**Response to 82-FR-32172, University of Houston**

## General Information

### 1. Are you involved in cybersecurity workforce education or training (*e.g.*, curriculum-based programs)? If so, in what capacity?

The University of Houston (UH) is extensively involved in workforce education and training for cybersecurity and related fields. UH is surrounded by some of the nation's largest industries (i.e., energy, medical, international port, manufacturing, transportation, hospitality, emergency response, and aerospace), all of which have significant cybersecurity and cyber-resiliency challenges. This is further compounded by the rapid growth of the data science and analytics industries in Houston, which have a dual role as both clients and contributors to cybersecurity.

Capitalizing on a combination of synergistic research capabilities and the majority of UH alums joining the Houston workforce, UH has become a leading partner with many companies in these sectors. Furthermore, UH has taken on a national leadership role in several of these industries, as evidenced by UH Energy and the UH/DHS Center of Excellence in Borders, Trade, and Immigration. Because of its research portfolio and location, UH is optimally positioned to respond to cybersecurity challenges, especially in terms of workforce development. Key topic areas of interest include cybersecurity in energy and infrastructure, cybersecurity in optical networks and distributed computing, and cybersecurity in mobile computing and internet-of-things-related hardware; transportation cybersecurity; biomedical and international cybersecurity; and cybersecurity policy and law.

UH researchers in these fields collectively mentor hundreds of students, and UH has hosted a National Science Foundation (NSF) Research Experiences for Undergraduates (REU) site focused on cybersecurity for over 10 years. UH is also home to the Center for Information Security Research and Education (CISRE). Based on these and other resources, UH has been nationally recognized for workforce development and training excellence as an NSA/DHS National Center of Academic Excellence (CAE) in Cyber Defense for Education and Research. We have been identified as a regional CAE lead, with the responsibility to aid less mature CAE programs and assist 2- and 4-year institutions in developing their cybersecurity programs and attaining the CAE credential. Holding this role allows us not only to produce curricula components, but also take an active role in working with institutions within our region to develop their programs through employment of our curriculum.

## 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?

There are currently a wide variety of studies, recommendations, and curricula available for cybersecurity education and workforce development. However, a current challenge remains in

developing universally accepted taxonomy for cybersecurity workforce development. The lack of a unifying taxonomy in terms of cybersecurity education complicates the implementation of a universal set of metrics.

However, there are some frameworks that could serve as foundational guidance documents for more rigorous metrics in the future. Two of the most comprehensive recommendation frameworks for foundational knowledge in cybersecurity are the NSA/DHS CAE certification requirements and the National Initiative for Cybersecurity Education's (NICE) Cybersecurity Workforce Framework (NCWF) produced by the National Institute for Standards and Technology (NIST).

The curricular bedrock of NSA/DHS-certified CAE programs is the set of Knowledge Units (KUs) employed to categorize topics in cybersecurity for educators at 2- and 4-year undergraduate and graduate institutions. However, for faculty outside core Ph.D.-generating security programs, to begin the process of assembling materials guided by the KU rubric may be daunting. Thus there is a need for intra-institutional mentorship and possibly more guidance to equip educators to widely implement this KU rubric. Furthermore, although the end users of the NSA's KU system have been cybersecurity educators, the consumers for those skills are agencies of the U.S. government; other government entities at the state, local, and tribal levels; organizations in the not-for-profit sector; and private enterprise, from small and medium firms to major corporations.

In terms of wide-scale academic rollout and subsequent data analysis, the NCWF could offer easier implementation. In its latest draft version, the NCWF maps NIST Cybersecurity Framework (CSF) functions to seven NCWF work categories: Securely Provision (SP); Operate and Maintain (OM); Oversee and Govern (OV); Protect and Defend (PR); Analyze (AN); Collect and Operate (CO); and Investigate (IN). These seven work categories are generally well understood by those in the field, and there is a strong case for developing educational benchmarks for these work categories, even if other categories or more detailed metrics are developed later.

Furthermore, there is no clear national path to postgraduation assessment of educational appropriateness for meeting employer needs. In such a rapidly developing field, workforce needs can change rapidly, and there is a need for greater partnership between academic institutions and employers to assess and implement new curricula as new technologies emerge.

Despite these challenges, there are some data available for human capital in cybersecurity. The Taulbee Survey conducted by Computing Research Association (CRA) annually provides information on PhDs graduated from US and Canada in a given year. They also provide information on the employment of these PhDs by their specialty (including Security/Information Assurance specialty). According to this survey, the yearly rate of PhDs awarded in Security/IA has increased since 2012. However, less than 15% of these graduates are teaching (tenure- and non-tenure track combined), with most graduates taking positions in industry. These Taulbee survey results are a useful tool for tracking the numbers of newly graduated PhD students in cybersecurity as well as their initial entry into the workforce.

