BHEF BUSINESS-HIGHER EDUCATION FORUM®
Creating Solutions. Inspiring Action.®

2025 M Street, NW, Suite 800
Washington, D.C. 20036

phone: (202) 367-1189
fax: (202) 367-2269
www.bhef.com

August 2, 2017

National Institute of Standards and Technology (NIST)
U.S. Chamber of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Re: Docket Number 170627596-7596-01, Document Number 2017-14553

Dear NIST Representatives:

The Business-Higher Education Forum (BHEF) is pleased to submit this response to NIST's Request for Information (RFI) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development.

The cybersecurity talent gap is growing.[1] In 2015, approximately 209,000 positions went unfilled, and demand is expected to increase.[2] In a 2016 Business Roundtable (BRT) survey of 177 member companies on workforce talent, BRT found that:

- Over half of respondents believe that talent gaps are problematic or very problematic for their company and their industry, and almost all believe that the gaps are at least somewhat problematic.
- Talent gaps exist across skill categories with general applied knowledge, STEM-specific skills, and workplace skills all cited as both highly relevant and in short supply.
- Identifying qualified and diverse applicants remain a challenge with more than half of respondents facing difficulty in finding qualified candidates for open engineering positions and most companies struggling to hire qualified, diverse candidates.
- Members mainly rely on apprentice / intern programs, employee referrals, and social media to recruit with most recruiting from 4-year colleges and universities and only half focused on community colleges.
- Respondents are investing to close the talent gap with a combined $4.5 billion per year in employee learning and development programs, which is likely to increase in future years. [3]

Closing the cybersecurity talent gap — both existing and emerging — will require an expansion of strategic partnerships between business and higher education as well as investments in new talent development and recruitment strategies.

BHEF has catalyzed many such partnerships. As the nation's oldest membership organization of Fortune 500 CEOs, college and university presidents, and other leaders dedicated to the creation of a highly skilled future workforce, BHEF and its members form strategic partnerships to build new talent pathways; improve alignment between higher education and the workforce; and produce a diverse, highly skilled talent pool to meet demand in emerging fields. BHEF members are leaders in developing strategic partnerships that have the potential to transform higher education programs to meet employers' cybersecurity talent demands rapidly and have engaged in a number of initiatives and partnerships to meet those demands.

As part of its broader strategy to meet the cybersecurity talent needs of U.S. employers, BHEF facilitates the Future Cyber Leaders program in the Washington, D.C. metropolitan region, a summer professional development program that exposes undergraduate students to the wealth of career opportunities in government and defense available in cyber. This program has been generously supported by the Office of Naval Research. In its second year, program participants included interns from Northrop Grumman Corporation and Raytheon Company from 10 colleges and universities across the U.S. The program incorporates proven methods of attracting and retaining students in high-demand science, technology, engineering, and mathematics fields, such as experiential learning, into its design, establishing itself as a "gold standard" of cyber internship initiatives.

In partnership with the Commonwealth of Virginia, BHEF published a report, *Gaining Ground in Virginia: Challenges and Opportunities Across Cyber-Physical Systems*, detailing the challenges and opportunities at the intersection of cyber-physical systems (CPS) and the Internet of Things, autonomy, and critical infrastructure. It also emphasized Virginia's world-leading technology ecosystem and the need to align the educational system with workforce needs.[4] In addition, three case studies accompanying the report highlighted:

- Raytheon Company's work to address increasing cyber threats through the use of autonomous technologies.
- Northrop Grumman Corporation's work in addressing threats to critical infrastructure through its highly skilled workforce, robust internal research and development program, and partnership with government and academia.
- Telos Corporation's work to address the growing attack surface from the Internet of Things through representation on the Commonwealth of Virginia's Cyber Security Commission, work on its Innovation Committee, and its internal information security efforts.[5]

Building on previous work commissioned by BHEF on cybersecurity demand from Burning Glass Technologies, BHEF's publication, *Understanding Cybersecurity Talent Needs: Findings From Surveys of Business Executives and College Presidents*, provided firsthand viewpoints of the relationship among government, business and higher education sectors in developing a workforce that meets today's cybersecurity skills needs. Among its findings, business executives shared a belief that multiple strategies could be helpful in building a pipeline of cybersecurity talent, and in particular, 83% said that knowledge sharing among companies would be helpful in building a cybersecurity talent pipeline.[6]

Based on data from a 2017 Gallup survey of business executives and higher education leaders, a Burning Glass Technologies jobs analyses, and detailed student demographic and wage data, BHEF's publication, *Invest to Improve: The Cybersecurity Talent Deficit*, provided seven recommendations for stakeholders to pursue in support of the development and retention of professionals with cybersecurity skills.[7]

Recommendations:

- Align investments to support a cyber workforce: *coordinate to leverage others' investments*
- Re-examine the role of certifications in hiring and career development: *modernize certifications to reduce constraints on hiring talent*
- Create new models to develop talent: *invest in innovative models to build skills at all levels*

Strategic Investments for Employers:

- Focus the talent recruitment model on career mission and opportunities: *capitalize on the increased public interest in cybersecurity*
- Invest and recruit at higher education institutions with diverse student populations: *build relationships to expand talent pool*

Strategic Investments for Higher Education:

- Graduate students with proven skills needed for a cybersecurity career: *provide students with real-world experiences*
- Design inclusive educational pathways: *reduce barriers between academic departments to increase the number of students exposed to cybersecurity*

Strategic business-higher education partnerships are critical to developing the cybersecurity talent that our economy needs, and BHEF welcomes others to join its efforts to build those partnerships and close the cybersecurity talent gap.

We greatly appreciate the opportunity to respond to this RFI. If you have any questions or need any additional information, please do not hesitate to contact Debbie Hughes, Vice President of Higher Education and Workforce, at debbie.hughes@bhef.com.

Regards,

Brian K. Fitzgerald, Ed.D.
Chief Executive Officer

---

[1] The 2015 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, 2015.
[2] Demand to Fill Cybersecurity Jobs Booming, Ariha Setalvad, March 31, 2015.
[3] Business Roundtable 2016 Education & Workforce Survey: Survey Results and Analysis, September 2016.
[4] http://www.bhef.com/publications/gaining-ground-virginia-challenges-and-opportunities-across-cyber-physical-systems
[5] http://www.bhef.com/publications/cyber-physical-systems-case-studies
[6] http://www.bhef.com/publications/understanding-cybersecurity-talent-needs
[7] http://www.bhef.com/publications/invest-improve-cybersecurity-talent-deficit