The Federal Register

The Daily Journal of the United States Government

Notice

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

A Notice by the National Institute of Standards and Technology on 07/12/2017

This document has a comment period that ends in 19 days. (08/02/2017) Submit a formal comment

Document Details

Printed version:
PDF
Publication Date:
07/12/2017
Agencies:
National Institute of Standards and Technology
Dates:
Comments must be received by 5 p.m. Eastern time on August 2, 2017.
Comments Close:
08/02/2017
Document Type:
Notice
Document Citation:
82 FR 32172
Page:
32172-32174 (3 pages)
Agency/Docket Number:
Docket Number 170627596-7596-01
Document Number:

2017-14553

ACTION:

Notice; Request for Information (RFI).

SUMMARY:

Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (the "Executive Order"), directs the Secretary of Commerce, in conjunction with the Secretary of Homeland Security, and in consultation with other Federal Departments and Agencies, to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and provide a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors. The National Institute of Standards and Technology (NIST) is seeking information on the scope and sufficiency of efforts to educate and train the Nation's cybersecurity workforce and recommendations for ways to support and improve that workforce in both the public and private sectors.

Responses to this RFI—which will be posted at *https://nist.gov/nice/cybersecurityworkforce*—will inform the assessment and report of the Secretaries of Commerce and Homeland Security to the President.

DATES:

Comments must be received by 5 p.m. Eastern time on August 2, 2017.

ADDRESSES:

Online submissions in electronic form may be sent to *cybersecurityworkforce@nist.gov*. Please include the subject heading of "Cybersecurity Workforce RFI". Attachments to electronic comments will be accepted in Microsoft Word or Excel, or Adobe PDF formats only. Written comments may be submitted by mail to Cybersecurity Workforce RFI, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials.

All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included.

Submissions will not be edited to remove any identifying or contact information. Do not submit confidential business information, or otherwise sensitive or protected information. Please do not submit additional materials. All comments received in response to this RFI will be made available at *https://nist.gov/nice/cybersecurityworkforce* without change or redaction, so commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

FOR FURTHER INFORMATION CONTACT:

For questions about this RFI, contact: Danielle Santos at 301-975-5048 or *Danielle.Santos@nist.gov*. Please direct media inquiries to the NIST Public Affairs Office at 301-975-2762 or *Jennifer.huergo@nist.gov*.

SUPPLEMENTARY INFORMATION:

Executive Order 13800 of May 11, 2017, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," directs the Secretary of Commerce and the Secretary of Homeland Security to consult with the Secretaries of Defense, Labor, and Education, the Director of the Office of Management and Budget, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, in conducting an assessment and making recommendations regarding the nation's cybersecurity workforce.[1] Specifically, these departments are to:

(A) "jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and"

(B) "within 120 days of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors." [2]

The Commerce Department's National Institute of Standards and Technology is soliciting comments from the public that will aid the Department of Commerce (DOC) and the Department of Homeland Security (DHS) in preparing the assessment and report to the President. For the purposes of this RFI, "education and training" of the American cybersecurity workforce does not include general workforce cybersecurity awareness efforts. Rather, "education and training" refers to curriculum- or practicum-based programs to increase the effectiveness of the workforce addressing cybersecurity challenges. As the Executive Order states, comments are sought on the cybersecurity workforce in both the private and public sectors.

NIST may conduct workshops to gain further public input to the assessment and recommendations regarding the cybersecurity workforce. Information will be made available at *https://nist.gov/nice/cybersecurityworkforce*.

This RFI does not address additional aspects of the cybersecurity workforce that are included in the Executive Order.

Request for Information

Given the nature and importance of the Executive Order, NIST requests information from the public about current, planned, or recommended education and training programs aimed at strengthening the U.S. cybersecurity workforce.

Respondents are encouraged—but are not required—to respond to each question and to present their answers after each question. The following questions cover the major areas about which NIST seeks comment. They are not intended to limit the topics that may be addressed. Respondents may address related topics and may organize their submissions in response to this RFI in any manner. Responses may include estimates; please indicate where the response is an estimate.

