Journal of Business & Technology Law

Volume 8 | Issue 1 Article 4

A Commission on a Cyber Mission

Adrian Wilairat

Adrian Wilairat*

A Commission on a Cyber Mission**

Introduction

The need for comprehensive cybersecurity[1] currently enjoys more support than ever before.[2] The State of Maryland and its executive and legislative branches are taking advantage of the high value currently placed on cybersecurity.[3] Anyone who has read a newspaper, listened to the radio, or watched television in Maryland during the last year cannot escape the concept of cybersecurity. Advertisements touting cybersecurity businesses, training, and educational programs, for example, inundate the media.[4] In close proximity to Washington, D.C., Maryland should, and is, prioritizing cybersecurity in several capacities.[5] The State's most recent effort to strengthen cybersecurity has resulted in the formation of a three-year legislative body, the Commission on Maryland Cybersecurity Innovation and Excellence.[6] This Commission is the appropriate vehicle to improve cybersecurity in Maryland, and it

* Adjunct Professor of Law, University of Maryland Francis King Carey School of Law. The author recently accepted a position at the U.S. Department of Homeland Security's (DHS) Transportation Security Administration (TSA) to work on cybersecurity policy and communications issues.

** This Article captures and expands upon the talk I delivered at the *Journal of Business & Technology Law*'s conference entitled *Cybersecurity: Safeguarding Information in a Digital Age* on March 30, 2012. Opinions and views expressed in this piece are my own and do not reflect those of current, former, or future employers. Kudos to the superb staff of the *Journal of Business & Technology Law* for their edits to this Article.

1. In this Article, I will use the compound noun "cybersecurity" except when referring to sources, such as reports produced by the Commission that are the subject of this piece, or proper names that spell the concept with two words.

2. *See* Jonathan G. Cedarbaum et al., *Cybersecurity and the Law: What to Expect in 2012*, WilmerHale, (Jan. 17, 2012), http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=10017 ("Cybersecurity has grabbed the top spot on the federal government's national security agenda, both in the Executive Branch and on Capitol Hill.").

3. *See infra* Section I.A. (describing Governor O'Malley's efforts toward promoting cybersecurity); *infra* Section II (recounting the legislature's creation of the Maryland Commission on Cybersecurity Innovation and Excellence).

4. *See, e.g.*, *Cybersecurity*, Univ. of Md. Univ. Coll. (2012), *available at* http://www.umuc.edu/visitors/news/videos/.

5. *See, e.g.*, *About the Maryland Cybersecurity Center (MC2)*, Univ. of Md., http://www.cyber.umd.edu/about (last visited Nov. 14, 2012). MC2 is a program started by the State's flagship university to promote interdisciplinary approaches to cybersecurity. *Id.*

6. *Md. Commission on Cybersecurity Innovation and Excellence*, Md. Manual On-Line, http://www.msa.md.gov/msa/mdmanual/26excom/html/10cyber.html (last updated Oct. 10, 2012).

has important decisions to make about how to do so. Section I in this Article describes the Governor's cybersecurity strategy.[7] Section II discusses the Commission.[8] Section III analyzes the Commission's activities and the Maryland executive branch's cyber efforts.[9] Section III goes on to argue that although the Commission's structure and goals are strong, it needs to increase efforts to strengthen cybersecurity in Maryland and focus more on issues within its control.[10]

I. Prelude to the Commission

A. Maryland Cyber Resources

First, Maryland's proximity to the nation's capital makes it a prime location for increased cybersecurity efforts. Maryland is home to 50 federal agencies, including the National Security Agency (NSA) and the Defense Information Systems Agency, twelve major military facilities, and many of the country's leading defense contractors.[11] In 2009, U.S. Secretary of Defense Robert Gates established a central cyber command office, U.S. Cyber Command (USCYBERCOM), housed alongside the NSA at Fort George G. Meade in Maryland.[12] Maryland has a burgeoning computer design industry,[13] and has major research universities that are working on technological developments.[14] Clearly, the infrastructure necessary to make Maryland a cybersecurity epicenter exists.

With such an abundance of cyber resources already in Maryland, Maryland Governor Martin O'Malley has made cybersecurity a major part of his agenda.[15] With the launch of his cybersecurity initiative in 2010,[16] he encouraged: the

7. *See infra* Section I.

