To: Kevin Kimball, *Chief of Staff, National Institute for Standards and Technology (NIST), Department of Commerce*

From: Simone Petrella, *Chief Cyberstrategy Officer, CyberVista LLC*

Date: August 1, 2017

Re: NIST Cybersecurity Workforce RFI

CyberVista is pleased to submit the following response to NIST's Cybersecurity Workforce Request for Information (RFI) on the scope and sufficiency of efforts to educate and train the cybersecurity workforce. CyberVista is a cybersecurity training and workforce development company based in Washington DC. Our mission is to create a cyber-ready workforce through personalized training programs that provide organizations with people, knowledge, and skills required to defend their most critical assets. CyberVista is a wholly owned subsidiary of Graham Holdings Company (NYSE:GHC) and sister company to Kaplan, Inc. and brings innovative education technologies and personalized approaches to learning.

General Information

1. *Are you involved in cybersecurity workforce education or training (e.g.,curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)?*

   CyberVista is a cybersecurity training and workforce development company. Our current area of focus is on cybersecurity curriculum development for and delivery of highly demanded security certifications in the cybersecurity industry. Many of these certifications are enumerated and required by Department of Defense Directive (DoDD) 8140, which provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. We develop curricula that support these exams by creating programs that start with a diagnostic assessment, provide personalized feedback, and deliver modular learning content. We bolster this learning pedagogy by reinforcing learning through frequent practice and reinforcement, using innovative technologies and a robust learning management system.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. *What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?*

   The National Initiative for Cybersecurity Education's (NICE) Cybersecurity Workforce Framework (NCWF) contains the most comprehensive data set of U.S. Government cybersecurity job roles and the associated knowledge, skills, and abilities (KSAs) required for each of those roles. That data, however, is largely unorganized and unranked regarding the priority certain skills may have over others. Data around the specific characteristics and qualities that make a candidate qualified for any one of these roles is only truly impactful when it can be distilled into testable traits that training and education providers can use to develop curricula. KSAs are most often the result of a job task analysis, which provides critical insight into a job role's duties and responsibilities. However, the

data contained in the framework could be vastly improved if the KSAs currently identified are validated against qualified individuals excelling in their associated cybersecurity roles to parse out the testable qualification areas from those that are more qualitative in nature.

Another useful data set can be found on Cyberseek (cyberseek.org), which is an interactive data set that provides a detailed snapshot of supply and demand in the cybersecurity job market, as well as a breakdown of most requested skills in job requisitions and descriptions. This serves as the first consolidated snapshot of open job roles and associated skills requested within each of these job roles, including associated salaries and job openings by state. The limitation of this data, however, is that the data is primarily created from open job requisitions, which lack a common lexicon and don't uniformly use the NIST Cybersecurity Workforce Framework job roles definitions and descriptions when it comes to defining skills that are critical at each particular job role. For example, Cyberseek will list both Information Security and SQL on the required skill list for a given role without a level setting of priority within a job role. Information Security is a broad concept and topic which is foundational to all cybersecurity roles but can also be found in candidates in varying levels of depth and sophistication while SQL is a very specific query language used to interact with databases and would be a primary requirement for a database administrator. Further developing this data set to utilize a common lexicon for skills that can truly be compared and differentiated across job roles would be instrumental in helping educators and curriculum developers to focus on course creation that develops skills most needed in the workplace from a practical and implementation perspective.

2. *Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?*

   The NCWF has resulted in significant strides when it comes to understanding and agreeing to U.S. Government workforce categories and common functions. While its stated and intended purpose has been to create a common language to categorize and describe cybersecurity work, the reality is that there is still a significant amount of overlap, redundancy, and discrepancy in how agencies and other employers in the United States refer to certain job roles. Job titles and descriptions still vary widely from organization to organization and sector to sector. Additionally, since the NCWF only applies to federal government positions, talent management is difficult when looking to recruit from the private sector since few, if any, private sector employers follow the job roles as outlined in the NCWF. Without a common lexicon that transcends the public and private sector, there will continue to be a lack of understanding and agreement over which roles are truly transferable versus those that are particularly aligned to government work and authorities.

3. *Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?*

   As a workforce education company, CyberVista supports training and education of its own staff by providing each employee carte blanche access to our own cybersecurity courses and trainings. Staff are also encouraged and scheduled to attend courses in new areas of cybersecurity/technical training and others that emphasize best practices when it comes to curriculum development and learning delivery.