Similarly, a team of researchers led by Northeastern University began collecting information on the magnitude of the potential shortage of qualified educators in cybersecurity among higher education institutions. They plan to survey Center of Academic Excellence (CAE) in Cyber

Defense institutions about their faculty hiring and retention. While this is useful, the conclusion can be predicted: there is a shortage. To better understand these workforce data, more detailed surveys assessing reasons for career choices and following cybersecurity graduates over the course of their careers are likely needed.
Finally, the NSF maintains information on various CyberCorps programs. These data may be useful to better understand current workforce training efforts and identify best practices.

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

Simply put, no. As mentioned in the response to Question 1, the number of competing interests – certificating organizations, academic organizations, vendors, and governments - has not lent itself to finding consensus about workforce categories. There are numerous challenges associated with attempting to match real-world job roles to extant frameworks.

Not every professor is aware of the necessary security skills in industry. This has resulted in frequent complaints from industry about the students coming out of the universities being unprepared for their job roles. There is insufficient dialog between academia and industry about the skill sets needed. Many secondary organizations attempt to bridge this gap between employers and academia, but this results in a very localized patchwork of curricula to meet the particular needs of local or regional industries. This disjointedness is further exacerbated by differences of vision in terms of whether education should be focused on fundamental principles or very specific skills, be it in security or other areas.

Finally, there is a common misconception that all cybersecurity positions require STEM education. This is not accurate. While there is certainly a need for technical staff, cybersecurity positions as a whole are interdisciplinary in nature and include areas such as law, policy, critical thinking, communication/graphic arts, social sciences and others. The workforce able to address many of these interdisciplinary cybersecurity topics is exceptionally anemic, and there is a significant need to enhance workforce diversity, both academically and otherwise, in cybersecurity.

Although the NSA and DHS have attempted to address these sources of heterogeneity via their Centers of Academic Excellence, there remain many gaps in standardization that need to be addressed and promulgated to the wider cybersecurity education field.

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

While there are appropriate policies and practices in place within our organization, they are not consistently enforced throughout the organization due to fluctuations in resources and funding. Different areas within the organization assign different priorities to cybersecurity efforts which affect consistent enforcement.

**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 vs financial sectors)?**

The cybersecurity field is interdisciplinary and therefore requires a variety of knowledge/skills. The types of knowledge/skills required for positions seem to vary more by size of organization than sector. Larger organizations tend to have a larger need of a variety of skill sets and expertise than smaller organizations with fewer devices, users and technology needs. However, there are some sectors that have more areas of required special skills. Often, these industry-specific skills are poorly addressed in existing cybersecurity curricula, and there is a pressing need for more dialog between academic institutions and technical experts in industry.

Furthermore, the cybersecurity field faces a major challenge in that cybersecurity is now recognized as a universally important aspect of business operations, but many employers lack the knowledge and experience necessary to adequately communicate their cybersecurity needs. Thus, it often falls to cybersecurity staff to both assess the cybersecurity needs of their organization and then communicate those needs in a non-technical way to other business units. As a result of this employment environment, cybersecurity employees require extensive training in terms of collaboration, which encompasses both development and development operations as well as employee education and even remediation. Furthermore, many executives and managers from outside the cybersecurity field often have unrealistic expectations and expect cybersecurity staff to implement sweeping security policies and products without adequate monetary or staff support. Thus, cybersecurity professionals also need training or experience in project scoping and management and corporate communications.

**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?**

The Centers of Academic Excellence program run by NSA/DHS offers a comprehensive set of cybersecurity programs from multiple universities, overseen to ensure that the correct materials are being taught by qualified people. Although not an accreditation program, this group of universities works as a large, diverse collective, sharing the limited resources and reusing rather than recreating – which provides two significant outcomes: improved quality and lower costs.

The most effective development programs are the ones that address workforce as a pipeline and integrate stakeholders for mutual benefit. This begins with higher education and industry collaboration at the ISD level. An example of this in Houston is UH's work with HISD/Eastwood Academy, their work with the Greater Houston Partnership's Cybersecurity Task Force and integration of the Air Force Association's CyberPatriot competition program. Many of the students in Eastwood Academy's cybersecurity program have achieved professional cybersecurity certifications and have gone on to pursue university information assurance degrees

after graduation. These efforts illustrate a pipeline approach that illustrates the effectiveness of school/industry/academia in producing workforce-ready personnel with practical skills with very little economic investment. Additionally, programs such as the UH CISRE combine graduate student education with opportunities to work with industry partners through internships and engagement of industry professionals in an advisory board that shapes curriculum and ensures relevant and timely course offerings to meet industry needs. Finally, programs such as UH Downtown's Information Security Management program offer options that reflect different levels of engagement – students can start with a basic certificate offered online and transition to a full Master's degree with added instructor-led course offerings.

