General Information

1. Are you involved in cybersecurity workforce education or training

Yes, I have 17 years of curriculum development and training experience in the field for information assurance, cyber security, teaching CISSP and other related DOD 8570 certifications.

For the past three years, I have taught as a private contractor for two different community college programs at the CYBR 101 level.

I have 20 courses in the NICCS Education and Training Catalog.

I have executed contracts with CISCO, SANS, and ISC2 for curriculum development, train-the-trainer, and professional training.

Over a 12-year period of time, I have collected statistics from both commercial and military students revealing what works in developing new skills and/or updating existing skills in cyber security education.

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?

Current metrics for cyber security education are the total number of certified people.

Improvements:

1. Create a cyber professionalization exam process such as: CPA or JD (BAR Exam) with an apprenticeship program.

   1. This must be bound to legislation such as the GDPR, where only certified professionals may sign-off on the controls that are protecting the organization.

2. Formalized following of the NICCS categories and specialty areas to organize the professionals into collections of skill sets.

   1. A generalist would be proficient in four of seven categories, a Specialist would be proficient in 1 or 2 categories but have all of the specialty areas covered in that category.

3. None of this should be managed by for-profit organizations (such as SANS/ ISC2— conflict of interest)

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

No; I reviewed and worked on the draft csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf

Many of the positions were specifically for military and government.

Please see those draft comments as a separate attachment.

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

Yes. Continuing professional education (CPE) should also be a separately tracked independent body, not connected to any certification organization (conflict of interest).

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce?

Organizations only value compliance; this is insufficient because compliance is not security. The cyber security workforce is directed by the organization’s individual profit motives.

What is needed by the organization: GDPR-type requirements and professionalization.

Are employer expectations realistic? No; they do not treat cyber security as a process; they treated as a checkbox.
Separately but just as important: the skills that are required in most corporations are neither in line with position descriptions nor applied in any consistent manner.

Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline?
The inconsistencies in these expectations and the lack of standard knowledge by hiring professionals to meet the needs of the organization make it close to impossible for cyber security individuals to do their job. The people who are hiring are asking the wrong questions. The job definitions do not match the job expectations. Solution: NICCS categories and specialty areas go a long way in creating matching statements and expectations.

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today?
I taught for 10 different organizations using their programs; active learning techniques and student engagement are the most effective. Practical application of skills on both the micro and macro level, such as problem-based learning are the most effective. These skills must be based upon: Core vocabulary, fundamental principles, and basic analysis techniques.
What makes those programs effective?
High student interaction with the instructor and other students in a mentoring process.
The care and concern that instructors have for the students' well-being and career.
What are the goals for these programs and how are they successful in reaching their goals?
The goal for my program is 90% proficiency and 99% pass rate.
Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?
Yes; as long as it is not turned into computer-based training/ watching a recording.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?
A conversion to professionalization and removing certification bodies' profit motive.

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?
They require courseware, curriculum development and instructors not be tied to a pre-approved curriculum process that sometimes takes 2 to 3 years to yield a result for the classroom. This is why the apprenticeship program is critical to long-term success.
How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?
They need to adapt on a monthly and quarterly basis.

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?

Remove FEDVTE low bidder limitations for curriculum development.

Eliminate recording watching/ Bad CBT

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

iii. By the private sector, including employers?

Convert to professionalization, require employers to match job descriptions, to NICCS cats/spec

iv. By education and training providers?

Require the same certification, and professionalization, convert CPE’s to an open system regulated by a professional organization

v. By technology providers?

Use a consistent vocabulary.

Dean Bushmiller