All responses that comply with the requirements listed in the **DATES** and **ADDRESSES** sections of this RFI will be considered.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publicly at *https://nist.gov/nice/cybersecurityworkforce*. Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

General Information

1. Are you involved in cybersecurity workforce education or training (*e.g.*, curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? *Note:* Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (*e.g.*, personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

Security University is 26,000 student strong with a 100% student success pass rate. SU is a MSA-CESS accredited non degree, SCHEV Certified to Operate school located in Herndon VA,

Corporate location Delaware. SU students attend short 5 day accelerated hands-on cybersecurity courses that are (were) NSA CNSS 4011, 4012, 4013, 4015, 4016A approved since 2008. Since 1999 SU's mission is *solely* focused on performance based cybersecurity skills that qualify and validate the cybersecurity workforce resulting in Certificates of Mastery that lead to high wage in demand cybersecurity careers. All cybersecurity courses and certifications lead to employment.

SU was awarded a 2.75M 2013-2017 DOL TAACCCT grant - Security University's (SU) **CSEAL Team X** Project (**CyberSecurity Stacked Education Achievement Lattice): Addressing the Cybersecurity Professional Shortage** that **served 847 TAACCCT** participants (CyberSecurity TAA-Affected Workers and Military Veterans veteran, unemployed, underemployed and women) from Oct 2013 – Sept 2015 thru today with free cybersecurity courses, education and hands-on skills. SU exceeded the 375 TAACCC participant goals by 472 participants, delivered 6,000 hours, 150 accelerated 5 day hands-on instructor led CS certification training classes, earning 4874 industry recognized cybersecurity certifications (2013-2015) that match the needs of employers for high wage in demand jobs that resulted in 97% (new & improved) employment outcomes. SU is GIB CH 31 approved. SU is not Title IV approved.

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 certified or DoD 8570 metrics are incorrect, ineffective and biased. They certify a person has passed an exam. Students who pass performance based courses, hands-on labs, exam and practicums are not counted in the metrics, and technically not eligible to be counted in the metrics. The DoD 8570 office often said the 8570 M was never meant to *train* the cybersecurity workforce.

After 15 years of hundreds of thousands of exams that certified an unqualified workforce we must qualified and validate our workforce by using effective accelerated courses that validate cyber skills not scores. There are a number of successful models that have qualified and validated the workforce.

Like pilots and Doctors who are trained and validated, so must the cybersecurity workforce. Or we will continue down a certified unqualified path. Statics position the "Global spend on cybersecurity is expected to reach $1 trillion over the next four years, yet by just 2019, experts foresee a cybersecurity skills shortage to the tune of 1.5 million unfilled jobs. (**2017 Hiring Trends in Cybersecurity)**

Security University mission is to train IT professionals to be IT Security professionals. 26,000 students strong have graduated courses, earned certificates and certification that lead to high wage in demand cybersecurity employment. Training and practicums are essential to build a qualified workforce.

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

If there was *sufficient* understanding and agreement about workforce categories – there would be a plan to build a highly qualified, skilled and validated cybersecurity workforce. Instead years of *obfuscation* has blurred the path. 95% of cyber security professionals do *not* require a cybersecurity degree for a high wage in demand cyber job. They need qualified and validated skills learned from seasoned, skilled cybersecurity professionals with a practicum that demonstrates the student has learned a process and methodology that uses cybersecurity tools and understands enough of the risk policy to determine how to defend based on known threats in order to defend against unknown threats.

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 SU has appropriate cybersecurity policies in place regarding workforce education and training efforts and those policies regularly and consistently enforced.

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)?

Executives fear their organizations are ill equipped to prevent, detect, and respond to cyberattacks. Check.There are a lot of job openings in the cybersecurity profession. Check. Employers have a dream list of qualifications they want it's either not realistic, or definitely not realistic for the pay. Check. We can take the IT workforce and with little effort, good curriculums and great instructors teach thousands if not millions to be cyber security professionals in less time and money than invested by Obama's TAACCCT 2013-2019 grants.

