Written Testimony of

Douglas C. Rapp, CISM

President, Cyber Leadership Alliance

Before the

U.S. House of Representatives, Subcommittee on Cybersecurity and Infrastructure Protection on Homeland Security and Subcommittee on Higher Education and Workforce Development of the Committee on Education and Workforce

Hearing on “Public-Private Solutions to Educating a Cyber Workforce”

October 24th, 2017

Thank you, Chairman Ratcliff and Chairman Guthrie and Members of the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection and Subcommittee on Higher Education and Workforce Development of the Committee on Education and Workforce for holding today's hearing on the extremely important topic of Public-Private Solutions to Educating a Cyber Workforce. As technology continues to connect us in ways that create synergy and solve complex problems more efficiently, so must we connect our public and private organizations to do the same. By integrating, understanding, and accepting our respective capabilities and differences, we can solve the difficult problem of educating a modern cyber workforce quicker and more efficiently. The Cyber Leadership Alliance, a 501c6 industry non-profit that represents the cybersecurity thought leadership of more than $20B dollars of Indiana industry, is dedicated to finding solutions to reducing the cybersecurity workforce deficit through effective use of public-private partnerships.

Indiana: A Case Study in Cyber Partnership

Indiana has long recognized the value of public-private partnerships. One need only to look at the Office of the Indiana Secretary of Commerce to see an example of a successful and enduring public-private partnership. Other successful public-private partnerships span utilities, emergency response and other areas.

Indiana is a State of collaboration that has figured out how to bring stakeholders to the table specifically in cyber security. Indiana has built coalitions across government, military, and industry to take a holistic approach to cybersecurity. Five specific examples of cybersecurity public-private partnerships are illustrated below:

Indiana National Guard Cyber Incident Response Plan – The Indiana National Guard Cyber Incident Response Plan was the first integrated response plan in the State targeted at a statewide cybersecurity incident. Through public-private collaboration during development, this plan was developed to define the role of State military cyber assets while coordinating the integration of State military, public, and the private sectors.

Indiana National Guard Cybersecurity Working Group – The Indiana National Guard Cyber Security Working group was the State's first formal public-private group to meet on a consistent basis and share information regarding significant cybersecurity issues. The group initially consisted of public entities such as the National Guard, Indiana Department of Homeland Security, the Indiana Utility Regulatory Commission, FBI and others. Private entities followed including Rook Security, Vespa Group, Pondurance, and Citizens Energy to name a few. This group no longer exists as three separate initiatives have arisen to fulfill the functions that were identified in this group.

Crit-Ex (Critical Infrastructure Exercise) – Crit-Ex was sponsored by the Indiana Department of Homeland Security, Indiana Office of Technology, the Indiana National Guard and was managed by the Cyber Leadership Alliance. The event, which is the first of its kind, brought together 2 federal agencies, 8 state agencies and 15 private sector organizations. The exercise was

formulated to explore the intersection between critical infrastructure and cyber security. Partnerships between the government agencies and private organizations made during the exercise are helping prevent major incidents in our current high threat environment. An important footnote is that while Crit-Ex was groundbreaking and spawned other initiatives, it has not been repeated in Indiana due to lack of funding and competing demands on government resources.

Indiana Cybersecurity Economic Development Plan – In 2016, the Secretary of Commerce of the State of Indiana Victor Smith, directed the creation of a State Cybersecurity Economic Development Plan as a component of his economic development strategic sector plan. Completed in early 2018, the plan was created by nineteen noted subject matter experts with input gathered during 7 cybersecurity town halls around the State of Indiana. Input from over 200 stakeholders from private industry, academia, government, and the military provided the data that shaped the final report. The plan gives significant attention to cyber workforce development and recognizes it as one of strategic 5 Lines of Effort. The report has been published and is currently available from the Indiana Department of Workforce Development (IEDC).