When these holistic pipeline efforts are aligned and guided by a particular framework, such as the NSA CAE requirements or NCWF, they become even stronger because they can reinforce fundamental concepts at various levels throughout the educational and work path while still building technical and specialized knowledge at every educational level. As might be expected from this trend, many federal training programs in both the military and security services excel at producing candidates via continuous training and development of role-specific skills. However, one of the core reasons this approach is so successful in these agencies is their top-down structure, in which senior leadership are able to implement a unified vision across the service in question. This sort of structure does not exist in the commercial or academic realms, and thus, other models are needed for defining and implementing workforce training.

The NSF Scholarship for Service (SFS) or "CyberCorps" program is arguably the most effective and scalable federal cybersecurity education, training and workforce development program being conducted in the US. It has two goals: the first is to expand capacity in cyber security ("capacity expansion") and the second is to produce well-trained US citizen/permanent resident graduates in cyber security, who get generous scholarships during their study and in return for this support commit to working in government agencies. The reasons for its effectiveness are: (i) the initial selection process, which is based on external peer-review of proposals submitted by qualified faculty from CAE institutions, and (ii) the comprehensive training programs provided by expert faculty for qualified students selected by those institutions.

However, the CyberCorps program faces a number of challenges related to student recruitment due to the particular features of the cybersecurity training pipeline. The Taulbee survey shows about 2/3 of PhDs produced by Computer Science graduate programs are foreign citizens. Thus, the potential pool of candidates for the graduate level of the CyberCorps program is immediately reduced to 1/3 of the student population. The NSF has recently relaxed the rule to provide financial support to permanent residents, but the requirement of working for a government agency after graduation and as a summer intern is a significant challenge for many foreign students because many relevant positions require federal security clearance. This is further exacerbated by a pervasive fear amongst permanent residents that they can't get the required clearance to advance their career.

**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 many challenges and opportunities in the cybersecurity field, and these are primarily influenced by three main factors: the heterogeneity of the cyber environment, the emergent nature of cybersecurity as a major societal and business concern, and workforce supply and demand.

The volume, variety, and velocity of technologies and the specific threats around each of those technologies is constantly evolving, as are the environments (both large-scale and local) in which those threats are encountered. The highly complicated, hyper-connected technology environment has resulted in an environment where no single person/organization/machine has full visibility into the entire environment. This is further exacerbated by the complexity of the modern electronics supply chain. Software integrity and providence needs to be ensured while concurrently ensuring that hardware is actually from the OEM and does not advertently or inadvertently contain malicious code, exploits, and/or backdoors. Finally, these diverse risks are not static, and thus cybersecurity efforts must be both intensely agile and continuous. This risk environment makes risk assessment and monitoring exceedingly challenging, and although there are several cyber risk frameworks available for assessments, cybersecurity professionals are rarely adequately trained in the successful implementation of these frameworks.

Because of this complexity, cybersecurity professionals require a diverse skill set that is rarely fully addressed by educational background and often requires on-the-job experience to fully mature. Although this is to be expected in most technical professions, the rapid growth of the cybersecurity field has resulted in a dearth of senior leadership and mentors capable of fully training junior employees, and this training and mentorship often must be repeated at each new employer due to the diversity of computer systems and policies among employers. This gap represents a significant opportunity in terms of developing systematic cyber risk assessment curricula and introducing them to existing training programs.

Furthermore, there is a significant knowledge gap between many academic faculty and professionals. Few academic faculty have extensive experience in industry, and similarly, many industry professionals are unequipped to train and assess students in a rigorous way. It is also often very difficult for even highly experienced cybersecurity professionals to transition into academia because of publishing and other faculty requirements, which cybersecurity professionals often have difficulty fulfilling unless they have already spent significant time in an academic environment. Experiential training, in the form of internships, mentorships, and/or guest lecture series, must be a critical component of training programs in order to narrow the gap between practical and academic training.

Although many groups have attempted to address many of these challenges, the lack of coordination between these groups has resulted in a patchwork of standards and recommendations that are often duplicative or dilutive. This patchwork translates to significant instructional diversity at every level of workforce development, and there is currently no guarantee that curricula based on a single standard will be comparable to those based on other competing standards. Thus, there is significant opportunity for the development and implementation of a unified and focused public strategy.

Finally, cybersecurity workforce enhancement efforts are currently almost entirely focused on the technical fields of computer science and technology. This focus neglects the interdisciplinary nature of the cybersecurity field and has resulted in a dearth of experts in fields such as cybersecurity policy/law, communications, and human factors. However, this lack of experts represents a significant opportunity to expand the cybersecurity workforce pipeline by actively recruiting students and experts in these “non-traditional” cybersecurity fields.

