

**Improving Cybersecurity**  
**CSIS Center for Strategic and International Studies**  
March 12, 2008

**Summary of remarks**

**Guy Copeland**

**Vice President, Information Infrastructure Advisory Programs**

**Computer Sciences Corporation**

**gcopelan@csc.com**

**Introduction**

*My thanks to our moderator, Howard Schmidt, CSIS and CSIS' Jim Lewis and the Commission on Cybersecurity for the 44<sup>th</sup> Presidency and its Co-Chair, Harry Raduege, for inviting me here to offer my views and suggestions for consideration. I wish to be clear that while I have recently completed a two year term as Chairperson of the Information Technology Sector Coordinating Council, and I work for Computer Sciences Corporation, my remarks today are my own and do not necessarily reflect the opinions of either of those two organizations or any of the other groups with which I am associated. However, my opinions are formed by my experiences in those organizations and the many fine people I have been pleased to work with in them.*

*The next President of the United States and his or her administration will face a seemingly endless list of daunting challenges as they take over the reins of government. Cybersecurity has not been high on the list for past administrations but that should be and is changing. Like all past successful technologies, as we embrace and proliferate them we grow ever more dependent on them for our national security, economic security, safety and virtually every other aspect of our daily lives. That very dependency is a lucrative target to anyone seeking to do harm or take advantage of us. Recent public news reports show growing concern that massive intrusion and exfiltration of government and private sector information has already taken place, in addition to exploitation on large and increasing scales for criminal and other purposes. This administration realizes the danger and the need to work with the private sector to find and implement practical solutions. The next administration will inevitably need to do even more.*

**Environment**

Consider the environment in which we face the challenge of cyber security. The Internet is what we commonly focus on but the total environment is far more complex than just the Internet and includes

- the collection of networks which openly cooperate in the Internet and
- the traditional telecommunications networks,

which are both huge and international in scope. But it is even much more than that. It also includes

- the computers, embedded processors and other devices (e.g., SCADA devices) accessible via networks,
- wired, optical and wireless systems,
- huge scale of the legacy installed base,
- complexity in numbers and configurations,
- increasing and often critical interdependencies between cyber and physical,
- increasing numbers and sophistication of applications,
- increasing number and sophistication of attacks and exploits,
- dependence on human beings for systems and enterprise design, installation, operation, maintenance and upgrades,
- dependence on human beings for compliance with policies and procedures in every aspect in which they play a role,
- the terrible compliance and error rates associated with human beings,
- the time phased nature of legacy systems replacement,
- affordability issues,
- international scope of virtually all aspects,
- immature legal frameworks, national and international,
- legislative initiatives that appear out-of-synch with real issues and focused more on an issue-of-the-day reaction,
- government and private sector relationships that are traditionally forced to comply with regulations and rules for either or both an acquisition relationship or a regulatory relationship but do not contemplate or support a partnership of equals,
- corporate general counsels who generally do not understand cyber risk and thus tend to advise against external sharing and collaboration in order to reduce potential liability or other risks they do understand,
- the toughest aspect to define and manage: the culture, which in many respects tends to be highly independent, organizationally protective, individually disdainful and often in denial of either a serious problem or a need for external help,
- and much, much more

The bottom line is it is complex. There are policy, technical, business (or mission) and human factors issues to challenge the best and brightest among us. A near-term, “silver bullet” solution is not likely. The “solution” will be a constantly evolving and complex mix of policy, technology, training, monitoring, feedback, analysis and adjustment, applied with sound experience and informed judgment in a risk management framework.