8. *See infra* Section II.

9. *See infra* Section III.

10. *See infra* Section III.

11. Press Release, Office of Gov. Martin O'Malley, Governor Martin O'Malley Releases Plan to Make Maryland Nation's Epicenter for Cyber Security (Jan. 11, 2010), http://www.gov.state.md.us/pressreleases/100111.asp; Md. Dep't of Business & Economic Development, CyberMaryland 2 (2011) [hereinafter CyberMaryland].

12. Memorandum from Secretary of Defense Robert Gates on Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009), *available at* http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyber_command_gates_memo[1].pdf; *U.S. Cyber Command*, U.S. Strategic Command, http://www.stratcom.mil/factsheets/Cyber_Command/ (last updated Dec. 2011); *see also* CyberMaryland, *supra* note 11, at 11 ("Just with the federal presence, there is such an enormous amount of computing being done in Maryland. All of those resources are here — they're not going anywhere.").

13. In 2009, for example, Maryland ranked first in the country in development of jobs in computer design. *See* Press Release, Office of Gov. Martin O'Malley, *supra* note 11.

14. *See* CyberMaryland, *supra* note 11, at 12.

15. *Id.* at 2.

16. Press Release, Md. Dep't of Labor, Pathways to Cyber Consortium Celebrates First Anniversary of Training Maryland Workers for Cyber Economy (June 29, 2011), http://www.dllr.state.md.

commercialization of discoveries made in public research labs;[17] exercises simulating cyberattacks;[18] the Multi-State Information Sharing & Analysis Center's (MS-ISAC)[19] designation of Maryland to pilot a cyber threat detection initiative that would involve examination of computer logs to search for patterns suggesting an immediate threat;[20] chief information officers' meetings;[21] and audits conducted by the State Office of Legislative Audits that focus on data security.[22] He oversaw the Department of Information Technology's (DoIT) creation of a Cyber Security Policy, which establishes computer security standards for the State.[23] He is stimulating the growth of a technology industry that has expertise in cybersecurity and will be able to prevent and respond to cyberattacks.[24] Governor O'Malley prioritizes cybersecurity so strongly that he considers strengthening it to be a gubernatorial duty.[25]

B. CyberMaryland

As tasked by Governor O'Malley, in January 2010 the Maryland Department of Business and Economic Development (DBED) issued a report of its survey and analysis of Maryland cybersecurity resources.[26] After examining data and

us/whatsnews/cyberpath.shtml ("In January 2010, Governor Martin O'Malley launched CyberMaryland, an interagency initiative to make Maryland the epicenter of cybersecurity for the entire nation.").

17. CyberMaryland, *supra* note 11, at 24 ("Cyber security technologies transferred from the federal laboratories and universities in the State can become an engine for Maryland-based economic development and growth."). The phenomenon of labs transitioning from public to private entities is commonly referred to as "spinning off." Benedicte Callan, *Introduction: The New Spin on Spin-Offs*, 2001 Sci. Tech. Indus. Rev., no. 26 at 7, *available at* http://www.oecd-ilibrary.org/sti-review_5lmqcr2kb38t.pdf?contentType=/ns/Book&itemId =/content/book/sti_rev-v2000-1-en&containerItemId=/content/serial/16097637&accessItemIds=&mimeType= application/pdf ("Research-based spin-offs are generally understood to be small, new technology-based firms whose intellectual capital originated in universities or other public research organisations.").

18. *See* Gov. Martin O'Malley, Remarks on the National Initiative for Cybersecurity Education (Sept. 20, 2011), http://www.governor.maryland.gov/blog/?p=5984 (recounting the first cabinet-level security tabletop exercise with 160 participants which simulated a cyberattack).

19. MS-ISAC is an organization working to improve cybersecurity for state and local governments. *About Us*, Multi-State Info. Sharing & Analysis Ctr., http://msisac.cisecurity.org/about/ (last visited Nov. 14, 2012).

