JAMES R. LANGEVIN
2ND DISTRICT, RHODE ISLAND

COMMITTEE ON ARMED SERVICES
EMERGING THREATS AND CAPABILITIES (RANKING)
SEAPOWER AND PROJECTION FORCES
TACTICAL AIR AND LAND FORCES

COMMITTEE ON HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE PROTECTION
EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

Congress of the United States
House of Representatives
Washington, DC 20515–3902

WASHINGTON OFFICE:
2077 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225–2735
FAX: (202) 225–5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732–9400
FAX: (401) 737–2982

https://langevin.house.gov

August 1, 2017

Ms. Danielle Santos
Cybersecurity Workforce RFI
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Dear Ms. Santos:

The National Institute of Standards and Technology has requested information on the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future. Investment in our nation's cybersecurity workforce is crucial to our national and economic security, and I write to applaud NIST for its efforts in this matter. While we often focus on the technologies that result from research, it is at least as much the skilled workforce behind the breakthroughs that drives our country forward.

Unfortunately, we are far behind where we need to be. Within the cybersecurity workforce today, we have hundreds of thousands of jobs unfilled, thereby limiting our ability as a nation to respond to the malicious actors who daily target our infrastructure, finances, and intellectual property. We need short, medium, and long term solutions that reach all components of the educational pipeline from K-12 education to university programs to certifications. We also need to explore retraining and apprenticeships as ways to infuse additional talent into the field.

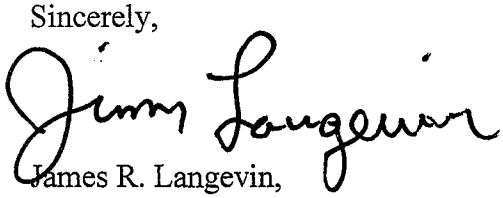
In order to properly understand the scope of the challenge, it is crucial that NIST applies measures and metrics to the cybersecurity workforce, and I was pleased to see their inclusion within the request. As a nation, we must analyze the expected demand for cybersecurity personnel, the efficacy of training programs in producing skilled workers, and the ability of our educators, both in number and in capability, to instruct students. Furthermore, we must share across our communities the lessons and best practices learned from these studies to ensure that

students throughout the nation have access to the best cybersecurity education possible no matter where they live.

Additionally, the dynamic nature of technology development ensures that even our best laid plans will require adaptation as innovative technologies come on the market. This is perhaps one of the most significant challenges that we will face in shaping tomorrow's workforce, and it will require novel approaches to training. The emerging use of artificial intelligence to assist cybersecurity tasks, for example, may dramatically alter the tasks of a computer and network security engineer in the coming decades. Similarly, the rapid growth in connected devices may create new classes of cybersecurity professionals focused on the unique challenges posed by the Internet of Things. We must prepare our workforce for this future while also preparing them to be adaptable to the disruptions that we expect but cannot predict.

Only by continuing to invest in our skilled workforce will we be able to ensure our nation's continued security and prosperity in the digital economy. This request for information is a positive contribution to understanding where the workforce is today and what we must do in the future. I thank you for your leadership on this issue and I look forward to the results of your request.

Sincerely,



James R. Langevin,
Member of Congress