## So What Are We Doing

There are a number of important efforts or developments under way. Here are just a very few examples:

- There are a large number of professional membership organizations, associations, government bodies and treaty organizations that are active. They include, for example, ITU (International Telecommunications Union), IETF (Internet Engineering Task Force), FIRST (Forum of Incident Response and Security Teams), ISSA (Information Systems Security Association), the SANS Institute, NANOG (North American Network Operators' Group), ISA (internet Security Alliance), ITAA (Information Technology Association of America) and many more.
- Under the National Partnership Model for Critical Infrastructure Protection sectors have formed Sector coordinating Councils. In particular, the Information Technology Sector Coordinating Council (IT SCC) and the Communications Sector Coordinating Council (CSCC) have developed sector specific plans and are doing sector risk assessments, as are the rest of the 17 (or so) critical infrastructures
- The Partnership for Critical Infrastructure Security (PCIS) and the Department of Homeland Security have organized the Cross Sector Cyber Security Working Group (CSCSWG) made up of over 90 representatives from all the Sector Coordinating Councils and their counterpart Government Coordinating Councils. It is chaired by DHS Assistant Secretary Greg Garcia, Stuart Brindley, a Canadian who represents the electric power sector, and me, representing the information technology sector.
- The Information Technology Information Sharing and Analysis Center (IT-ISAC) is collaborating across most of the 17 sectors and, in particular, is working with the National Coordinating Center for Telecommunications (NCC) and the United States Computer Emergency Response Team (US-CERT) to strengthen information sharing and operational collaboration.
- Private sector representatives are participating in federal government exercises more than ever before. For example, they are part of the Cyber Storm II exercise taking place this week.
- Private sector representatives are meeting with government counterparts in a trusted environment to find better ways to turn classified threat information into useful, credible, actionable, unclassified information for private sector operatives, and
- Market forces are at work

## What More Could Be Done

Certainly it would help tremendously if we could go back and rebuild this environment, knowing what we know today. And eventually, we will replace legacy systems, protocols, processes and other elements with better thought through, better designed, better tested, better configured, better managed and maintained replacements. But that isn't going to happen fast and we have problems right now. So we need some things to do that are practical, affordable and relatively fast.

Thankfully, we are not the first to consider this challenge and some solutions have been developed and recommended in the past. Unfortunately, they were either ignored or deemed unnecessary. I suggest they are worthy of serious reexamination for potential near-term (i.e., the 44<sup>th</sup> President's administration) implementation. In particular, I have two to recommend. They are specific and could be implemented in reasonable time by any administration that wants to do them. They probably won't solve every challenge but they will help tremendously.

### 1. National Crisis Coordination Center

The first recommendation is focused on immediate improvement of our operational preparation and responsiveness. It was a recommendation of the Early Warning Task Force, an industry led coalition of interested security experts from the public and private sectors created as part of the National Cyber Security Summit held in Santa Clara, California on December 2-3, 2003. The recommendation was later repeated in substantially the same form by the President's National Security Telecommunications Advisory Committee (NSTAC) in a report on Next generation Networks. The recommendation is to create a government funded, National Crisis Coordination Center to:

- House government, industry and academic security experts, both physical and cyber (because they are so intertwined in the real world), to bridge the cultural barriers that have hampered a true partnership in counterterrorism and cyber security,
- Start initially with the "millisecond sectors" (information technology, communications and electric power) and build out quickly to include resident member experts from all critical infrastructures and government counterparts,
- Jointly prepare, exercise, evaluate and update National Joint Crisis Response plans to prevent, detect and respond,
- Operate joint watch centers,
- Conduct joint exercises at the national level to train and test the plans

- Conduct joint field training at the regional level to train and further test the plans,
- Respond jointly to traditional natural events, as well as malicious events, physical or cyber,
- Include a secure, compartmented intelligence facility staffed equally with government and private sector representatives, as well as appropriate state, local and other representation, all with clearances to proactively share intelligence – both national security and law enforcement – and perform fusion center functions,
- Proactively address priority remediation of systemic vulnerabilities in national level infrastructures, and
- Quickly evolve to include international liaison (as, for example, the Joint Task Force for Global Network Operations (JTF-GNO) includes Canadian liaison today),
- Updates to the original recommendation may be appropriate in today’s environment. For example,
  - o government should be willing to pay a fixed stipend to entities contributing expertise to partially defray their costs
  - o a Congressional charter (under Title 17) should detail the roles and responsibilities of the NCCC and provide the authority. [Note: this is similar, for example, to the Congressional Charter of the American Red Cross for the inherently federal functions which it performs in disaster response activities.]
- Requirements for participation should be formally agreed and include qualifications, duration, clearances, nondisclosures, etc.
- Governance, including mandatory ethical rules, must be established and documented for all participants, based on true partnership principles, and not simply invoke rules and regulations derived from acquisition and regulatory relationships, even if a legislative waiver or exception is required.