20. Gov. Martin O'Malley, *supra* note 18.

21. *Id.*

22. *Id.*

23. *Governor Martin O'Malley Proclaims October as Cyber Security Awareness Month*, Office of Gov. O'Malley, Oct. 2, 2009, http://www.governor.maryland.gov/pressreleases/091002.asp. These standards closely follow National Institute of Standards and Technology (NIST) standards, while providing agencies with leeway in their application. Dep't of Info. Tech., Info. Sec. Policy 4–5 (2011), http://doit.maryland.gov/support/Documents/security_guidelines/DoITSecurityPolicy.pdf.

24. *See also* Act of May 19, 2011, 2011 Md. Laws, ch. 409 (creating the Invest Maryland Program, in part to attract investment in the technology industry in Maryland); CyberMaryland, *supra* note 11, at 23.

25. *See* CyberMaryland, *supra* note 11, at 2 ("One of my most solemn obligations is to safely guard our citizens which includes protection from cyber threats.").

26. *Id;* Md. Comm'n on Cyber Security Innovation & Excellence, Interim Report of Findings and Recommendations 2 (2011) [hereinafter Interim Report].

interviewing fifty cybersecurity experts from companies and government agencies,[27] the report, *CyberMaryland,* found that cybersecurity assets in Maryland were strong, with an abundance of federal and military, technology research and development, private business, and education resources.[28] Moreover, the report provided ten recommendations for improving Maryland's leadership in cybersecurity, including establishing federal partnerships, transforming public technological developments into commercial ones, enhancing cyber certification standards, developing cyber educational programs, and attracting cybersecurity industry and business.[29] *CyberMaryland*'s Recommendation Seven argues that because of Maryland's nexus with the federal government, through similar cyber breaches and the location of many federal agencies, "Maryland should seamlessly align its priorities to match those of the federal government."[30]

II. The Maryland Commission on Cybersecurity Innovation and Excellence

As a follow-up to *CyberMaryland*, in 2011 Governor O'Malley signed Maryland House Bill 665 establishing the Maryland Commission on Cybersecurity Innovation and Excellence (the Commission).[31] The twenty-five-person commission consists of a hodgepodge of individuals: two members of the Maryland General Assembly, three directors of state agencies, three directors of business-oriented non-profit organizations, five members of cybersecurity companies, three members of business associations, four academics, three individuals from sectors vulnerable to cyberattacks, one representative of a criminal victims' advocacy organization, and one person from a company specializing in electronic health records.[32] The Commission also invites representatives of the federal government to join the Commission; as of the printing of this Article, no federal members had joined.[33] The University of Maryland University College, the country's largest online university,[34] staffs the Commission.[35] The Commission's purpose "is to provide a road map for

27. CyberMaryland, *supra* note 11, at 4; Press Release, Office of Gov. Martin O'Malley, *supra* note 11.

28. CyberMaryland, *supra* note 11, at 9–15.

29. *Id.* at 23–31.

30. *Id.* at 30.

31. Act of May 10, 2011, 2011 Md. Laws, ch. 251 (codified at Md. Code Ann., State Government § 9-2901 (West 2012)).

32. Md. Code Ann., State Gov't § 9-2901(b)(1) (West 2012).

33. The current list of commission members does not include any federal representatives. For the list of committee members, see *Commission Members*, Univ. of Md. Univ. Coll., http://www.umuc.edu/legal/cyber/members.cfm (last visited Nov. 14, 2012).

34. Daniel de Vise, *Chancellor Says UMUC Is Sound Academically*, Wash. Post, Apr. 2, 2012, at B1.

35. Interestingly, the original version of the bill named DBED and DoIT as joint staffers, without naming UMUC. *Compare* H.B. 665, 2011 Leg., 428th Sess. (Md. 2011) (calling for DBED and DoIT to staff the Commission), *with* State Gov't § 9-2901(d) (calling for UMUC to staff the Commission).

making the State the epicenter of cybersecurity innovation and excellence."[36] To achieve this purpose, the Commission has five wide-ranging duties that include everything from analyzing Maryland and federal cybersecurity laws and policies to recommending best practices for computer networks in the State to recommending ways to promote cyber business and enterprise.[37]

These five duties have seventeen different parts.[38] Citing *CyberMaryland*, the Commission's Interim Report distilled these different parts into two "major components."[39] First, according to the Interim Report, the Commission must design strategies to prevent cyberattacks against Maryland cyber networks.[40] To achieve this initiative, the Commission will analyze State and federal laws and policies, review how the State can better partner with the federal government, and analyze proposed federal laws and policies.[41]

