding positive aspects of the IT SCC relationship with the government and IT SCC concerns regarding the proper way for the government to approach the private sector. Assigned to Executive Committee.

20060628-05: Begin planning a joint IT SCC, IT GCC, Communications SCC, and Communications GCC meeting. Assigned to the Executive Committee.

20060628-06: Plan an Executive Committee retreat to take place within 30-60 days. Assigned to the Executive Committee.

20060628-07: Plan a series of “road shows” to socialize the IT SSP, raise the IT SCC’s profile, and potentially solicit contributions. Initial target dates in September. Assigned to the Communications, Nominations, and Membership Working Group.

20060628-08: Send out a revised funding proposal package with supporting documentation to the membership for review and comment. Assigned to Scott Algeier.

20060628-09: Finalize the financial support model prior to the next quarterly meeting. Assigned to the Executive Committee and the Strategy Work Group.

20060628-10: Provide relevant portions of the National Strategy to Secure Cyberspace, HSPD 7, HSPD 8, and other supporting documentation along with the SSP. Assigned to Paul Kurtz and the Plans Work Group.

20060628-11: Set up a meeting with the Business Roundtable (BRT) to discuss their cyber terrorism readiness report. Assigned to Executive Committee.

Sector Coordinating Council Participants

Valerie Abend, KPMG (*via telephone*)
Michael Aisenberg, VeriSign
Scott Algeier, IT-ISAC
Peter Allor, Internet Security Systems
David Barron, BellSouth Corporation
James Bean, Verizon
Judy Bedmar, DOD CIO
Bruno Bottcher, EWA/IIT
Larry Clinton, Internet Security Alliance
Jerry Cochran, ISSA
Guy Copeland, IT-ISAC
Robert Dix, Citadel Security Softwear
Greg Garcia, ITAA
Mike Gibbons, Unisys Corporation
Barbara Gorsen, System 1
John Hopkinson, ISSEA
Tiffany Jones, Symantec
Canning Kraft, EWA/IIT
Paul Kurtz, Cyber Security Ind Alliance
John Lindquist, EWA
Jared Mauch, NTT America
Paul Nicholas, Microsoft Corporation
Franklin Reeder, Center for Internet
Security
Phil Reitinger, Microsoft Corporation
John Sabo, ISSEA
Lucy Thomson, CSC
Tim Vogel, Verizon
Ken Watson, Cisco Systems
Brian Willis, Intel Corporation (*via
telephone*)

Government Coordinating Council

Observers

Marcia Fagan, BAH
Lieysl Franz, DHS
Hun Kim, DHS
Cheri McGuire, DHS
Angela McKay, DHS
Andy Purdy, DHS
Jordana Siegel, DHS
Christina Watson, DHS

Support

Kevin Bryan, Meridian Institute
Josephine Burton, George Mason
University
Brett Callahan, George Mason University
Larry Clark, George Mason University
Kathryn Condello, George Mason
University
Molly Mayo, Meridian Institute
Kim Morgan, George Mason University