Meeting Minutes
Maryland Cybersecurity Council
Subcommittee on Education and Workforce Development
Friday, November 15, 2019
11:00 am – 1:00 pm
College Park Hotel and Conference Center at UMGC
Room 1101/1102
3501 University Boulevard East
Hyattsville, Maryland

Subcommittee Attendance (6/10)

Subcommittee members: Senator Katie Fry Hester (chair), Maryln Aguilar (for Miheer Khona), Dr. Michel Cukier, Dr. Richard Forno (for Dr. Anupam Joshi), Dr. Kevin Kornegay (for Morgan State University President David Wilson), and Jonathan Powell.

Other Council members participating: Dr. Anton Dahbura, Christine Ross, Gregg Smith, and Stacey Smith.

Staff: Hannibal Kemerer (Director of Legislative Affairs, OAG) and Dr. Greg von Lehmen (University of Maryland Global Campus, staff to the Council).

Contributors: Carolyn Baker (UMBC), Dr. S Bhaskar (UMGC), Dr. Richard Cerkovnik (Montgomery College), Mark Loepker (Cyber Center for Education and Innovation – Home of the National Cryptologic Museum), Kent Malwitz (UMBC Training Centers), Casey O'Obrien (Prince Georges Community College and CyberWatch PI), Dr. Loyce Pailen (UMGC), Amy Ratzburg (Vetegrity), Latoya Staten (Connected2Tech), and Roy White (Diverse Concepts),

1) Senator Hester welcomed everyone and thanked them for joining the subcommittee's meeting. After self-introductions, she identified the meeting objectives as threefold: to formulate a list of cyber workforce development recommendations for Maryland, to prioritize them for the 2020 legislative session, and to invite the continued participation of everyone at the meeting and anyone else interested in the issues.

2) The plenary discussion thematically identified four major needs. Subgroups were formed during the meeting to make the themes or needs more concrete as a step toward informing possible legislative recommendations to the full Council. The following summarizes by themes the report-outs of the four discussion groups:

   a) *Scaling and coordination of cyber workforce training efforts.* (Subgroup: Dr. Cerkovnik [facilitator], Dr. Kevin Kornegay, and Latoya Staten). Subgroup suggestions:

- Catalog and coordinate workforce programs focused on developing cyber/IT talent including: Academia research and non-credit workforce programs
  - State and Federally funded skill development program
  - Maryland EARN Grants
  - Department of Labor Techhire Grants
  - Youth Skill Development
  - Internship/Apprenticeship Programs

- Industry-led initiatives
  - Capture the Flag Events and Cyber Ranges
  - Job Boards
  - Open Research Projects
  - Short-term projects that provide hands-on skills

- Assess cataloged programs for best practices

- Scale and Fund top echelon programs which:
  - Provide "good" return on investment (ROI)
  - Have private investment
  - Can be self-sustaining

Illustrative questions: Could job boards be coordinated across postsecondary schools to more efficiently match students with recruitment needs in the market? Could county workforce development boards be networked and focused to have a greater impact on cyber workforce needs? Could access to the Baltimore Range be greatly expanded to provide many more students with an option for hands-on experience before entering the job market?

It was suggested that the Governor's Workforce Development Board had started a database of activities related to cyber workforce development and that this might provide a more comprehensive view from which to gauge which activities could be scaled or coordinated to have the greatest impact.

b) *Upscaling training to help close the cyber skills gap.* (Subgroup: Casey O'Brien [facilitator], Dr. S Bhaskar, Kent Malwitz, and Jonathan Powell). Subgroup suggestions:

- Subsidized professional development for educators is a missing critical component in many discussions re: to cybersecurity
- Determine ways to incentivize commercial orgs to upskill their incumbent IT workforce so they can move into specialized cybersecurity roles; backfill their vacated positions with workers getting not only IT foundational knowledge and skills, but security baked in

- Change State procurement requirements dictating bachelor's degrees; focus on the competencies needed to do the job. The NICE Cybersecurity Workforce Framework (NIST Special Publication 800-181) has 52 defined work roles, with requisite knowledge and skills that can guide this effort.

c) *Messaging/marketing to raise awareness of cybersecurity careers and training opportunities* (Subgroup: Dr. Richard Forno [facilitator], Dr. Anton Dahbura, Mark Loepker, Dr. Loyce Pailen, and Amy Ratzburg). Subgroup suggestions:

- Assess current State legislation and programs with awareness component (or opportunities) and review bills with this objective that failed in prior sessions to see if they might be worth a second legislative attempt.
- Create and prominently promote a cybersecurity education and training clearinghouse that would make it easier to identify resources for those considering a cyber-related career.
- Interdisciplinary messaging kits for K12 schools that are audience-specific (parents, students, school counselors), companies (e.g., regarding hiring practices/job descriptions/qualifications), the military, underemployed, etc. Key items of emphasis: that 'cyber' is not just a technical STEM field, 'cyber' does not require a security clearance for all jobs everywhere and fostering diversity in the cyber pipeline/workforce.
- Develop a network of audience-appropriate mentors/volunteers to go into K12 schools to talk about their careers in cyber. (The mentor program of the Maryland Business Roundtable was noted with suggestions that it might be expanded.)
- Public/private partnerships to provide scholarships for teachers to spend time during their summers in government or corporate work settings to give them an understanding of cyber that they could take back to their classrooms. Perhaps matched with private/public funds.
- A sustained, intensive, and substantially funded general awareness campaign in Maryland that cybersecurity is critical to individuals, companies, the State and nation and that there are many different careers in the field. This suggestion is to go well beyond the uncoordinated efforts that occur briefly each year around National Cybersecurity Awareness Week.

d) *Public/Private Partnerships* (Subgroup: Hannibal Kemerer [facilitator], Marilyn Aguilar, Caroline Baker, Dr. Michel Cukier, Christine Ross, Gregg Smith, and Roy White).

- Co-Teaching: Stand up a program of industry and government cybersecurity professionals co-teaching with certified teachers in high-school. Have them trained not to scare the students with horror stories but, instead, to provide real-life stories about day-to-day work in the cybersecurity space. Formalize the co-teaching component through a partnership with MSDE.
- Video Education: Have company and industry representatives explain to high school students, through in-person presentations and videos (a la Life Journey) their daily work. Mentoring: Recruit and deploy industry and government cybersecurity professionals to

serve as organized mentors to high school and college students. (Christine Ross and Gregg Smith offered to help recruit mentors on an ad hoc basis).

- Business at the Table with Education: The Kirwan Commission had only one business member. Industry cybersecurity professionals need greater representation in any Maryland educational reform task forces.

3). Senator Hester thanked the participants for their time and feedback. With a view to the 2020 session, the attendees agreed that the next step in the subcommittee's work is to prioritize the suggestions. The Senator observed that the key criterion is what is practical or do-able. The challenge is to identify initiatives that are impactful but not over-reaching and that could involve investments that are jointly funded by the public and private sectors.

4). The next meeting will be on Friday, November 22 (10:00 – 11:00 am) to identify the short list for possible development into legislative proposals.

The meeting was adjourned at 1:15 pm.