Pikes Peak Community College

Response to Executive Order 13800 RFI
Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

1. Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)?

Pikes Peak Community College (PPCC) offers academic, corporate, and community programs in cybersecurity. The College is located in Colorado Springs and surrounding communities along the Southern portion of Colorado's Front Range, just 60 miles south of Denver. Established in 1968 and accredited by the Higher Learning Commission, PPCC offers 158 associate degrees and certifications in career and technical fields. With three campuses, two learning centers and two military education centers, PPCC provides access to a quality, affordable and flexible education.

Our 19,000 students range from high school graduates seeking transfer path to four-year schools to veterans transitioning into the civilian workforce to the unemployed or under-employed looking for fresh starts in such high-paying careers as cyber security and advanced manufacturing. In addition, PPCC offers a full array of non-credit corporate and workforce training programs. These programs usually lead to industry-recognized credentials in a variety of high demand occupations for the region. PPCC also offers middle and high school career exploration and experiential programs that build upon PPCC curriculum. The College enrolls an additional 1,500 students annually into these programs.

2. *If so, in what capacity?*

PPCC's cybersecurity offerings include:

- An Academic Cybersecurity Certificate, offered since 2013, and a Computer Networking Associate of Applied Science Degree with a focus in Network+, offered since 2015.
- An Associate of Science Degree in Computer Science, allowing students to transfer to four-year university programs in computer science.
- An Associate of Applied Science Degree in Computer Information Systems.
- Corporate and Workforce Training, to include
    - Industry Certification Training: (i.e., Network+ Security+, Certified Ethical Hacker)
    - Non-Credit Industry Training Courses in secure coding practices
    - Non-Credit Cybersecurity Modularized Professional Development Courses
- High School Academic programs, including:
    - Articulation agreements with area high schools
    - Concurrent enrollment programs at area high schools
    - High School programs offered at PPCC campuses in selected disciplines

PPCC community involvement and cybersecurity workforce development and education initiatives include:

- *The Pikes Peak Regional Defense Assistance Program:* The Colorado Springs Chamber and Economic Development Corporation, PPCC is undertaking an economic

development strategic planning process focused on cybersecurity this fall, to include working with PPCC to develop cybersecurity education and training capacity. PPCC serves as the lead agency on the Department of Defense Office of Economic Adjustment grant that supports this initiative.

- *The RAMPS Western Region Cyber Prep Program:* PPCC is the lead agency for the NIST, National Initiative for Cybersecurity Education (NICE) Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) program for the Western Region of the U.S. This partnership is designed to help teens to choose cybersecurity careers by defining cybersecurity career pathways, supporting the development and growth of cybersecurity programs in area high schools and offering teens meaningful work experiences, including internships and apprenticeships.

3. Growing and Sustaining the Nation's Cybersecurity Workforce

a. 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?

There are three data sources we believe are important for workforce development planning and implementation: data on labor demand, labor supply, and metrics about education and training program quality and outcomes.

With respect to labor demand, understanding the number and types of jobs available regionally, statewide, and around the nation is imperative. On a national scale, the NICE CompTIA cybersecurity heat map, called CyberSeek, is the best source available today for general geographic statistics and demand information about cybersecurity. In addition, several public and private sources of labor demand data that have been useful to us. Of note are the state-sponsored supply and demand data offered at the Colorado Labor Market Information Gateway (www.colmigateway.com), data about available jobs aggregated by Talent Neuron (formerly WANTED Analytics), and demand forecast data from private firms like Economic Modeling Specialists International (EMSI).

However, these data are only as good as their source information, and cybersecurity jobs are hard to find among the available occupational data, requiring a deeper analysis than most tools are capable of offering today. First, most cybersecurity-focused jobs are still emerging from more traditional information technology (IT) occupations like network administrator or systems analyst. This is especially true in smaller firms where the IT staff wear many hats. Our region is dominated by smaller companies employing a few IT generalists, so this makes demand analyses more labor intensive in our region.

Second, in some sectors, cybersecurity jobs are maturing far faster than the systems that capture and report labor demand data. For example, Department of Defense contractors providing cybersecurity services have developed very specific job requirements and descriptions, yet these positions still aggregate to occupational codes that emphasize one aspect of the work—like Network Analyst or Software Developer—when the new breed of cybersecurity worker is often required to do a great deal of work within both of these occupations.