The second major component, as determined by the Commission itself, is to create a strategic roadmap for making Maryland the national leader and epicenter in cybersecurity.[42] This includes, *inter alia*, a hodgepodge of activities including formulating a plan to create jobs, fostering public private partnerships, commercializing technology, spurring cyber education and a cyber workforce, and determining an official to coordinate cybersecurity strategies.[43]

In furtherance of its purpose, the Commission met three times in its first year.[44] It has more deeply analyzed the goals outlined in the authorizing statute[45] and received a briefing by a national organization dedicated to improving cybersecurity in states.[46] The Commission must finish a final report with its strategies and recommendations, presumably addressing its seventeen components by September 1, 2014, when its mandate ends.[47]

36. Md. Code Ann., State Gov't § 9-2901(f) (West 2012).

37. State Gov't § 9-2901(g).

38. *Id.*

39. Interim Report, *supra* note 26, at 2. The Commission submitted the interim report pursuant to section 9-2901(h) of the State Government article of the Maryland Code.

40. Interim Report, *supra* note 26, at 2.

41. *Id.*

42. *Id.*

43. *Id.*

44. The Commission met on Nov. 22, 2011, Mar. 13, 2012, and June 8, 2012. *Meeting Dates*, Univ. of Md. Univ. College, http://www.umuc.edu/legal/cyber/meetings.cfm (last visited Nov. 14, 2012).

45. Interim Report, *supra* note 26, at 5.

46. *See* Comm'n on Md. Cybersecurity Innovation & Excellence, Tentative Agenda, *available at* http://www.umuc.edu/legal/cyber/upload/MD_Cyber_Commission_Agenda_June8_2012_Meeting.pdf (stating that the Commission invited a presentation by the National Association of State Chief Information Officers (NASCIO)). For the NASCIO briefing on the issue, see Pam Walker, Nat'l Assoc. of State Chief Info. Officers, Cybersecurity in the States 2012: Priorities, Issues and Trends (2012), http://www.umuc.edu/legal/cyber/upload/NASCIO_MD_Cyber_Commission_2012.

47. Md. Code Ann., State Gov't § 9-2901(i) (West 2012).

III: The Commission Is Set Up Appropriately

A. Purpose and Duties

In its Interim Report, the Commission identifies two major components of its work: strategizing against cyberattacks and creating a strategic road map for turning the State into a cybersecurity epicenter.[48] The second component, as determined by the Interim Report, is nearly the same as the Commission's purpose as defined by the authorizing statute.[49] Instead of categorizing the second goal of the Commission in the manner of the Interim Report, it would be more precise to categorize a second component of the Commission as business development. An examination of the Commission's stated duties, however, indicates that the Commission has three main goals: 1) reviewing and analyzing State and federal laws and identifying inconsistencies; 2) determining ways to combat and recover from cyberattacks; and 3) spurring commercialization.[50]

Although the Commission's purpose and duties, regardless of how they are broken down or grouped, are not inconsistent with the recommendations of the earlier *CyberMaryland* report discussed *supra*, the Commission's approach to a relationship with the federal government has shifted from that in *CyberMaryland*. Two of the *CyberMaryland* recommendations focused on aligning the State with the federal government: the very first *CyberMaryland* goal was establishment of a federal National Center of Excellence for Cyber Security, and the seventh was to "align" Maryland's cybersecurity priorities with President Obama's.[51] The Commission, on the other hand, does not have duties of aligning or partnering with the federal government, but rather has duties of ensuring that there is nothing inconsistent and that there is no preemption.[52] The seemingly small distinction between *CyberMaryland*'s federal alignment and the Commission's focus on lack of inconsistency with the federal government is an important one. Rather than adopting *CyberMaryland*'s recommendation that "Maryland should seamlessly align its priorities to match those of the federal government,"[53] the Commission is Maryland focused, and will use the federal government in ways that benefit

48. *See supra* text accompanying notes 40–44.