The trusted relationships that can be developed in such a facility are critical to

- collaboration in a fast paced crisis response,
- full and open sharing of sensitive information, and
- to develop fully informed plans and responses

## **2. Information Systems Security Board**

The second recommendation is focused on providing an authoritative structure for codifying, evolving and using informed expert judgement to apply known standards, practices and other criteria for cybersecurity. Congress has legislated the responsibility for Federal computer security standards and guidelines to the National Institute of Standards and Technology (NIST) and the National Security

Agency (NSA). There is no analogous information systems security focal point for the private sector. The need for such an organization was identified by the National Research Council (NRC) as early as 1991. The Information Systems Security Board (ISSB) was a recommendation of the President's National Security Telecommunications Advisory Committee in 1996, aimed at meeting that need. It represented the first major recommendation of the NSTAC which envisioned private sector implementation rather than government implementation. At that time, government saw a need but saw no reason for government to fund it. Unfortunately, it was well before its time and no organization in the private sector took up the challenge to organize the ISSB. Interestingly, major private sector end users who were briefed on the concept supported it whole heartedly.

The ISSB was proposed to perform the following functions for voluntary use in the market place:

- Evaluate and endorse information systems security standards and practices and evaluation/testing criteria developed by the standards community or other recognized bodies, including international bodies.
- Develop or endorse testing criteria.
- Develop and maintain information systems security principles (ISSP).
- Identify areas in which information systems security standards are lacking and new standards need to be developed, working with the standards community to initiate development.
- Develop rating criteria to identify varying levels of security.
- License testing laboratories and auditing organizations to use the ISSB logo and ratings to identify that a product or system meets ISSB endorsed standards, practices and other criteria for the intended type of application or environment. The license would be issued based on application and proof of competence.
- Enhance the understanding of information security issue solutions and promote the use of ISSB endorsed standards and methodologies.
- Issue technical notes to license holders, product developers, and the standards community.
- Establish a process to adjudicate ISSB rules, testing results, and auditing determinations appeals.

The situation has changed radically since 1996. Government has national and international interests to protect and needs voluntary private sector cooperation and collaboration to achieve them for cybersecurity and homeland security generally. Accordingly, updates to the original recommendation are appropriate in today's environment. For example,

- Government should fund the startup for an updated ISSB
- Government should provide incentives for major "cyberspace" players to support and participate actively in the ISSB.

- A Congressional charter (under Title 17) should detail the roles and responsibilities of the ISSB and provide it with authority and accountability. [Note: this is similar, for example, to the Congressional Charter of the American Red Cross for the inherently federal functions which it performs in disaster response activities.]

## **Discussion and Questions**

Clearly the recommendations I have briefly described have significantly more detail behind them and would require more discussion in today's environment to fully understand them and update them.

I welcome questions and further discussion toward that end.

## **Postscript**

Finally, I would be remiss if I did not note that research and development has been mentioned often here today. For those who are interested, I Chair the R&D Task Force of the NSTAC. We are planning for our next R&D Exchange Workshop at Motorola's campus in Schaumburg, IL, September 24-26, 2008. For those who have not attended previous RDX's, they are a unique format that brings together industry, academia and government participants at the senior executive, mid-level management and hands-on practitioner levels. That mix of viewpoints allows them to look at some current pressing issues for communications and information technology, R&D and deployment, from literally all vantage points and – working through breakout sessions – allows them to make cogent, actionable, timely recommendations to senior government resource and program decision makers. In past RDX's, the senior attendees have literally requested for their immediate use in pressing decisions, the power point slides used by breakout sessions to report back to those seniors and the plenary. If you would like additional information or would like to participate in the preparation for this next RDX or attend it, please contact me.