December 10, 2019

AFCEA Cyber Skills Pipeline Program Overview

Problem Statement: The US has a well-documented shortage of cyber professionals. There are many organizations (universities, training institutions, organic training efforts) who are initiating or expanding education and training initiatives to address this shortage. While these initiatives are largely well intentioned, a cursory review of the initiatives shows that not all are equally effective. There are two needs that arise out of this situation. First, is the need for a way of identifying those cyber education and training initiatives that are truly effective. Second, is the need to publicize the techniques and processes that are proving to be most effective so that other initiatives can adopt these techniques and processes.

Proposed Program: The program would start with the development of a set of criteria that can be used to evaluate the effectiveness of cyber education and training initiatives. The criteria would focus on the specific measures that would identify a truly effective cyber training/education initiative. Once developed, the criteria would be used to assess the effectiveness of cyber education and training initiatives for those who would choose to participate in the assessment process. The results of the assessments (i.e., identifying the most effective programs) would be publicized along with a summary of the techniques and processes used.

Proposed Approach: It is proposed that AFCEA establish a program that would develop an objective criterion (largely focusing on results) for assessing the effectiveness of cyber education and training programs and that AFCEA conduct an annual assessment of cyber education and training initiatives. AFCEA would leverage their standing committees—cyber, homeland security, technology, intelligence—to identify a board of nationally-recognized individuals who would develop the effectiveness metrics. In addition, the board would draft the call for submissions that would be issued for cyber education and training initiatives to submit the data required for the assessment. It is proposed that AFCEA leverage member companies and universities to assist in the assessment process.

Background Information: Cyber Skills Pipeline Program Concept

AFCEA members are among the largest employers of cybersecurity talent; we feel the pain caused by shortages of high-end cyber skills every day. More importantly, without a reliable pipeline bringing much larger numbers of very talented and well-trained professionals into the cybersecurity workforce, it will be difficult for any nation to withstand a sustained wave of cyber-attacks.

Program Objective:

Create a program that moves quickly from "admiring the problem" of cyber skills shortage to taking action to solve the problem in the near term by enabling a series of competitive pilot implementations in each element of the pipeline, to find the most promising immediate solutions that can scale, provably and cost-effectively, to meet the national need. Those "most promising" solutions would then be shaped into as National Plan for Closing the Cyber Skills Gap with realistic but aggressive schedules.

No one would be excluded. Any group with a solution will be encouraged to demonstrate that it works. All that are demonstrated will be evaluated using a consistent set of metrics. An aggressive schedule will focus attention and accelerate progress. The results of all competitive pilot implementations complete in time will be shared with the community at the CERTS conference in January 2020.

Why AFCEA?

AFCEA is an honest broker that can bring all key players to the table, and AFCEA is serious about its mission to be a "forum for the ethical exchange of information." That's what it will take to bring the entire ecosystem (students, teachers, schools, commercial employers, government employers, and technology providers) together to discover what works and should be implemented immediately to close the cyber manpower gap. Further, AFCEA can credibly ask each group with a proposed solution to fund their pilot programs themselves, and AFCEA be trusted to be fair in the evaluation of the proposed solutions.

Proposed Vision:

The AFCEA Cyber Skills Pipeline Program will encourage all groups that believe they have a solution for each of the constituent components of the pipeline problem, including perhaps to conduct a live demonstration of their solution with sufficient numbers of representative candidates to demonstrate efficacy in the real world. The following is a strawman list of the components that might compose a national cyber skills pipeline:

1. Identify high school students with high aptitude for cybersecurity careers.
2. Enhance the cyber skills and excitement for careers in cybersecurity for high school students (through camps or other programs)
3. Enhance diversity in the cybersecurity pipeline through programs that recruit substantial numbers, and develop the skills, of high school students from populations that are underrepresented in the cybersecurity workforce
4. Identify college students with high aptitude for cybersecurity careers.
5. Enable college students to develop hands-on mastery of key aspects of cybersecurity sought by employers through courses, simulators, and other learning modalities
6. Provide college students with apprenticeships through which they develop advanced mastery of key cyber skills under the tutelage of skilled professionals
7. Enable undergraduate college students to master hands-on cybersecurity skills in high demand from employers, such as intrusion detection, advanced forensics and reverse engineering, web application security, and industrial control systems security.
8. Identify veterans with high aptitude for success in cybersecurity careers, develop their cyber skills, and place them in cybersecurity jobs.
9. Identify current employees in non-IT roles that have high aptitude for success in cybersecurity careers, develop their cyber skills, and move them into roles in cybersecurity.
10. Provide just-in-time, continuous education for specialists in each area of cybersecurity that can enable them to maintain currency in those areas.