Likewise, among commercial firms offering cybersecurity defense and detection services, occupations are often listed in the Protective Service occupation, right alongside security guards and physical asset protection positions. As the field matures, it is expected that jobs like these will merit their own occupational titles. Until then, these emerging jobs will continue to be buried in the data.

Most demand analyses include job postings as a data source. In our region, where many contractors compete for defense and other government IT contracts, job postings may exaggerate demand, as many companies competing for contracts will post similar openings, hoping to recruit and sign new talent contingent on an awarded contract. Thus, we have had to be cautious in our approach to estimating labor demand from these sources. On the other hand, because many smaller firms require cybersecurity skills among their more generalist IT staff that have generic job titles, we also know that we must consider a certain number of these generalist positions as having a cybersecurity focus. Whether this consideration balances the overestimation of contractor positions is difficult to determine.

In order to get more clarity about this concern, we have taken an additional step in our demand analysis. Organizations like the Computing Technology Industry Association (CompTIA) have done a thorough job of putting in place certifications with the goal of standardizing the knowledge base of students and future cybersecurity workers. We decided to review job descriptions from the 59 local cybersecurity companies in our region most likely to higher PPCC graduates by assessing their open positions based on the industry certifications required for the job, not just on the knowledge, skills and abilities listed.

This analysis showed us the certifications we needed to help students attain if they are to be successful locally; these certifications formed the basis of our new degree and certificate programs. However, through this analysis, we also learned that companies do not always align job descriptions with the certifications required. For example, some companies require the CISSP certification for entry-level positions, yet this credential requires five years of continuous work experience in cybersecurity, a credential that puts employees far above entry-level work.

Indeed, this has been a problem with federal contracts as well, where bachelor's degrees are often the government's required threshold credential for entry-level cybersecurity jobs. Companies report that they would prefer to either substitute industry credentials for higher education minimums or designate an Associate of Applied Science (AAS) degree as the minimum requirement. Why? Employers tell us that AAS graduates understand theory and have learned enough applied skills to perform in the job, and because they have completed their program in two years or less, their knowledge is still relevant in the workplace. Local firms report great difficulty in recruiting for these positions, where their most knowledgeable candidates lack a bachelor's degree.

Finally, we have tried to estimate demand for PPCC graduates by analyzing the job postings of companies with the region's cybersecurity industry that are most likely to hire our graduates. This, too, has proven somewhat problematic as companies self-identify their North American Industry Classification System (NAICS) codes, so companies providing a similar range of cybersecurity products and services may classify themselves very differently within broader IT services or industries. As a result, we now focus on companies within 13 different NAICS codes in our region as those that comprise our region's cybersecurity industry, and must sort through

data about these firms from among the larger group of companies listed within these 13 codes. Just as with cybersecurity occupations, the cybersecurity service industry is emerging as well, maturing faster than the data systems that capture its growth.

The most useful workforce development analysis tool we found as we gathered, analyzed, and disseminated demand data was the National Cybersecurity Workforce Framework (the Framework), which outlines 31 functional work specialties within the cybersecurity field. It provides a common understanding of, and lexicon, for cybersecurity work and groups similar types of work into categories and specialty areas. The Framework, developed by NICE, serves as a comprehensive way to define cybersecurity work in any organization.

With respect to labor supply, PPCC does collect and report student data by program as does every public college and university in the country. However, the data reported about our college nationally is about a small subset of students at the college—first time, full time college students—which comprise less than five percent of our student body. As a result, it is difficult for employers to use national data to understand the supply side issues they face because data collection and reporting is limited by the scope of the current data set.

In our region, we are working to improve efforts to collect and report data from area high schools and all higher education programs about the number of students in area programs, their completion rates, and their post-graduation status. We are in the process of collecting these data from our education partners. Further, while we collect data about PPCC student success, we do not conduct in depth follow on surveys once students graduate, which is when they obtain the industry certifications so crucial to their success. This information would help us to improve our programs and help employers to understand the issues facing recent graduates in the workplace.

The federal agencies that collect most data about labor supply include the US Department of Labor and the US Department of Education. The US Department of Education collects data about the number of secondary and postsecondary students graduating from Career and Technical Education (CTE) programs around the nation by CTE program name, especially those receiving federal funds from the Carl Perkins Act. These data could give a more thorough idea about labor supply, but CTE programs—like the occupations they serve—are tied to the IT, Engineering, Management and Protective Services occupation structures that do not yet single out cybersecurity. Further, while every state is required to report their CTE data publicly, we have been unable to find a place where this information is aggregated and available in a national report.