4. *What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy v.s financial sectors)?*

In the course of dozens of conversations with cybersecurity employers, hiring managers will primarily cite emotional intelligence (EQ) and analytic thinking as the primary skills they need as they build their cybersecurity workforce. The underlying reason for this is that cybersecurity knowledge and technical ability can largely be trained, while EQ and critical thinking are more innate skills that can't necessarily be taught.

Current employer expectations are often not realistic when it comes to job roles. Many job descriptions are written poorly, require more years of experience than a certain technology has even been around, and prefer to solve the short-term problem through poaching talent as opposed to taking longer-term solutions aimed at growing their own/growing the pipeline. Where employer expectations are realistic is when it comes to the student pipeline. There is an expectation (and in larger employers, robust internal programs) that universities are not producing students with the tangible skills/abilities in order to effectively perform their job tasks. Much of the actual training occurs through internal programs, on the job training, and mentorship at work.

Knowledge and skills does vary by sector, but the vast majority of demonstrable ability is consistent, agnostic of industry. The biggest variance comes from the specific networks and systems a particular industry relies on and providing staff with the applicable exposure and training in order to effectively operate on (or secure) those systems. For example, banking security means a level of knowledge of SWIFT, while critical infrastructure requires literacy in ICS/SCADA.

As we examine the student pipeline, we see that university degrees in cybersecurity vary greatly and over-emphasize computer science skills (in fact, a majority of cybersecurity degree programs are merely modified computer science degrees). Given the current lack of focus relative to soft skills , the need for well-rounded candidates at the student pipeline level is paramount. Currently the issue is compounded as the hyper-technical who may succeed in independent vulnerability exploitation or hacking research often lack the skills to work in a corporate or agency team systems of systems environment.

5. *Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?*

Organizations like the Department of Defense (DoD) and the Department of Homeland Security (DHS) are developing, curating, and delivering some of the most effective cybersecurity skills training to their staff in the U.S. Government. On the private industry side, some of the most effective cybersecurity training is happening through on the job and internal programs. Companies like GE, Booz Allen, Raytheon, Sands Corporation, and American Express all have robust internal training and workforce development programs. These corporate programs in particular are effective because they focus on the job roles most needed across the enterprise and work backwards to determine the skills and knowledge staff and candidates need to succeed in those particular roles. From there, they are able to provide programs and training to give their staff access to the resources they need to accumulate needed skills.

The largest limitation in these programs, regardless of their success, is their ability to scale. Providing a robust training program, developing internships, and investing in cybersecurity staff development takes time and is costly. Regardless of industry or area of expertise, training budgets are

often the first to get cut. Without consistent and significant buy in from the top of the organization, security teams spend an inordinate amount of time continuing to justify their training budgets, resulting in inconsistent application of workforce development in the cybersecurity space.

6. *What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?*

There are three primary challenges facing the Nation and employers: 1) lack of a consolidated and cohesive cybersecurity training initiative that defines the real areas of expertise needed within the workforce from a job role and performance perspective, 2) funding, and 3) marketing and recruiting new candidates into the cybersecurity field.

Regarding a comprehensive national strategy, initiatives like NICE and the NCWF have made some progress in this area, but are still approached from a removed academic perspective and lack the input of the actual mission from the public or private sector. Other initiatives across the U.S. Government to inventory and track cyber positions have been done repeatedly but have borne little fruit. For example, the DoD has gone through at least three separate exercises to inventory job codes that perform "cyber functions" since 2007. On the funding issue, government spending on cybersecurity is significant but is implemented through a series of fragmented programs through a variety of agencies. Some of this is necessary in order to test hypotheses and identify programs that work, but there is very little consolidated follow up to really scale those programs once they are deemed effective.

Workers (and employers) have the additional hurdle of the high cost of obtaining cybersecurity education and training. The cost of developing innovative and next generation cybersecurity curricula and programs by universities, education institutions, and training providers is significant, forcing them to sell programs at a price point that becomes cost prohibitive for individuals and their employers. Even employers that provide some amount of training budget to their staff are unable to fund the full suite of knowledge training a worker might need over the course of their career, leading to retention issues.

Lastly, the cybersecurity industry has been slow to actively market and promote cybersecurity as a hot new field. There have been continued challenges to attract real diversity into cybersecurity positions and retain diverse candidates once they've entered the field. As an example, according to the 2017 Global Information Security Workforce Study, women are globally underrepresented u the cybersecurity profession at only represent 11% (14% in North America) whereas in the United States women comprise 48% of the workforce. Without a workforce full of a variety of backgrounds, experiences, and education, the profession suffers from lack of well-rounded perspectives, which is what it needs to ultimately create more secure infrastructures.