Indiana Executive Council on Cybersecurity – The Indiana Executive Council on Cybersecurity can be traced back through the working group for the Crit-Ex initiative to the Indiana National Guard Cybersecurity Working Group. The counsel, created by executive order under former Governor Mike Pence and continued by Governor Eric Holcomb is made up of government (local, state, and federal), private-sector, military, research, and academic stakeholders. The mandate of the counsel is to collaboratively increase Indiana's cybersecurity posture and maturity. With 28 Council members, 9 subcommittees, and more than 150 advisory members, the Council's first deliverable is a comprehensive strategy plan to Governor Holcomb by September 2018. One of the council's focus areas is cyber workforce development.

Addressing the Cyber Workforce Crisis

Currently, Indiana is approaching the shortage of cybersecurity workforce professionals like many other States - through its academic institutions. Indiana currently has 31 higher education institutions that offer cybersecurity education, 6 R1-R3 Research Centers, and 7 DHS/NSA Cybersecurity Centers of Excellence. However, the Cyber Leadership Alliance believes that the popular methodology of recruiting self-selected college-trained graduates to meet the cyber workforce demands is not only flawed but rather that anyone suggesting that as a solution is at best incapable of simple math. A visit to CyberSeek.org, an online cybersecurity workforce development tool created in a public-private partnership between the National Initiative for Cybersecurity Education (NICE), Comp-TIA, and Burning Glass will immediately invalidate that solution.

The partners within the Cyber Leadership Alliance believe that the most effective way to address the current cybersecurity talent crisis is by taking a holistic approach. Only by creating and following a long-term process of "growing your own" can you solve this problem. We have modeled that process and are currently proposing it to the Indiana Department of Workforce Development in the form of an application for a SkillUp! grant.

The Cyber Leadership Alliance SkillUp! Solution

The SkillUp! proposal is governed by a public-private partnership referred to as the Cyber Leadership Alliance Coalition (CLAC) and plans to inform, educate, grow, and retain an Indiana based workforce, with jobs awaiting them post-(re)training at the most critical levels of commerce. The SkillUp! solution is based on the following tenants:

Cybersecurity Workforce Development efforts must be driven by public private partnerships. No one private entity, industry sector, branch or level of Government should attempt to "own" cybersecurity.

Cyber Public – Private partnerships should be run by or always include non-profit industry organizations. These organizations provide a neutral ground where the direction of the project is more likely to be driven by the needs of the industry rather than political agenda or personal profit. Additionally, these organizations attract subject matter experts from across many sectors and industries.

Cyber Public-Private Partnerships must provide value to its partners. – These partnerships must understand and not be threatened by each other's agendas. Businesses need to understand that Governments are trying to solve complex problems while competing for limited resources. Government needs to understand that businesses can only participate in partnerships if they can afford to work at the rate at which the government is willing or able to pay. The allure of an appointment or invitation to a government partnership fades quickly when weighed against the responsibility of creating value for the shareholders.

Cyber Public – Private Partnership must reduce redundancy and capitalize on core competencies. Participants in partnerships should be vetted for their expertise and ability to produce results. Competing interests and inclusion for any other reason than expertise is counterproductive to measurable results.

Cyber security public-private partnerships should capitalize on and use the most accurate data available. Whenever possible, the creation of cybersecurity workforce should directly correlate to the needs of the market. Partnerships should receive demand data directly from employers and match those needs to the programs and institutions that produce the required skills.

Cybersecurity Public – Private Partnership must be creative and disruptive when necessary. The workforce deficit in cybersecurity is showing little signs of getting better. Current methodologies are routinely failing to produce the required result through the traditional method of granting block funding to government subsidized higher education. This problem will only be solved with careful analysis, accurate data and creative and disruptive ideas. Ideas such as allowing coding to be utilized to fulfill a foreign language credit in high school or offering incentives to cybersecurity professionals to purchase a house within a State's borders could produce unprecedented results if resources and political support are given.

Thank you for the opportunity to be here today and I look forward to answering any questions that you may have.

Douglas Rapp, CISM