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?

For 7 years DOL and Department of Ed invested 2B in Community Colleges called the Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program. A $2 billion federal workforce investment aimed at helping community colleges across the nation increase their capacity to provide education and training programs for in-demand jobs. The US Department of Labor (DOL) administers the seven-year grant program in partnership with the US Department of Education.

Yes there are effective scalable cybersecurity education, training, and workforce development programs being conducted in the United States today. Many qualified educated statics are not captured for instance:

As far back as 2009 SU has been the leader in Qualified CyberSecurity Education
Army Fort Gordon: Q/SA® Q/PTL® Class Training April 2010 - As an Army Information Systems Management (FA53) officer focusing on Cyber Defense, I've had the opportunity to train and certify in several IA/CND specific programs as well as work a myriad of Army Cyber Defense workforce training and development issues.

Having just recently completed the Security University (SU) Qualified Security Analyst (Q|SA) and Qualified Penetration Tester License (Q|PTL) courses I can confidently say that Sondra and her team have built an exceptional program of instruction; capturing the essential elements of security analysis and penetration testing methodologies and delivering them in a clear and concise format in a blended learning environment of lecture and hands-on practical skill development with scenario-based final examinations. SU training techniques are a perfect match for our military cyber defense workforce goals since they not only train the relevant concepts of cyber defense and its CND specialties but also in the case of Q|SA and Q|PTL courses challenge the students to apply those concepts in a "tactical" setting that an actual security analyst or penetration tester might see.

Security University's Q|SA / Q|PTL program of instruction is impressive and superior to some other training programs in several ways; one of them being the daily hands-on assessment of critical skills being taught. Another was the realistic practical final exam which included a penetration test with a final report that required some in-depth analysis of the resulting sets of data. I spent 30 post-course hours alone on analyzing the data and developing a 32 page report. That's definitely an experience you're not going to get through other training programs that teach a five day curriculum that's predominately lecture based. The Q|SA and Q|PTL courses also expose the students to a wide range of open and closed source automated tools for use in security analysis and penetration testing as well as the built-in assessment and exploitation capabilities of both Linux and Windows based operating systems. I honestly can't understand how we expect to conduct defense in depth across the GiG without our technical workforce understanding basic exploitation, which is exactly what's missing from many other approved certifications. SU equally balances this with methodology and analysis techniques rather than relying on specific toolsets since tools frequently change and are always subject to interpretation of their results.

Many leaders and managers in a resource constrained environment try to meet FISMA compliance by targeting those one-shot, many-kills certifications that are on the DoD 8570.01M chart with little regard for how relevant the training might be for certain 8570 categories. No better example can be given than the inclusion of CISSP as an IAT validating certification. Being a CISSP I can attest that it's a great certification for a security manager as it is wide and deep in several essential bodies of knowledge. But it will not enable a security technician, especially at the enclave level, to secure enterprise environments from a hands-on technical approach nor understand the threat and environment essential to effective defense in depth. Therefore it adds little value for an organization to have an IAT-III CISSP from a technical standpoint, but practically, that person can also fill other roles since CISSP covers everything from IAT-I through IAM-III. Hence, managers focus on CISSP and miss excellent training like Security University's programs.

Security University training should be a major part of any organization's information security training programs.

List of Hands-on Computer Security Classes/ Qualification & Certification Tracks:

All SU classes are instructor led 5 day class format - unless specified in class syllabus.
Security University Testing (SUT) owns the Q/ISP® Exam & Q/EH®, Q/SA®, Q/FE®, & Q/ND® micro credential exams. SUT Q/ISP®, Q/IAP®, Q/WP®, Q/SSE®, Q/CND® Certification exams are provided by TESTRAC high-stakes testing on site.