In addition, the US Department of Labor Unemployment Insurance (UI) data may be used to help higher education institutions understand how long it takes graduates to become employed, how long they remain employed, and by which firms. While these data would be very useful in determining the perceived quality of cybersecurity program graduates, Colorado does not yet participate in national data sharing services like Wage Record Interchange System (WRIS), which would allow us to use these data to track graduates' progress as they move around the country pursuing their cybersecurity careers.

Finally, with respect to the quality of cybersecurity education and training programs. Local companies indicate that they need to hire employees—even at entry-level—that can perform on the job, not just pass an industry certification exam. In fact, several local employers have had to

create in-house training programs because the quality of their new hires is so low. As a result, program quality is an enormous issue for local employers. As we tried to assess our own program's quality, we found that it is difficult to determine a quality cybersecurity education program from a less-than-quality program or to make comparisons between programs. Until the industry sets these standards across the board, there is no real quality cybersecurity program template.

The benchmark that comes the closest to outlining quality cybersecurity education is the National Centers of Academic Excellence (CAE), jointly sponsored by the National Security Agency and the Department of Homeland Defense. This program offers designations for regionally accredited two year, four year and graduate level institutions that meet stringent CAE criteria and map their curricula to the core knowledge required of cybersecurity professionals. However, each program approved as a CAE is unique and although they all meet the required standards, these programs are very different in execution, implementation, and practice. Further, the CAE does not assess the quality of graduates nor is data collected that demonstrates to employers that students have received a quality education.

In the absence of a set of quality standards or metrics, we have decided to focus on work-based learning—including internships, apprenticeships, and other experiential learning—as a way to improve the relevance of our programs to our students and prospective employers. Absent a quality metric, giving students more opportunities for work-based learning seems to be the best way to exceed employer expectations in this rapidly changing work environment.

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

While the Cybersecurity Framework provides the most stable outline of workforce categories and work roles, and the CAE offers the most comprehensive outline of knowledge/skills/abilities for cybersecurity workers, we have found that very few non-federal contractors or employers use these tools yet. However, we do think that the Framework is the most comprehensive way to describe cybersecurity work, and have been promoting its use with local employers and within our own institution.

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

At PPCC, we are just beginning more comprehensive cybersecurity training across our workforce this fall, though we have been providing IT training to all new employees—and refreshing that training for all employees regularly for more than a decade. We have little data on enforcement beyond the fact that we have not had a large data breech nor have our networks been compromised with much frequency. One of the reasons PPCC is now requiring college-wide cybersecurity awareness training is because our college is pursuing its CAE cybersecurity designation. This is a good example of using the CAE designation process to require adoption of cybersecurity best practices among education and training providers.

d. 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 vs financial sectors)?

In our region, cybersecurity industry employers have similar standards they use to hire their workforce, and most positions seem to fall within the Cybersecurity Framework, even if they are not easy to find among the data. With the exception of those companies mismatching industry credentials to job category (i.e. the companies requiring the CISSP credential for entry-level workers), most employers have realistic technical expectations of their candidates for mid- and upper-level positions.

However, these cybersecurity industry employers must recruit their workforce outside our region, poach employees from other local firms, or train less-qualified candidates to their specifications in house. For example, local data from CyberSeek reveals that even though our region has a large cybersecurity workforce, we face a shortage of workers in all but Security+ certification holders.

Further, employers tell us that holding an academic degree and demonstrated technical experience are not the sole indicators of success in a cybersecurity career. Employers find it particularly hard to find candidates that have these qualifications *plus* adequate critical thinking, problem solving, communication, and teamwork skills. Companies spend extra time and expense to train to and reinforce these skills.

Local headquarters employers are most interested in building a local pipeline of cybersecurity workers and have been eager to participate in our efforts to develop a pipeline that extends back to middle school career exploration. These employers are requesting that we help them to grow a well-rounded workforce, one with the requisite personal attributes and characteristics, technical skills and academic and industry credentials.

In addition, for positions requiring security clearances, employers are looking for ways that they can sponsor high school students into positions requiring a clearance. Finally, employers are looking to increase diversity of thought, background, socioeconomic status, gender and experience in their workforce. This has been a tremendous challenge for our college as we try to build the student pipeline needed to meet current and forecasted demand.

