August 2, 2017

To: **National Institute of Standards and Technology**

RE: **Response to Request for Information, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development"**

Via e-mail to: cybersecurityworkforce@nist.gov

Palo Alto Networks appreciates the opportunity to respond to the National Institute of Standards and Technology's (NIST) Request for Information, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development."

We commend NIST's efforts to solicit input from a broad range of cybersecurity stakeholders on the crucial task of supporting the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors. The challenge is acute. According to the latest *Cybersecurity Jobs Report* by Cybersecurity Ventures, the worldwide deficit of qualified cybersecurity professionals will reach 3.5 million by 2021. A deficit of this magnitude can inhibit the industry's ability to prevent cyber incidents, and the challenge is compounded by the growing frequency and sophistication of cyberattacks. Getting ahead of tomorrow's threats requires a larger, diverse and innovative team of cybersecurity professionals.

At Palo Alto Networks, we have approached this challenge by creating scalable programs that address structural issues in three areas: 1) cybersecurity education; 2) training; and 3) workforce development.

Education: Eliminating Traditional Barriers to Access to Cybersecurity Education

In June, Palo Alto Networks announced a collaboration with the Girl Scouts of the USA (GSUSA) to deliver the first-ever national Girl Scouts cybersecurity badges. Working with a panel of expert cybersecurity advisors, GSUSA and Palo Alto Networks are developing a series of 18 cybersecurity badges which we expect to begin rolling out in September 2018. Our goal is to provide cybersecurity education to over a million girls throughout the United States while helping them to develop their problem-solving and leadership skills.

We believe this collaboration will go a long way toward eliminating traditional barriers to access to cybersecurity education, like gender and geography, and will cultivate an early interest in cybersecurity by girls ages K-12. In addition to providing widened access to

cybersecurity skills development, this collaboration will provide online safety education and activities to deepen interest in cybersecurity as a career.

Building interest in STEM at a young age is crucial. According to the Computing Technology Industry Association (CompTIA), 69 percent of women who do not have a career in information technology cited not knowing what opportunities were available to them as reasons they did not pursue one. With this collaboration, Palo Alto Networks and GSUSA plan to introduce cybersecurity education to millions of girls across the United States through programming designed to increase their interest and instill in them a valuable 21st Century skillset. This national effort will target girls as young as five years old, helping to ensure that even the youngest girls have a foundation primed for future life and career success.

Training: Hands-On Experience for Students, and Integrating Cybersecurity into the Boardroom for the C-Suite

Cybersecurity training must also be given high priority as the sophistication, complexity and sheer volume of successful cyberattacks increases and threatens our digital way of life. Large-scale programs, accessible to students, are vital to developing a pipeline of well-trained and qualified cybersecurity professionals. To advance this goal, Palo Alto Networks dedicates significant resources to helping colleges and universities address the critical shortage of cybersecurity professionals. The Palo Alto Networks Academy creates partnerships with qualified colleges, universities, and technical institutes to provide next-generation security technology, courseware, certification, and training labs incorporated into academic cybersecurity curricula. The Academy's goal is to make teaching state-of-the-art cybersecurity technology as easy as possible for instructors while providing a hands-on learning experience for students, resulting in a core curriculum of relevant, immediately-useable knowledge and skills based on practical experience for success in the cybersecurity industry. The Academy program is currently active with more than 200 partner universities and colleges in more than 26 countries.

Cybersecurity training should not, however, be limited solely to a company's cybersecurity professionals. C-Suite leaders must also have the knowledge base, skills and tools needed to mitigate the cyber risks inherent in our digital age. To that end, Palo Alto Networks in conjunction with NYSE developed a book series to bring cybersecurity awareness to business leaders: "Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers." These books collect the expertise and experience of CEOs, CISOs, lawyers, forensic experts, consultants, academia, and current and former government officials to address current cybersecurity issues that businesses must consider, such as how to manage strategic cybersecurity initiatives at the boardroom level, compliance and breach avoidance, and prevention and response. The goal is to

ensure leaders see cybersecurity and risk management as an extension of, rather than a barrier to, their business operations and growth.

Workforce Development: Extending Educational Opportunities to Bring Veterans into the Cybersecurity Industry

Another element of building the cybersecurity workforce of the future entails extending our educational reach beyond students and those professionals who already have a strong cybersecurity background. To advance this goal, Palo Alto Networks has collaborated with VetsInTech to bring more veterans into technology and cybersecurity roles.

Veterans are valuable assets in our industry, because their service gives them skills that make them uniquely qualified for careers in cybersecurity. Yet one of the biggest challenges many veterans face is a lack of confidence in their skills relative to private industry needs, particularly for high technology. They often overlook their intangible skills like dedication, initiative, self-motivation, communication and leadership reporting. In fact, many veterans find they already have cybersecurity-related training, such as intelligence gathering from electronic, signal, human and imagery sources, or even threat analysis and tracking. Thus an important component of our work with veterans – in addition to a core cybersecurity training curriculum – includes insights on life after the military, how to translate military skills into civilian cyber skills, best practices for applying for jobs in Silicon Valley, and resources to help move closer to careers in cybersecurity.

Conclusion

Building an effective cybersecurity workforce requires addressing structural issues in education, training, and workforce development: eliminating traditional barriers to access to cybersecurity education; integrating cybersecurity training into college curricula and into the boardroom; and expanding training opportunities to bring those with translatable skill sets into the cybersecurity industry. Should the Commission require any additional information about the programs discussed within this response, we would be happy to set up further discussions. Any questions may be directed to Coleman Mehta, Senior Director, U.S. Policy (cmehta@paloaltonetworks.com). Thank you for the opportunity to comment.