Statement for the Record – National Commission on Military, National, and Public Service

Lisa Monaco, Co-Chair, Aspen Cybersecurity Group

Will Hurd, Co-Chair, Aspen Cybersecurity Group

Ginni Rometty, Co-Chair, Aspen Cybersecurity Group

John Carlin, Chair, Cybersecurity & Technology Program, The Aspen Institute

---

On behalf of the co-chairs of the Aspen Cybersecurity Group (Aspen Cyber Group), the Aspen Institute's Cyber & Technology Program is pleased to enter this statement for the record concerning the Commission's preliminary summaries of research and analysis, as expressed in the Commission's published Staff Memorandum (Memorandum).

The Aspen Cyber Group is a cross-sector, public-private forum comprising former government officials, Capitol Hill leaders, industry executives, and respected voices from academia, journalism, and civil society who have come together to translate pressing cybersecurity conversations into action. At its inaugural meeting in January 2018, the Aspen Cyber Group decided to focus its efforts on three key areas of need as requiring urgent attention by a group that crosses party lines and includes both policymakers and practitioners: (1) improving operational collaboration between the public and private sectors; (2) securing and ensuring confidence in emerging technologies, including the Internet of Things (IoT); and (3) developing the skills and education necessary for a workforce that will increasingly confront cybersecurity challenges.

Accordingly, the Aspen Cyber Group immediately focused its time and attention on the well-known cybersecurity talent gap facing both public and private entities across the nation. Demand for employees and instructors with cybersecurity knowledge, skills, and abilities far outstrips the available supply. The resulting scarcity presents a critical danger to an American society that depends on vulnerable computing infrastructure.

In November 2018, the Aspen Cyber Group published eight principles for cybersecurity workforce development intended to encourage scalable practices that can address the cybersecurity skills gap. These principles can be summarized as:

- Widen the aperture of candidate pipelines by adopting New Collar principles
- Revitalize job postings to be engaging and to focus on core requirements
- Simplify career models and build transparency
- Think about new ways of hiring and training
- Launch apprenticeship programs
- Commit to employee development
- Adopt key principles for productive partnerships and programs

- Make cybersecurity everyone's business

Aspen Cyber Group members are currently working to implement these principles and look forward to sharing the results with the Commission in the future. However, this statement offers more narrow feedback addressing specific elements of the Memorandum.

Conceptualizing a Civilian Volunteer Corps

A key function of the Commission is to explore avenues for "[a]ttracting and retaining public service employees, especially those with critical skills." In discussing alternatives to improve the competitiveness of federal agencies for workers with critical skills, the Memorandum references "a civilian corps of former federal cybersecurity employees to retain a reserve of critical technical talent in case of emergency." This is a promising avenue for achieving the Commission's stated purpose. However, Commissioners should consider expanding the concept.

First, a civilian corps need not be limited to a purely emergency function. A standing group of trained cybersecurity specialists could add value to routine operations. Some of the most significant gaps in cybersecurity arise from an absence of basic cybersecurity controls, i.e., cyber hygiene. Research into past security breaches strongly suggests that implementing time-tested steps such as application whitelisting or patch management can thwart a high percentage of attacks. In cases where limited personnel prevent federal agencies from implementing these best practices, a more regular access to skilled volunteers could make the difference. While the logistics of supporting an ongoing volunteer program does pose challenges, the Commission should closely study the benefits of a civilian corps that plays a role in day-to-day, steady-state cybersecurity activities. Most important, a more expansive program would provide far more opportunities for high-impact public service.

Second, a civilian cyber corps should have a more expansive mission that supports a range of national cybersecurity goals. While one potential model might limit support to federal entities alone, as the Memorandum appears to contemplate, many non-federal entities and private companies could benefit from a standing pool of skilled cybersecurity volunteers. For example, it was the lack of cybersecurity capacity across local governments and small businesses that pushed Michigan and Wisconsin to create the Michigan Civilian Cyber Corps and the Wisconsin Cyber Disruption Response teams. (These are discussed in detail below.) Allowing volunteers to leverage their cyber expertise to serve their own communities should be an important element of any national service program focused on cybersecurity.

Third, an effective volunteer civilian corps should draw its ranks from the broadest pool of appropriate expertise. Limiting membership to former federal cybersecurity employees carries the practical advantage of selecting volunteers who can readily obtain the proper clearances. A civilian corps established as a reserve to assist federal cybersecurity operations in emergencies will likely require access to sensitive resources, knowledge, and facilities. Conducting background checks during an emergency is impractical, and so building the corps out of pre-cleared, former federal employees is sensible. But if the Commission considers the value of a volunteer cyber

corps whose service includes assisting with day-to-day cybersecurity across a range of federal *and* non-federal entities, security clearances may not prove necessary for many important duties. Moreover, expanding the pool of volunteers not only goes to the heart of the Commission's task—maximizing opportunities for national service—but it would also fulfill critical needs in cybersecurity that former federal cybersecurity employees alone could not address simply because their numbers are too low.

Existing Models

Notwithstanding the recommendations above, the Commission should in any case investigate two existing programs at the state level that could serve as models for any national cyber volunteer corps.

