CSIA RFI Responses, January 15, 2019

Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

From: Dean Bushmiller
Subject: RFI Response: Federal Cybersecurity R&D Strategic Plan

Your Question #5 What changes to cybersecurity education and workforce development, at all levels of education, should be considered to prepare students, faculty, and the workforce in the next decade for emerging cybersecurity challenges, such as the implications of artificial intelligence, quantum computing, and the Internet of Things on cybersecurity?
--
Answer:
As a technical educator with 15 years of training in cyber security, including teaching CISSP for 12 years for over 1000 students: I find basic skills applied at an expert level to be lacking at all levels. The technology will always change - the basics will not. People do not know the basics.

Solution:

1. Professionalization of cybersecurity through- Government approved, state by state mandated exam like the accounting CPA or legal BAR- with a license to practice cybersecurity. Including an ethics organization with the power to sanction inappropriate behavior.

2. Professionalization of cybersecurity through- Government approved, apprenticeship program, where key NICE/NICCS roles are identified, SME define number of hours to successfully achieve expertise from apprentice, master, senior master.

...with Freedom and Responsibility and Security for All,
Dean Bushmiller, President Expanding Security CISSP+25