SU Discount Class Packages - SU v0upon Classes 23 class/ 24 months $11,000
Q/ISP® Qualified/ Information Security Professional Certification Platinum Pass $8,475 (Q/EH, Q/SA-Q/PTL, Q/FE, Q/ND)
Q/ISP® Qualified/ Information Security Professional Certification Platinum Pass+ $9,500 (Q/EH, Q/SA-Q/PTL, Q/FE, Q/ND + CISSP)

Security University Course Listing 2017

Course Number	Course Title *denotes optional Practical ~repeat course names	Course Hours	Cost
Required- R Q/ISP CoM	SU Q/ISP® Qualified/ Information Security Professional Certificate of Mastery CoM / non degree (5 classes + Security+® + CASP® or CISSP® & 3 Practical's required to earn CoM)	Exam 325 hrs	
R	Q/SA® Qualified/ Security Analyst Penetration Tester Certification Class	50	$2,995
R	*Q/PTL® Qualified/ Penetration Tester License Class/ Workshop Practical	30	$2,995
R	Q/EH® Qualified/ Ethical Hacker Certification Class	45	$2,995
R	*Q/ND® Qualified/ Network Defender Certification Class Practical	40	$2,995
R	*QFE® Qualified/ Forensic Expert Certification Class Practical	40	$2,995
R	SU CISSP® Certified Information Security Systems Professional Class (optional)	40	$2,995
R	SU CASP® - CompTIA Advance Security Professional Certification Class	40	$2,995
R	SU Security+® CompTIA Certification Class	40	$2,995

O	Python Forensics	40	$2,995
	Q/ISP® Qualified/ Information Security Professional Certification Platinum Pass (Q/EH, Q/SA-Q/PTL, Q/FE, Q/ND)	200	$8,495
	Q/ISP® Qualified/ Information Security Professional Certification Platinum Pass+ (Q/EH, Q/SA-Q/PTL, Q/FE, Q/ND + CISSP)	240	$9,500
Q/IAP CoM	SU Q/IAP® Qualified/ Information Assurance Professional Certificate of Mastery CoM (Q/AAP, Q/NSP, Q/CA*, CISSP CISM, CASP & Security+ , ISMS ISO 27001) Practicals * below	Exam 320 hrs	
R	Q/AAP® Qualified Access, Authentication & PKI Professional Certification Class	40	$2,995
R	Q/NSP® Qualified/ Network Security Policy Administrator & SOA Security Oriented Architect Certification Class	40	$2,995
R	*Q/CA Qualified/ Certification & Accreditation Administrator Certification Class Certificate of Mastery CoM	40	$2,995
R	DoD Information Technology Security Certification and Accreditation Process DITSCAP Certification Class	40	$2,995
R	SU Security+® CompTIA Certification Class	40	$2,995
R	SU CISSP® ISC2® Certified Information Security Systems Professional Class	40	$2,995
R	SU CASP® - CompTIA Advance Security Professional Certification Class	40	$2,995
R	ISSEP® ISC2® Information Security Systems Engineer Certification Class	40	$2,995
R	SU CISA® Certified Information Security Auditor Certification Class	40	$2,995
O	SU CISM® Certified Information Security Manager Certification Class	40	$2,995
O	Certified ISO 27001 SU ISMS® Lead Auditor Certification Class	40	$2,995
O	Certified ISO 27001 SU ISMS® Lead Implementation Certification Class	40	$2,995
Q/WP CoM	SU Q/WP® Qualified Wireless Professional Certificate of Mastery CoM non degree (Q/WP, Q/WSP, Q/WAD® + Security+®, CASP®)	Exam 245 hrs	
R	Q/ WP® Qualified/ Wireless Professional Certification Class (CWNA exam)	40	$2,995
R	Q/WSP® Qualified Wireless Security Professional Cert Class (CWSP™ exam)	40	$2,995
R	*Q/WAD® Qualified/ Wireless Analyst & Defender Bootcamp Class & Practicum	45	$3,490
R	Q/WP®/ Q/WSP® Bootcamp Class (CWNA™/ CWSP™ exam not incl) Qualified Wireless / Qualified Wireless Security Professional Certification Class	(80)	$4,690
R	SU Security+® CompTIA Certification Class	40	$2,995
R	SU CASP® Certified Advance Security Professional Certification Class	40	$2,995
Q/SSE CoM	SU Q/SSE® Qualified/ Software Security Expert Certification Certificate of Mastery CoM nondegree (9 Q/SSE classes + Security+)	Exam 400 hrs	
R	*Q/SSE® Qualified/ Software Security Expert 5 Day Bootcamp Certification Class	40	$2,995
R	Q/SSPT® Qualified/ Software Security Penetration Tester Certification Class	40	$2,995
R	Q/STP® Qualified Software Testing Bootcamp Certification Class	40	$2,995