Outside of the cybersecurity services industry, the issue of cybersecurity worker knowledge, skills and abilities becomes far murkier. In fact, the question we are now posing in our college is, how much should EVERY WORKER know about cybersecurity? And, how do we infuse this knowledge into our curriculum?

There does not appear to be a standardization of work force categories in cybersecurity that crosses industries, though, again, the Cybersecurity Framework comes the closest to describing the most thorough process to use to determine needs within a company. Thus, at PPCC, we have been interviewing faculty about what the cybersecurity issues and best practices are for their industry or occupation, and are documenting what they are already teaching and providing funds for faculty to develop new cybersecurity-focused curricula.

In addition, we have selected a few employers in areas with high cybersecurity risk—like finance, public sector agencies, and health care—and are interviewing them about their needs for a cybersecurity IT workforce. So far, we have not found material differences in the

requirements of these organizations and those that provide cybersecurity services as the knowledge, skills and abilities are quite similar.

However, since we have begun to study this issue, we have recognized that we should be requiring every PPCC graduate, regardless of discipline, to have a basic level of awareness, ethics, and ability to respond to or escalate cybersecurity situations. In fact, cybersecurity education must not only be deep (focused and technical) but now it must also be broad (across disciplines) because every discipline is now technology-dependent.

e. 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?

An effective cybersecurity education, training and workforce development program will be embedded in a workforce development ecosystem that includes employers, educators, students and parents. The program will start with cybersecurity career pathway exploration in middle school through coursework and experiential activities (e.g. summer cyber camps and competitions). In high school, students should be able to continue exploring careers and take classes that, hopefully, will offer college credit or will prepare them for college coursework. College programs should follow the CAE standards and be infused with work based learning opportunities like internships. Ideally, colleges also should offer either advanced degree and certificate opportunities or continuing education opportunities to help workers fine tune or add to their skills throughout their careers.

There are several local universities that have been working in cybersecurity far longer than PPCC and have established and well-respected programs. Regis University is the primary example in our area of a university that embraced cybersecurity education early on, has active articulation agreements with Colorado community colleges, and has large classes, great industry connections, and employed graduates. The Regis faculty and staff have been terrific colleagues, mentoring us as we work to grow our own programs and seek employer and industry partners.

In addition, one school district in our region, Colorado Springs School District 11, has taken a leadership role in developing and offering a comprehensive cybersecurity CTE program. This program has been largely dependent upon the background and efforts of a single instructor, who is a former IT executive at a Fortune 100 company.

Beyond this instructor, we are challenged to find the instructional staff subject matter experts required to deliver secondary and post-secondary cybersecurity classes and provide students with real-world scenarios. Traditional teacher compensation, the work environment, career progression and maintaining technical currency are all contributing factors. In fact, this lack of teaching talent prevents us from believing that any training and education program in our region could be considered scalable.

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

The greatest challenge in our region is to find industry experts interested in and proficient at teaching and sharing their experience and expertise while maintaining their currency on technology and the cybersecurity threat situation. These experts are highly paid, very busy, and difficult to lure into the far less lucrative world of teaching. Further, cybersecurity jobs do not follow a regular schedule, making part-time teaching of a regularly scheduled cybersecurity class challenging.

The second biggest challenge in our region is to recruit students into cybersecurity education programs. While cybersecurity is constantly in the news, it is not perceived as sexy, and many shy away from it because they perceive the work as too technical, too stressful, or too boring. Finding the ways to explain the field to potential students is something we are trying to solve as we begin recruiting students for our new degree in cybersecurity.

The third biggest challenge may be the ongoing professional development needs of the cybersecurity workforce of the future. Staying knowledgeable about cybersecurity threats, understanding new tools and techniques, and offering these opportunities in a way that is affordable and accessible to all who need it may be a challenge that rises in importance as cybersecurity threats increase.

g. 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)?

The Internet of Things (IoT) brings cybersecurity from its technical stovepipe to the world of every individual and student. This expansion requires that cybersecurity be integrated into all aspects of education to make students aware and sensitive to the vulnerabilities and increase their critical thinking skills and vigilance. Cybersecurity needs to become a mainstream subject like math, science, language arts, and grammar.

