



Cybersecurity Advisory Committee

Tuesday, August 21, 2012 10:00 a.m.
Speaker's Conference Room, 6th Floor, General Assembly Building

The first meeting of the Cybersecurity Advisory Committee of the Joint Commission on Technology and Science was held on August 21, 2012. Advisory Committee members present were Delegate Tom Rust (chairman), Senator Mamie Locke, and Delegate John Cosgrove.¹ In addition to the legislative members of the Advisory Committee, citizen members from the private sector, local governments, and the Commonwealth's institutions of higher education were present and actively participated in the Committee discussions.

Delegate Rust called the meeting to order. He noted that cybersecurity issues were ripe for discussion and that the goal for the Advisory Committee was to gain an understanding of those issues and to look to the citizen members and the public to help develop possible solutions.

Staff provided a brief overview of proposed federal legislation related to cybersecurity. There is broad support for cyber legislation. The President, Congress, the intelligence community, and many members of the private sector are in support of and working towards legislation to address cybersecurity issues. While several different approaches have been proposed, they each include a mechanism for information sharing between the federal government and the private sector. This information sharing is the key to protecting against cybersecurity threats, but it does raise some privacy concerns. Three particular bills of note are the Cyber Information and Security Protection Act (CISPA), the Cybersecurity Act of 2012 (CSA), and the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act (SECURE IT). While Congress was not able to pass cybersecurity legislation before going to recess, future action is likely.

The Advisory Committee noted that the federal government has gaps in its knowledge of threats and hopes the private sector can fill those gaps. The goal of any legislation is to protect critical information and infrastructure. Cybersecurity threats are not just from individuals but are coming from other governments. In addition to the federal government and large corporations, state and local governments and small businesses are also targets of cybersecurity threats. Cybersecurity threats are not always disruptive and the target may not know it has been attacked.

¹ Senator Stephen Martin and Delegate Bob Purkey were not present.

Cameron Kilberg, Assistant Secretary of Technology, provided an overview of the Governor's Cybersecurity Initiative. The Governor has a number of current initiatives and future goals related to cybersecurity. One such goal is to develop the concept of cyber minutemen. The minutemen would be a taskforce designed to maximize the security of the Commonwealth by acting as first responders in case of cyber emergency. The Advisory Committee noted that while there are many challenges in implementing this concept, the task force could prove beneficial for evaluating threats and coordinating responses.

The Assistant Secretary highlighted a number of educational initiatives related to cybersecurity. Currently the Governor has created a Cyber Challenge for Virginia High School students. Participants take a series of cyber related tests and the top scorers go on to participate in an interactive learning environment competition at George Mason University. The Advisory Committee noted that all secondary students need to be well versed in cyber "hygiene," and that students interested in cyber related careers would benefit from simulators and internships in the private sector.

David Ihrle, Chief Technology Officer, and Kent Murphy, Entrepreneur-in-Residence, both of the Center for Innovative Technology (CIT), gave an update on CIT's cybersecurity initiative. CIT's goal is to foster new growth of cybersecurity companies in the Commonwealth. CIT hopes to achieve this growth by understanding the market and the Commonwealth's cyber assets, find ways to improve efficiencies in both product development and cybersecurity response, to support leaders in cyber related business growth.

Throughout the presentations and discussion the Advisory Committee was particularly interested in the Commonwealth's current cybersecurity status. The Committee wanted to know how does the Commonwealth compare to other states, how does it test itself, and what are the risks and standards associated with protecting Virginia's cyber assets? Beyond the details, the Committee wanted to know the broader vision for the Commonwealth's goals for cybersecurity.

The meeting was adjourned. The next meeting is scheduled for October 16, 2012 at 1:00 p.m. in the 6th Floor Conference Room of the General Assembly Building.