49. *Compare* Interim Report, *supra* note 26, at 2 ("[T]he Commission will provide a Strategic Road Map for making Maryland the leader and national epicenter for cyber security, innovation, and jobs that fuel a knowledge based economy."), *with* State Gov't § 9-2901(f) ("The purpose of the Commission is to provide a road map for making the State the epicenter of cybersecurity innovation and excellence.").

50. *See* State Gov't § 9-2901(g). Alternatively, one could view the Commission as having four goals centered around "four major themes": legal analysis, government structure and practice, marketing and partnerships, and education. *See* Comm'n of the Md. Cybersecurity Innovation & Excellence, Summary: Mar. 13, 2012 Open House & Meeting 2 (2012), http://www.umuc.edu/legal/cyber/upload/Summary_March 13_2012_Meeting_MCC.pdf.

51. *See* CyberMaryland, *supra* note 11, at 23, 30.

52. Md. Code Ann., State Gov't § 9-2901 (g)(1)(i), (g)(3) (West 2012).

53. CyberMaryland, *supra* note 11, at 30.

Maryland.[54] The needs of a state, and in this case, Maryland, inevitably will differ in at least a few ways from those of the federal government. States have different people, policies, priorities, and programs, and thus their goals, particularly cybersecurity goals, must be appropriately tailored and nuanced. Ultimately, this focus on Maryland, rather than simply serving as a conduit for helping the federal government achieve its regulatory goals, seems to be an appropriate focus of a Commission whose purpose is to lead the way for establishing Maryland as a haven for cybersecurity innovation and excellence.

The Commission has legitimate objectives. Although the Commission has established committees focused on important themes,[55] to fully serve as a vehicle for strengthening cybersecurity, it needs to increase its efforts. Although part of the Commission's first listed goal is to examine federal cybersecurity laws, it should not wait until the passage of a federal bill, which has been held up in bipartisan bickering,[56] to really get to work. Even after a federal bill is passed, enactment — and challenges — of regulations will take time. With inevitable reformulations, amendments, and a potentially lengthy rulemaking process that could last well into 2014 if not longer, the Commission should not wait to examine federal law before addressing Maryland-specific initiatives. It is unclear how many years down the road it will be before the existence of a comprehensive statutory and regulatory framework for the Commission to thoroughly assess. Additionally, rather than becoming mired in the political process of establishing a Center for Excellence, the Commission should focus on strategizing on appropriate amendments to State laws regarding data breach and notification, as well as find ways to incentivize public-private partnerships.

54. The Commission's duties regarding the federal government are to ensure that there are no inconsistencies between Maryland and federal law, to coordinate State and federal resources, and to leverage federal funds. *See* State Gov't § 9-2901(g).

55. *See* Comm'n on Md. Cybersecurity Innovation & Excellence, *supra* note 46 (noting discussion of "Committee Reports" at a meeting of the Commission).

56. There were competing federal cyber bills — one sponsored by Senators Joseph Lieberman, I-Conn., and Susan Collins, R-Maine, and one by Senator John McCain, R-Ariz. — in Congress in 2012. Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012) (Lieberman's bill); SECURE IT Act, S. 2151, 112th Cong. (2012) (McCain's bill). The surviving Cybersecurity Act of 2012 failed in August and November 2012. *See* Harry Reid's Virus, Wall St. J., Nov. 16, 2012, at A22, *available at* http://online.wsj.com/article/SB10001424127887324735104578120800351382218.html. Agreement on a Senate bill almost certainly will not come until the 113th Session of Congress in 2013 — at the earliest. *See* Jennifer Martinez, *Cybersecurity Bill Likely Dead*, Hillicon Valley (Oct. 27, 2012, 9:31 AM), http://thehill.com/blogs/hillicon-valley/technology/264417-cybersecurity-bill-likely-dead-in-congress. Further, in early 2013, President Obama likely will issue the White House's cybersecurity plan through an executive order. Jennifer Martinez, *Obama Likely to Issue Executive Order on Cybersecurity as Early as January*, Hillicon Valley (Dec. 21, 2012, 6:00 AM), http://thehill.com/blogs/hillicon-valley/technology/274175-cybersecurity-order-likely-in-january-observers-say#ixzz2Jn3bmQyF.

