Cyber Security Commission
Inaugural Meeting

June 11, 2014
Mason Inn and Conference Center
4352 Mason Pond Dr. Fairfax, VA 22030

Chairs:

Richard Clarke, Chairman and CEO, Good Harbor Security Risk Management
Karen Jackson, Secretary of Technology

Members Present:

Rhonda Eldridge, Director of Engineering, Technica Corporation
Jennifer Bisceglie, President and CEO, Interos Solutions, Inc.
Paul Kurtz, Chief Strategy Officer, CyberPoint
Paul Tiao, Attorney and partner, Hunton and Williams, LLP
Barry Horowitz, Munster Professor of Systems and Information Engineering and Chair, University of Virginia
Andrew H. Turner, Vice President and Head of Global Security, VISA
Jeffrey C. Dodson, Global Chief Information Security Officer, BAE Systems
Jandria Alexander, Principal Director of the Cyber Security Subdivision in the Engineering Technology Group at the Aerospace Corporation
Elizabeth Hight, Retired US Navy rear admiral
John Wood, CEO, Chairman of the Board, and Director, Telos Corporation
Maurice Jones, Secretary of Commerce and Trade
John Harvey, Secretary of Veterans and Defense Affairs

Guests in Attendance:

Sam Nixon, CIO, VITA
Michael Watson, CSIO, VITA
Dave Burhop, CIO, VDOT
Admiral Bob Day
Josh Heslinga, Office of the Attorney General
Jonathan Couch, iSight
Evan Sills, Associate, Good Harbor
Kelly Thomasson, Deputy Secretary of the Commonwealth
Zaki Barzinji, Special Assistant for Policy

Minutes

9:12 Governor's remarks

9:15 Call to order by Karen Jackson

Comments from Peter Stern, GMU Provost

- Welcomes Commission and offers any support GMU can provide

Opening comments from Richard Clarke, Commission Co-Chair

- Goal: Attract cyber security companies to the state and increase security at state level
- Emphasis on the need for a secure network and trained workers to fill workforce needs

9:20 Introductions from Commission members

9:30 Swearing-in of Commission members by Kelly Thomasson

9:32 iSight presentation by Jonathan Couch

- Mission: be the world's leading global cyber threat intelligence provider connecting security technology and operations to business
- Must know the battle you are fighting: intent of cyber attacks, how hackers target companies and data, be able to forecast future problems
- Challenge: expanded surface area for attack
- Not all adversaries as advanced as we think, but they are quickly adaptive. Low barriers to entry, will use whatever technology works. Tools to hack systems are readily available
- Types of cyber threats:
    - Cyber crime – Closer to traditional forms of crime, eg. identity theft for purposes of stealing money
    - Cyber espionage – intellectual, information-based eg. selling PII
    - Hactivism – advancing a philosophy; form of protest or revolt eg. Anonymous
    - Destruction of infrastructure – can be using traditional, physical means of attack or digital eg. installing a virus
- Threat data vs. threat intelligence
    - Data about domains, IP addresses, or URLs is not useful without analysis
    - With analysis and context, we can move from data to actionable intelligence
    - Should have multiple analysis methods
- Recommendations:
    1. Be proactive
        a. Obtain the right technology and the right people to effectively obtain and analyze cyber data

2. Shrink the problem
    a. Focus on threat sources, rather than the customer side
3. Improve prioritization
4. Enhance executive communication with the rest of the organization
    a. Address concerns, such as feeling of security using service after a data breach
5. Connect security interests to business interests
    a. Translate geek speech

- Intelligence-led security paradigm shift: from technology-driven to threat-led decisions
- Threat examples
    - Confluence of cyber espionage and cyber crime
    - Point of sale malware – eg. incidents at Neiman Marcus and PF Chang's
    - Use of social networking in cyber espionage – LinkedIn is particular risk, as designed to link people who don't know each other
    - Hactivism – eg. in Ukrainian conflict
    - Critical infrastructure – including water, electrical, financial, etc.

9:47 Group picture with Governor McAuliffe

10:05 Working groups discussion

- Proposed groups:
    - **Internal Infrastructure Security**
        - Proposed public/private sector split
    - **Leveraging VA Assets to Drive Economic Development**
        - How can an environment be created to encourage companies to come to VA?
            - NY is example – look at changes they have made eg. targeted tax breaks
    - **Education and Workforce**
        - How can we create a workforce that is capable of filling jobs in IT, Technology, Cyber, etc?
            - Look beyond 4 year degrees to include community colleges and even high schools
    - **Cyber Hygiene**
        - Public and government awareness of cyber issues and best practices
        - Educating the public about how to protect themselves online
            - Issue: how deep will we delve into this topic? Is this in the scope of what we are trying to accomplish?
            - Are media advertisements a feasible way to increase

awareness?
        - Possibly include cyber bullying, protection of children on the internet
- Discussion
    - What constitutes threats to state agencies and systems? Understand motivations, targets
    - Is legal system equipped to handle cyber crimes – with appropriate statutes, educated prosecutors?
        - Citizens need contact for low-end threats
    - Study leading states and their best practices
        - Leaders: NY, California
        - VA spent $1 million vs. $4 million by MD
        - But also need to think creatively if seek to become innovator
    - Use of universities, state agencies, and private sector groups as resources
        - Send letters introducing the commission, inviting them to send data and resources they already have collected. Ask what research or action in the cyber field they are already engaged in
        - Emphasize link with different domains eg. health care, energy
- Functioning of groups
    - Commission members should send group preference. Each group will have chair and 3-4 members total
        - Maurice Jones volunteered as Chair of Economic Development
        - Others can join groups informally – approach those who applied for Commission but were not selected
    - Reports from each by end of calendar year
        - Legislative session starts in January, budget submitted in October – recommendations for legislation to fill obvious holes must be submitted earlier
    - Establish how information will be shared within and among groups

10:50 FOIA briefing by Joshua Heslinga, Office of the Attorney General

- VA's FOIA is separate from federal law. Members must familiarize themselves with law
- "Magic number" defining meetings is 3 people
- Notice must be provided to public for all meetings, including remote/conference meetings
- Experts can be invited to assist in working groups, but this does not make them members of the Commission. And if to become continual part of the

group, they will need to undergo FOIA process

11:02 DMV presentation by David Burhop

- **Cross-sector Digital Identity Initiative**: Intended to create single, verified identity, which can be used across multiple vendors online
    - Grant provided by NSTIC (National Strategy for Trusted Identities in Cyberspace)
- **Commonwealth Authentication Services**: use of DMV data in all state agencies
- Consider liabilities that could be created for customers by these new services
    - Privacy, trust of government issues

11:20 VITA presentation by Sam Nixon, CIO and Michael Watson, CISO

- Statutorily responsible for IT security, including infrastructure
    - Applications and data are responsibility of agencies
- 95.5 million attack attempts in CY 2013
    - Attacks are primarily against applications, not infrastructure
- Currently 86 of 89 agencies in VITA-protected infrastructure

11:57 Open for public comment

11:58 Motion to adjourn from John Wood, seconded by Paul Tiao