R	How to Break & FIX Web Security Certification Class	40	$2,995
R	How to Break & FIX Software Security Certification Class	40	$2,995
R	Fundamentals of Secure Software Programming Certification Class	40	$2,995
R	Q/SH/D® Qualified/ Software Hacker / Defender Certification Class	40	$2,995
R	Q/STBP® Qualified/ Software Tester Best Practices Certification Class	40	$2,995
R	*Introduction to Reverse Engineering Certification Class	40	$2,995
R	SU Security+® CompTIA Certification Class	40	$2,995
Q/CDA CoM	Q/CND® Qualified/ Cyber Network Defense Certificate of Mastery CoM (Q/MC, Linux, IDS I, II, III, Q/CND, Security+, CASP or CISSP)	Exam 320 hrs	
R	Q/MC® Qualified/ Mission Critical Certification Class	40	$2,995
R	Linux/UNIX® Security Certification Class	40	$2,995
R	IDS I Catching the Hackers – Introduction to Intrusion Detection Certification Class	40	$2,995
R	IDS II Catching the Hackers II: Systems to Defend Networks Certification Class	40	$2,995
R	IDS III: On-site Log Analysis, Event Correlation and Response (Custom) Certification Class	40	$2,995
R	Q/CND® Qualified/ Cyber Network Defense Certification Class	40	$2,995
R	SU Security+® CompTIA Certification Class	40	$2,995
R	SU CASP® Certified Advance Security Professional Certification Class	40	$2,995
O	Python Forensics	40	$2,995
O	Conducting Network Vulnerability Analysis	40	$2,995
	CISSP® is a registered trademark of (ISC)2® SU CISSP Training classes are not endorsed or sponsored by (ISC)2® CEH® CHFI® are EC Council registered trademarks SU CWNA / CWSP Training classes are not endorsed or sponsored by CWNP®		

Q/EH April 2009 PSparks DoD/DISA/JITC

I have over 20 years experience in both teaching and information security. I am very particular about both and highly concerned with the decline in real training revolving around the current challenges which we face. I was honestly impressed with both the level of expertise and the instructor's ability to relay this information to the students. This is not simply another idiot boot camp but a well reasoned and directed classroom experience which prepares the student for the real world. I was impressed with the hands-on exercises. These combined with the instructor's elevated knowledge base made the class enjoyable and extremely topical. When you compare Security University to other training groups in the region, they are infinitely superior in both talent and developmental materials.

I think that Security University has the right mindset in the development of their classes. They are working to impart valuable knowledge and not simply to push students through. Whereas, I believe

that any student could pass any applicable exam after attending these courses, the test is not the focal point. They deserve to be commended for both their mindset and the efforts that they've made to enhance the knowledge-base of their students. I sincerely appreciate my time learning with Security University and would recommend it to any organization which actually wants to develop real IA professionals.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

The greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development is keeping cyber security education and training/labs & hardware current. The industry and threat landscape changes and evolves so quickly that it can be difficult even for talented cybersecurity professionals to keep pace with new skills, threats, tools and demands. Education should be as responsive by like just in time ordering – keeping ahead of the threat landscape is not the challenge its making time to ensure you stay ahead of cyber events/ skills and tools.

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)?

As technology advances so do tools. Staying ahead of the threat is based on a highly qualified skill set that questions why threat happened because all threats happen *only one of 4 ways* – in the payload from a single event or multiple events or in the header, from a single event or multiple events. Once cybersecurity technicians break down the threat can they defend?
We still have TCP threats to defended.. Anyone can take over anything – due to no regulations.

