Response to the NIST RFI
Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure:
Workforce Development

The University of Texas at San Antonio's (UTSA) Center for Infrastructure Assurance and Security (CIAS) offers the following in response to the NIST Request for Information on Workforce Development, July 2017. UTSA/CIAS is also the lead for the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) and the following comments include feedback from this organization.

General Information

UTSA is involved in both cybersecurity workforce education and training. UTSA offers concentrations, minors, and majors in cybersecurity and information assurance at the BS and MS levels and have cybersecurity research being conducted at MS and PhD levels in several colleges. In addition, the CIAS offers training programs in a variety of cybersecurity topics aimed at the state and local levels as well as in areas such as certification training and user awareness. UTSA is an NSA/DHS designated Center of Academic Excellence in Cyber Defense and is an NSF Scholarship for Service grant participant. The CIAS is also involved in programs aimed at the high school, middle school, and elementary school levels.

Response to Specific Questions

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?*

   Due to a lack of any other mechanism, the majority of organizations rely on certifications to determine suitability of applicants and to set minimum standards for potential employees. Less well understood are the capabilities of students out of educational programs at colleges and universities that have received an NSA/DHS designation as a Center of Academic Excellence in Cyber Defense. Adding to the confusion is the breadth of skills that exist in the field and the individual (unique) requirements that organizations may have. As a witness of this, the NIST NICE Cybersecurity Workforce Framework lists hundreds of tasks and knowledge description in seven categories. No single certification or educational program covers all of these. Even for a single category it would be very difficult to cover the required knowledge to address the tasks.

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

   The simple answer to this is 'no'. Again we can look at the NIST NICE Cybersecurity Workforce Framework to realize the challenge faced. This is one of the reasons that academia focuses on education versus specific system training but then it is also why industry is constantly complaining that academic programs don't sufficiently prepare students for the "real world" and are not preparing their students to be prepared "on day one" to be productive.

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

   n/a

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)?*

   Because of the need to address problems faced today, a large number of employers are focused on their specific environment and systems. In a mixed group of employers and educators, there will often be a consensus that academia is not adequately preparing students for industry but if the industry members present were polled on specifics, there often is not a single list of skills they can agree upon. This is natural because the needs of various organizations can differ tremendously (e.g. energy versus financial sectors). So academia is left to attempt to find a middle ground or a set of basic skills all can agree upon and then leave industry to accept the responsibility of training for specific (or unique) tasks. The same applies to certifications and is one reason there are a number of "general" security certifications as well as a large number of vendor and capability specific training courses.

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?*

   National Science Foundation (NSF) Scholarship for Service (SFS) program. NSA/DHS Center of Academic Excellence program. The plethora of cybersecurity competitions (National Collegiate Cyber Defense Competition – NCCDC, CyberPatriot, international Chapter the Flag – iCTF)

   The scholarship programs have been affective because they offer students a job upon completion of a course of study in cybersecurity. It has helped to introduce individuals who may not have previously considered a career in the security field to the many rewarding jobs that exist. The COAE program has had somewhat of a similar impact in that it has helped to spread the word about the cybersecurity career field. The SFS program, however, generally attracts individuals who are at least considering security as a career field, or who are the very least already majoring in a technology field of some sort (this is not universally true but certainly is for the vast majority of students). What SFS has done is to gain more employees for the government – individuals who might have gone into the private sector if it were not for the scholarship program. The COAE program has had a broader impact in terms of introducing individuals to cybersecurity careers but is at the collegiate level. One of the things that many schools have learned is that to attract students to their program, they need to introduce individuals to cybersecurity possibilities at an earlier age. This is where programs such as

CyberPatriot have proven extremely valuable. Other programs of note include the GenCyber camps sponsored by NSA and other summer programs offered by organizations such as the Air Force Association. At the collegiate level, sponsors of the NCCDC have stated that the event is the single best recruiting event annually for them as the participants of the competition have a better grasp of security in a real-world situation than do the majority of students who have not participated in a competition during their collegiate career. A number of recruiters now look for competitions such as NCCDC on resumes because it tells them something about what the student has been involved in outside of straight academic courses. The NCCDC also provides the benefit of a next level of competition for all of the CyberPatriot students who have been enticed to participate in the program and who do not want to stop competing when they go to college. NCCDC and CyberPatriot are similar in scope and concept and currently work together.

Finally, there are a number of programs aimed at individuals such as veterans leaving the military who are interested in finding employment and a career once they separate. These programs are effective in giving individuals a start in a new career path that is needed by the nation.

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 two aspects of cybersecurity training and education that need to be recognized and addressed individually:

1) Training and education of the cybersecurity workforce: This is what has been discussed so far. We need more cybersecurity practitioners in the workforce to fill the many cybersecurity jobs that are open. The challenges here are what has already been discussed or alluded to. Reaching individuals early enough in the education process so they consider cybersecurity as a valid career choice. Continued and potentially expanded government support of the programs mentioned will allow for an increase in the number of individuals entering the career field.
2) Cybersecurity training and education of the workforce: This is what will still remain even if all cybersecurity positions are filled. Many breaches have occurred not because the security professional had not done their job adequately but because a normal user in the organization did something they should not have done. All workers need a basic level of cybersecurity training. All workers need to better understand the threat to their organization. The challenge is getting to them. Security awareness training is certainly one way and for larger organizations this is an approach but for the thousands of small and medium size businesses that do not have the budget to afford a lot of training programs, or to afford security professionals, other efforts are required. One of the emerging programs is the creation of Information Sharing and Analysis Organizations (ISAOs) designed for small and medium sized businesses and geographic regions. Having small business owners attend a regular meeting or luncheon (monthly, quarterly, …) where cybersecurity is discussed would help introduce security to a segment of the

population that is drastically underserved currently. ISAOs do not need to be formal organizations such as ISACs. They can be informal and designed to address the needs of their members at a level that their members can handle. If the nation had all small and medium sized businesses participating in regular discussions on cybersecurity, how better off would it be? How much easier will it be for small and medium sized businesses to adopt programs such as the NIST Cybersecurity Framework if they already have a basic understanding of the importance of security?

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)?*

   Education and training programs have to constantly adapt to the changing environment. Twenty five years ago how prevalent was wifi in comparison today? What security issues were introduced as a result of wifi? Go back a decade and look at mobile devices and compare them with the power and us of mobile devices today. What about cloud computing, what changes or new issues did that introduce to cybersecurity? Security professionals need to constantly be updating their understanding of the environment. Education and training programs need to constantly be updated to ensure the most current technology, which often comes with immediate vulnerabilities, is understood by students.

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*
   a. *At the Federal level?*

      National Science Foundation's (NSF's) Scholarship for Service (SFS) program. Federal department/agency support of competitions at the collegiate and high school levels (e.g. the National Collegiate Cyber Defense Competition – NCCDC, and the CyberPatriot program).

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

      There are a couple states that are introducing or discussing a state specific scholarship program similar to the SFS program. Cities should consider doing the same. Industry also should consider this option.

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

      Internships and scholarship programs.

   d. *By education and training providers?*

Participate in SFS and other scholarship programs. Participation in NSA/DHS Centers of Academic Excellence program.

e. *By technology providers?*

Interns. Support of competitions and schools with equipment so students are introduced to systems/products that they will see upon completion of degree programs or certifications.