With Artificial Intelligence (AI) advances, many believe that we will not need the labor-intensive processes of network monitoring, threat detection, and pursuit that many companies use today. This means that the PPCC program of study may change to focus more on how to deploy AI tools effectively, rather than conduct manual monitoring and detection activities. Further, AI advances may mean that the projected 1.8 million cybersecurity workers needed in the U.S. by 2022 (according to the 2017 Global Information Security Workforce Study) will shrink considerably, as technology will replace some of this workforce.

On the other hand, with every AI advance, new threats will emerge and new workers will be required to thwart attacks that are more sophisticated. In fact, cybersecurity work may become higher order work, monitoring AI technology and developing better tools. Thus, we might need fewer workers, but they will need to train more rigorously.

The challenge for education and training organizations is to scale cybersecurity programs appropriately and keep them flexible enough to adapt to changing technology. At PPCC, we intend to keep our cybersecurity offerings embedded in broader IT theory and concepts in order to allow our cybersecurity students to operate along a continuum of IT occupations requiring broad cybersecurity knowledge, skills, and abilities.

h. 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:

Most importantly, we need to treat cybersecurity threats like a public health crisis—one that requires a focus on prevention AND cure simultaneously. As a result, training every student to be cybersecurity focused and vigilant is the preeminent defense against most cybersecurity threats. This may mean that cybersecurity and digital citizenship become one of the general education subjects taught in developmentally appropriate ways for all students, from kindergarten through graduate school.

At the Federal level?

1) Continue the NICE effort to raise the level of awareness, coordination, and cooperation between education and training providers and employers.
2) Focus on improving cybersecurity supply and demand, including federally sponsored tools like CyberSeek, Bureau of Labor Statistics information, US Department of Education data, and the like by capturing the emergence of new cybersecurity occupations, firms, and related educational programs and career pathways.
3) Continue the CAE program at NSA to increase cybersecurity program fidelity and find new ways to incentivize academic institutions to achieve CAE status.
4) Develop a way to assess education and training program quality and provide a regular feedback loop for employers about the quality of their recent hires.

At the state or local level, including school systems?

1) Require states to participate in the Wage Record Interchange System (WRIS2), a US Department of Labor effort allowing the sharing of wage and employment data among states for non-Workforce Innovation and Opportunity Act (WIOA) purposes. This would allow school districts, colleges, and universities in states like Colorado to better track graduates to determine if their work patterns are aligning with local labor market needs.
2) Continue to offer incentives for school districts to offer CTE special programs like high school cybersecurity competition programs, and expand to active middle school competitions and summer camp programs.
3) Develop ways to provide incentives for IT employees to become prepared for and teach at the secondary and post-secondary levels to help fill the demand for experienced instructors.
4) Develop and promote cybersecurity career pathways statewide to help build awareness about the need for cybersecurity workers.

By the private sector, including employers?

1) Continue to collaborate with CompTIA to improve Cyber Seek as a labor demand resource, and improve its ability to capture and report supply-side data nationwide.
2) Focus on defining specific career progressions that are standard across industries, narrowing and specifying the differences between entry-, mid-, and upper-level occupations. This will help to speed the maturation of the profession in a way that

makes it easier for workers to search for available positions, and for educators to describe career progressions more accurately.

3) Engage with local education and training providers as often as you are able, as we need your input about our curriculum, your feedback about the quality of our graduates, and your expertise to supplement what we teach.
4) Consider offering internship, apprenticeship, job shadowing, and other experiences to a wide variety of students interested in cybersecurity. We need your help to provide our students with the experiences they need to become your best workers.

By education and training providers?

1) Gather, analyze, and use labor market demand and supply data for your region as a way to assess the current state of cybersecurity employment and determine any possible gaps.
2) Continue to standardize curriculum at all education levels as the cybersecurity industry and workforce matures.
3) Engage employers in all aspects of program planning, curriculum development, and program assessment to keep programs relevant and responsive.
4) Find ways to engage faculty across disciplines to consider adding cybersecurity awareness, digital citizenship and ethics concepts, and skill building in every academic discipline.
5) Implement cybersecurity training and awareness campaigns in your own organizations to model best practices for preventing attacks.

By technology providers?

1) Invest in cybersecurity education and training partnerships with government agencies (such as NICE) and education and training providers working to improve cybersecurity education quality and increase the size of the cybersecurity workforce.
2) Continue to offer educational discounts and free or greatly reduced education and training resources (including software and hardware) so that students have access to your technology for training purposes.