The biggest opportunities the Nation, employers, and workers have in cybersecurity education are a direct result of all the challenges outlined above: 1) establish a cybersecurity "moonshot" effort, and 2) fund, create, and encourage recruiting efforts into cybersecurity.

A cybersecurity moonshot would provide the United States with the opportunity to invest in cybersecurity in the same way it did during the space race at the end of the 20th century. By creating, funding, and prioritizing both defensive and offensive cybersecurity programs, the U.S. can position itself not only as the most secure nation in the world, but also actively create hundreds of thousands of jobs that prepare people to operate and succeed in the 21st century economy. This moonshot could,

and would, include funding and marketing efforts to show candidates (both transitioning professionals as well as K-12 students) the opportunities, benefits, and excitement pursuing a career in cybersecurity brings.

7. *How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?*

   Advances in Artificial Intelligence (AI) and machine learning have, and will continue to, enhance our ability to collect greater and larger data sets, allowing us to develop strategies and mitigations that more effectively implement effective security controls. This will change the needs of the cybersecurity workforce by reducing some of the more basic and entry-level positions while increasing demands for human analysts to interpret and act on machine-driven data.

   The Internet of Things (IoT) will likely create even additional workforce needs. Currently IoT developers and manufacturers are not "baking" security into their products. It is faster and cheaper for them to prioritize getting a product to market over ensuring that product is secure. However, customer demand, privacy concerns, and regulations are starting to change the way manufacturers think about IoT from a security perspective. As that realization occurs and IoT companies start to invest more in the security of their devices, they will need to invest and hire in security personnel they are not currently investing in today. That will result in new security-related jobs in new industries where a plethora of cybersecurity positions do not exist today.

8. *What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:*

   At the Federal level, the following steps should be considered:
   - NICE should continue to lead the development of the workforce framework, but work more closely with U.S. Government agency and private sector employers to better articulate the practical knowledge and skills needed within each job role.
   - The U.S. government should introduce a cyber moonshot effort around increasing cybersecurity education dedicated to developing core curricula based on conceptual and practical learning best practices. Funding for curriculum and program development should be made available to universities and training companies, although limits should be put on that funding to ensure collaboration with employers to best determine how curricula support actual job role needs.
   - The Federal Government should leverage its convening power to bring both employers and educators (academic and industry) to the same table to discuss the greatest skills gap needs. This working group should be responsible to develop a set of requirements and common lexicon, that training providers can use to build and deliver programs that actually meet workforce demand.

   At the state or local level, including school systems, the following steps should be considered:
   - States should be incentivized to develop and integrate basic computer science and cybersecurity curricula into their school systems. This includes evaluating new innovations

in education gamification and identifying new ways to attract more girls and other diversity candidates into computer science and security.
- States in current geographies with heavy emphasis on manufacturing economies at risk of losing jobs to automation should implement programs to allow adults to gain training that allows them to transition into a cybersecurity field while giving them a safety net during that period of time where their focus should be on learning and not maintaining an income in their old industry.

In the private sector, including employers, the following steps should be considered:
- Provide incentives for businesses to identify existing staff that have the aptitude to be retrained into cybersecurity jobs. This can help to alleviate the current poaching model in the market today which drives salaries up yet doesn't help create more supply.
- Create and promulgate a job requisition model that uses a common lexicon (whether set by NICE or other) that allows job seekers/candidates and employers to quickly understand the role that's being filled. This would be used to reduce the amount of overlap and confusion there is based on job titles today.

For education and training providers, the following steps should be considered:
- Provide funding and/or incentives to education and training providers to build cybersecurity curricula that address the skills needs as articulated by actual employers (whether public or private sector).
- Incentivize academic institutions and education providers to actively seek input and feedback from employers to ensure curricula/programs developed are actually producing the right candidates and employees. Create a lifecycle that forces those institutions (and funds it as appropriate) to modify and implement new requirements based on employer feedback and changing job role priorities.
- Create a systematic and consistent method of education that utilizes cutting edge learning technologies and minimizes the reliance on singular instructors
- Integrate practical educational into curricula wherever possible, including but not limited to internship programs, externships, and lab-based environments.

For technology providers, the following steps should be considered:
- Create and promulgate a job requisition model that uses a common lexicon (whether set by NICE or other), identical to that used in the private sector section above, which allows job seekers/candidates and employers to quickly understand the role that's being filled.