B. Membership

Containing a mix of State officials, academics, and business sector representatives, the Commission consists of the right composition — and has the commitment — to strengthen cybersecurity in Maryland. That fifteen of the twenty-five members work in the private sector[57] reflects the significance that the private sector plays in cybersecurity. The Commission's heavy representation from the business sector is appropriate, as commercialization and economic development is essential to developing sophisticated and cutting edge systems and technologies for preventing and mitigating against cyberattacks.

As of the printing of this Article, no individuals representing the federal government had joined.[58] Although there is nothing inherently wrong with a state carrying out the federal government's regulatory scheme, this lack of federal representation should allow the Commission to more fully strengthen cybersecurity in Maryland, as the Commission can focus entirely on State strength and improvement. The Commission shows appropriate deference to the federal government, as its legal analysis should ensure that no current or proposed law conflicts or is preempted by current federal law.[59] Further, federal representatives will have input on the Commission; members of Congress have attended most of the meetings.[60] Although these Congressmen cannot become members of the Commission, these Congressmen's representation of Maryland bodes well for the likelihood that they will advocate for programs and policies best for Maryland.[61] Moreover, partisanship does not appear to have affected the work of the Commission — yet. High attendance — two thirds of its members were present at its March 13, 2012 meeting[62] — is a good indicator that the Commission means business.[63]

57. *See* STATE GOV'T § 9-2901(b)(1) (providing statutory requirements of Commission members); *Commission Members*, UNIV. OF MD. UNIV. COLL., http://www.umuc.edu/legal/cyber/members.cfm (last visited Nov. 14, 2012).

58. *See supra* note 33 and accompanying text.

59. *See* MD. CODE ANN., STATE GOV'T § 9-2901 (g)(1)(i), (g)(3) (West 2012) (providing that the Commission will study federal preemption).

60. COMM'N ON MD. CYBERSECURITY INNOVATION & EXCELLENCE, *supra* note 46; COMM'N ON MD. CYBERSECURITY INNOVATION & EXCELLENCE, RECEPTION (2012), *available at* http://www.umuc.edu/legal/cyber/upload/Reception_Agenda.pdf.

61. Only directors of executive branch agencies were invited to serve on the Commission. STATE GOV'T § 9-2901(b)(2). Senator Barbara Mikulski has been a leader of cybersecurity initiatives, and she has been referred to as a "cyber senator." COMM'N OF THE MD. CYBERSECURITY INNOVATION & EXCELLENCE, *supra* note 50 (citing U.S. Representative Dutch Ruppersberger's remarks on Senator Mikulski); *Launch of the National Cybersecurity Center of Excellence: Video Transcript*, NAT'L INST. OF STANDARDS & TECH. (Feb. 24, 2012), http://www.nist.gov/itl/csd/nccoe-transcript.cfm (last visited Oct. 12, 2012).

62. *See* COMM'N OF THE MD. CYBERSECURITY INNOVATION & EXCELLENCE, *supra* note 50, at 1 (indicating that twenty commissioners were present at the meeting); *supra* note 32 and accompanying text (explaining that there are twenty-five commission members).

63. Too often, it seems, *ad hoc* bodies — commissions, committees, working groups, and the like — have high ideals but end up doing little to next to nothing.

C. DoIT should Run the Pilot Program

The Commission will need to determine a "unit of State government that is suitable to run a pilot program regarding cybersecurity . . . ."[64] The most pressing questions establishment of this agency poses are: what will this pilot program look like, what will it do, and who will run it? Rather than being stuck in inertia, trying to accomplish too much, or becoming entangled in a bureaucratic morass, to be effective this entity will need to run a program with a limited scope and with specific goals. It should simulate intrusion detection and data breach. Its exercises should reveal vulnerabilities in Maryland agencies and businesses' systems, and it should propose solutions to strengthen protections and mitigate loss. Further, this pilot program should at least cover Maryland's electric smart grid, which is necessary for a flexible and energy-saving electricity delivery system. Unfortunately, establishment of a smart grid makes the electric power sector more vulnerable to a cyberattack.[65]

The two logical agencies to run the new program are DoIT and DBED. DoIT's expertise is information technology,[66] while DBED's is business.[67] An agency with technological programming and skills, such as DoIT, would be the best choice.[68] DoIT should be able, for example, to help determine structural deficiencies in the smart grid.[69] Although DBED issued *CyberMaryland*[70] and should assist with the