**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)?**

The cybersecurity workforce of the future will need significant training in data science, artificial intelligence, and embedded systems. Towards this goal, the University of Houston has developed and implemented several courses related specifically to security analytics and cyberphysical systems security. Many of these courses use modular curricula and other innovative methods to address the dynamic and diverse nature of the cybersecurity field.

Beyond dedicated training for cybersecurity professionals, cybersecurity needs to be integrated into all aspects of professional development. All degree programs should have some component of cybersecurity education. Ensuring that the academic approach with regards to cyber is interdisciplinary in nature allows for the individual degree programs to adapt to the changing landscape. Expanding cybersecurity training beyond computer science and technology students and providing at least basal levels of cybersecurity understanding throughout the workforce will have dual benefit in that it will both decrease organizational risk profiles (allowing cybersecurity professionals to respond to more advanced threats) and increase cybersecurity awareness related fields, which may encourage experts in other areas to transition into cybersecurity based on this exposure. Strong industry partnerships through program advisory boards will help academia make the needed modifications to ensure adaptability and relevance.

**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:**

**i. At the Federal level?**

Introduced: A focused, visible, coordinated workforce initiative that professional/public/private organizations and academia can contribute to instead of duplicated efforts throughout the country.

Continued: Linked Learning Program. This program provided federal funding and program development assistance which allowed HISD to successfully promote cybersecurity education at the high school level.

Modified: At the federal level, both components (capacity expansion track and scholarship track) of NSF's Cybercorps program should be expanded and strengthened. We propose an academic track of the CyberCorps program to attract all talents in the top research universities to study security/IA in the U.S. Rather than the current government service requirements, this track would require scholars to teach cybersecurity courses at a US university after getting a PhD. This would serve to both enhance the reach of the CyberCorps program and potentially provide some relief for the severe lack of cybersecurity faculty.

Modified: The CAE program (NSA/DHS Center of Academic Excellence) should be expanded. It is ready to double in size and broaden its base, but this will require additional federal funding. Long-term, a simple pass-through of funding to CAE's to help cover their costs will improve the programs as well.

**ii. At the state or local level, including school systems?**

Modified: School systems need more incentives and opportunities to encourage development of cybersecurity programs at the secondary school levels. Mandatory computer science course requirements, early introduction to computational thinking, and clearinghouses for data collection and dissemination of best practices in course/curricula/lab development and workforce training are likely to have a profound impact on future cybersecurity workforces.

Introduced: There needs to be more training opportunities provided to secondary school teachers for them to be qualified to teach cybersecurity courses. Teachers need to be provided with additional incentives for supporting students in CyberPatriot and other extra-curricular cyber competitions/activities.

**iii. By the private sector, including employers?**

Modified: More efforts need to be made to encourage partnerships between industry/academia/schools that result in student internships and provide for class instructors. Employers should encourage their employees to participate in courses and training programs that build their cyber security awareness and skills. Mechanisms could include release time, merit raises, and penalties for adverse behaviors.

Modified: More employers need to be engaged with advisory boards throughout all levels of academia – secondary schools, community colleges and higher education.

**iv. By education and training providers?**

Modified/Introduced: Cybersecurity focused programs that recognize non-STEM skills and abilities required for cybersecurity positions. Transition paths provided for non-technical

professionals (ex. Liberal arts majors) to gain basic cyber-skills to be able to successfully fill cybersecurity positions.

Introduced: Curriculum transition programs. These programs would characterized by highly experienced and qualified cybersecurity educators holding workshops for current computer science faculty who are interested in teaching security courses (not necessarily doing research) but do not have the time or depth of knowledge required to prepare the material in a given topic. The master teacher should provide all material (slides, homework, data sets, etc.) to the participating faculty. These professors will them offer courses in their institutions in the following years. This is a quick way of increasing the security curriculum capacity. There have been some curriculum modules developed with federal funding, but the adoption rate is too low. We should make it easy for professors to teach new security courses using proven course material.

Modified: Universities need to examine their own faculty career paths and see where the friction point is between highly qualified candidates from industry and the typical publish or perish cycle. The new world is technologically driven, has full integration of real world applications with deployment of solutions, and the academic paradigm of publishing reports based on very incremental findings does not fit within this model. Rather than discover new knowledge, much of the future growth will be in integrating concepts from a multidisciplinary point of view. Multidisciplinary faculty often face significant barriers to navigating traditional academic career paths, and the university community needs to realize that these are valid paths and find ways to be inclusive of them.

**v. By technology providers?**

Introduced/Modified: Technology providers should be encouraged in outreach efforts at every level of the workforce training pipeline, and cybersecurity groups both in academia and industry must build stronger partnerships with technology providers to ensure adequate workforce training in emergent technology and to certify and assess the security features of those technologies.