The Michigan Civilian Cyber Corps (MiC3) was launched in 2013. Now codified in state law,[1] the MiC3 is an innovative attempt to close the cybersecurity skills gap by enlisting volunteers in the private sector as a standing pool of talent who can respond to cyber emergencies. (Originally, the MiC3 could only activate upon an emergency declaration by the governor. New legislation changed that requirement, and the MiC3 can now deploy without an emergency declaration.) The MiC3 depends on a close partnership between the Department of Technology, Management & Budget, the Michigan State Police, and the National Guard. Interested volunteers complete a straightforward application process, demonstrating that they hold one of any basic security certificates and two years' experience. They must also pass an online knowledge assessment to verify their credentials and demonstrate experience in incident response. They also must obtain and submit written authorization from their employer allowing them to take *up to* ten days off every year for cybersecurity training. (These training opportunities are an important incentive for volunteers to join the MiC3.) Finally, prospective volunteers must complete a background check and associated confidential disclosure agreement.

Wisconsin has implemented a similar program grounded in their Cyber Disruption Response Teams. After recognizing the increasing tempo of cyberattacks targeting local government entities, combined with the realization that such entities provide opportunities for attackers to pivot and compromise state systems, Wisconsin's Department of Information Technology applied to use funding from the Homeland Security Grant Program to train local officials and conduct exercises. These informal gatherings have morphed into three teams of volunteers—totaling thirty-six (36) individuals—from local government across the state, supplemented by a fourth team from the National Guard. Over the past two years, these teams have responded to over thirty (30) cybersecurity incidents affecting local entities.

Distinguishing characteristics between the two models include membership and formalization. In Michigan, MiC3 members may hail from the private or public sectors. The Wisconsin teams comprise public sector volunteers only, and in practice resemble the kind of cross-jurisdictional mutual assistance that is common among local entities (such as fire stations). It is also important

to note that the MiC3 has now been codified in state law, whereas the Wisconsin teams operate on an ad-hoc, albeit semi-formalized basis.

Challenges Facing a Volunteer Corps

Establishing a national cyber volunteer program would be a significant undertaking, and the concept is not without critics. At least one security expert has described the concept "an entirely misguided approach" that overestimates the amount of hours cybersecurity experts—many of whom are already overworked—have to volunteer.[2] The experience of Michigan and Wisconsin offers potential lessons for any national-level cyber volunteer corps.

First and foremost, if a volunteer corps were to expand its ambit to encompass non-federal cybersecurity experts, significant investment in a training program would be necessary to ensure that activated volunteers provide constructive assistance. In a security community where instructors and effective training resources are already limited, this might necessitate new federal funding or significant contributions from private and academic partners. But it is opportunities for training and certification that some volunteers in Michigan and Wisconsin have cited as important incentives for them to volunteer their time and effort. Also note that at the national level, the full portfolio of potential victims that might request volunteer assistance is diverse; a one-size-fits-all training curriculum might not be appropriate.

Second, it is critical to account for concerns by vendors that these efforts might compete with private sector solutions. Indeed, it is for that very reason that some in private industry express skepticism when policymakers express interest in heavier National Guard involvement in cybersecurity response. Recognizing this challenge, the Wisconsin volunteer teams are careful to focus on basic assistance or over-the-shoulder counseling. But there remains a constant tension between offering volunteer support that is helpful on the one hand, and a desire to avoid offering services that are too sophisticated and provoke complaints from security vendors.

Another set of challenges arise from potential liability for volunteers. At its outset, MiC3 organizers faced questions from potential volunteers and employers regarding how volunteers might be liable for their actions during a cybersecurity emergency. For example, what if an MiC3 volunteer, in the course of efforts remediate an attack on hospital IT systems, unwittingly exposed HIPAA-covered data? Would that volunteer face the threat of litigation? As one MiC3 volunteer explained, "'We'd be going into an organization where we have no idea how their network is set up or what type of information they have . . . If we find something and suggest they make a change and it breaks something within their network, if we're held responsible or liable for that, we'll lose a lot of members because we're volunteers.'"[3] These questions prompted Michigan to pass a law that protects MiC3 volunteers from liability for actions undertaken in the course of their duties. Any national volunteer program will need to consider similar solutions to address liability concerns.

Finally, mechanisms for building trust will be an essential piece of any national cyber volunteer corps program. It will be important to grow a social fabric that builds personal ties between would-be volunteers and the victim organizations they might be called on to assist.

Conclusion

Despite the above challenges, the Commission should strongly consider formally recommending that Congress appropriate funding to establish a national, volunteer cyber corps. The experience in Michigan and Wisconsin underscore the model's viability. Today, dozens of volunteers are giving up days of their time at their own expense, and requests for assistance from these volunteers continue to grow in both states. Other states, including Hawaii and Montana, are already considering following in the footsteps of Michigan and Wisconsin. It is likely that scaling similar programs to more states or to the entire country through a national service program would yield significant benefits for public service and cybersecurity.

---

[1] http://www.legislature.mi.gov/documents/2017-2018/publicact/pdf/2017-PA-0132.pdf

[2] Kevin Townsend, *Proposal for Cybersecurity Civilian Corps Gets Mixed Reception*, SECURITY WEEK (October 31, 2018), *available at* https://www.securityweek.com/proposal-cybersecurity-civilian-corps-gets-mixed-reception.

[3] Jenni Bergal, *Michigan's Volunteer-Based Cybersecurity Strategy Catches On*, GOVERNING (August 4, 2017), *available at* https://www.governing.com/topics/mgmt/sl-cybersecurity-volunteers.html.