64. Md. Code Ann., State Gov't § 9-2901 (g)(5)(iii) (West 2012).

65. *See* Lisa Rein, *'Smart Grid' Audit Flags Cybersecurity*, Wash. Post, Feb. 7, 2012, at A17 (reporting that the Energy Department's Inspector General "found 'shortcomings' in the cybersecurity plans of more than a third of the utility companies that received federal funding for 'smart grid' projects . . . ."). Additionally, according to former White House cybersecurity czar Richard Clarke, "[t]he U.S. has done little or nothing to fix the vulnerabilities in its power grid or in other civilian networks." Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About it 62 (2010). Moreover, Clarke reasons that "[u]nfortunately, President Obama's 'Smart Grid' initiative will cause the electric grid to become even more wired, even more dependent upon computer network technology." *Id.* at 101.

66. *About DoIT*, Md. Dep't of Info. Tech., http://doit.maryland.gov/about/Pages/AboutDoIThome.aspx (last visited Nov. 4, 2012) (stating the agency's expertise).

67. *About Us*, Md. Dept. of Bus. & Econ. Dev., http://www.choosemaryland.org/aboutdbed/Pages/default.aspx (last visited Nov. 4, 2012) (stating the agency's expertise).

68. DoIT already has a Cyber Security Resource Center. *Cyber Security Resource Center*, Md. Dep't of Info. Tech., http://doit.maryland.gov/cybersecurity/Pages/CyberSecurityHome.aspx (last visited Nov. 4, 2012). Additionally,

> DoIT partnered with [the Maryland Department of Transportation] and the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide statewide training for web application developers on cybersecurity threat prevention, protection, and response. The 3-day class for web developers specifically addressed ways to mitigate security vulnerabilities in the development of online services.

Dep't of Info. Tech., State of Md. Info. Tech. Master Plan 3 (2011), *available at* http://doit.maryland.gov/policies/documents/policyplanning/fy2013itmpfinal.pdf.

69. As cybersecurity also includes standard crime, DoIT could also study the strength of gambling terminals introduced in 2012, which would allow the Commission to analyze the vulnerabilities to theft and criminal fraud.

development of cyber commercial enterprise, DoIT has the expertise necessary to lead the pilot program.

D. Cyber Security Policy Official

The Commission needs to appoint a "cybersecurity policy official" to coordinate Maryland's policies, strategies, and activities.[71] In effect, this policy official would take over and extend the Commission's role once its mandate terminates in 2014.[72] This leader should be proactive and lead the State in the coming years. The most appropriate traits seem to be someone with a degree of technological expertise who has a vision of the direction in which the State should go. Although there may be individuals currently within State government or academia, the Commission should not be opposed to considering a person from the private sector, which has many individuals skilled in cutting edge cyber issues.[73]

Conclusion

To achieve the Commission's goals, State agencies will have to work together. The public sector will have to work with the private sector. Coordination is paramount.

In 2012, Governor O'Malley declared that Maryland "is now the clear national epicenter for cybersecurity."[74] Perhaps such a declaration is premature, but legislative entities like the Commission, which enjoys the full support of the Governor, will allow this concept to be realized.[75] The emphasis of Maryland's executive branch and legislature on cybersecurity — and its support of the private sector — should yield the technologically savvy work force that Maryland needs to strengthen cybersecurity.

70. *See* CyberMaryland, *supra* note 11, at 1.

71. Md. Code Ann., State Gov't § 9-2901 (g)(5)(iv) (West 2012).

72. *See supra* text accompanying note 6 (indicating that the Commission has a three year term).

73. CyberMaryland, *supra* note 11, at 14.

74. Gov. Martin O'Malley, Remarks at the Johns Hopkins Carey Business School, Sept. 12, 2012, *available at* http://www.governor.maryland.gov/blog/?p=6684.

75. According to *CyberMaryland*, "Maryland companies and organizations are optimistic about the continued growth of cybersecurity efforts; specifically the unprecedented opportunities of Maryland's federal markets, superior workforce, outstanding education system and rich and robust quality of life." CyberMaryland, *supra* note 11, at 4.