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:

Look beyond traditional colleges
Discontinue the State Approving Agencies. They fail our veterans when it comes to current education needs - they don't approve certifications that lead to employment.

i. At the Federal level? Add qualified performance based CyberSecurity Certificate of Mastery courses with practicums to engage and validate student's cybersecurity skills. Even if they will never do the role.

Students and instructors have called congressman, veterans affairs both Local and Federal – to no avail, Qualified at SU has not been counted.. so we continue to have a certified, yet unqualified cybersecurity workforce.
CLASSIFICATION: UNCLASSIFIED

Mr Harvey, Governor Mc, I am reaching out to you for consideration and request to obtain approval for Security University as an approved school for the GI Bill.

I am a 25 year Army Veteran (currently US Army Reservist) and working to synchronize my career fields over the last 20 years (Military Intelligence, Commercial IT operations and now Cyberspace Security Engineering and Operations).

At the end of 2014, I came off of a one year mobilization at USCYBERCOM HQs supporting Cyberspace Operations. Having years of previous experience in IT management, Development, and support, I was not current with the work force because I did not have certifications to go along with my years of experience in the military and civilian world. Job hunting as you can imagine was difficult without having the certifications to go with my name. I was fortunate to attended using SU's grant program, since I was unable to use my GI Bill for approved technical training. I would prefer to use my GI Bill to take technical skills training that can keep me relevant in this field instead of trying to rely on a long term degree program that is more focused on theory rather than actual and current applications.

I started using Security University in early 2015 and within a few months I completed training that helped me certify in CISSP and Security +. I also took classes in Forensics and Wireless Security Applications. All of this training was a significant boost to my development as a leader and operator in the field of cybersecurity. I was picked up for a position at Vencore Inc, to be the Lead Security Engineer under a DHS contract supporting the Einstein Program and later selected as the Technical Lead on a new contract with CYBERCOM J3 for DoDIN Operations. In addition to my civilian career boost. The Certifications and training also played a role in my selection as the Chief Engineer for the 335th Signal Command (T)(P) in Camp Arifjan, Kuwait; where I am currently stationed.

I have been around SU for several years now and they have a commitment to help veterans in training and becoming not just certified but qualified cyber experts. Upon my return I would like to take more courses at SU and be able to use my GI bill to do so. The courses are better designed to keep up with the changing cyber environment than most of the courses offered at your traditional colleges and universities.

What I know of the school and can attest to:
SU is CH 31 Vo Rehab approved since 2006 - see attached.
SU is SCHEV Certified to Operate since 2006 - SU does Certificate - non degree granting programs.
SU courses are NSA- CNSS approved since 2009.
SU is MSA- CESS accredited until 2022

To my knowledge SU has had 0 student complaints, 0 student or school debt, 9 student refunds in 16 years.

I am also aware that there have been some issues with the State Approving Agency that I think SU has not been given a fair effort nor appeal process. I requested from the school a copy of the reply submitted on the non-compliance issues identified and was denied access, review or discussions.

I request that SU is provided a fair assessment. This will support veterans to use their GI bill and who are looking to get themselves qualified to work in the field of Cyberspace Operations and Support which is desperately needed in the Military, Government, and Commercial sector in order to defend our resources.

Thanks for your time.
LTC, MI Chief Engineer
G35, 335th SC (T) (P)
Camp Arifjan, Kuwait

ii. At the state or local level, including school systems? Work with State Postsecondary to improve performance based CyberSecurity skills that result in Certificates of Mastery

iii. By the private sector, including employers? Focus on qualified training with practicums that result in a Certificate of Mastery that results in a qualified and validated workforce.

iv. By education and training providers? Unite to build a qualified workforce model from Security University's successful Certificate of Mastery programs

v. By technology providers? Make them become accredited and held to a compliance standard.

Kevin Kimball,

NIST Chief of Staff.

Footnotes

1. Exec. Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 FR 22391 (May 16, 2017).
Back to Citation