A Department of Defense Report on the National Security Agency and Department of Homeland Security Program for the "National Centers of Academic Excellence in Information Assurance Education Matters"

In Response to Section 942 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66)

FEBRUARY 2015

Terry Halvorsen
DoD CIO

The estimated cost of this report or study for the Department of Defense is approximately $242,000 in Fiscal Years 2014 - 2015. This includes $228,000 in expenses and $14,000 in DoD labor.
Generated on 2015Jan28 RefID: 0-72C6A9D

Department of Defense Report on the National Security Agency and Department of Homeland Security Program for the "National Centers of Academic Excellence in Information Assurance Education Matters"

In Response to Section 942 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66)

DoD CIO
3020 Defense Pentagon
Washington, D.C. 20301-3020

Distribution Statement A: Approved for public release when Attachment 2 is removed

Contents

Attachments:

This page intentionally blank.

1 Introduction

This Report on the National Security Agency (NSA) and Department of Homeland Security (DHS) Program for the National Centers of Academic Excellence (CAE) in Information Assurance (IA) and Cyber Defense (CD) is in response to section 942 of The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2014 (Public Law 113-66) (See Attachment 1).

Over the last year, the Department of Defense Chief Information Officer (DoD CIO), in coordination with NSA's Information Assurance Directorate (IAD) and DHS's Assistant Secretary, Cybersecurity and Communications (CS&C), assessed the processes and criteria used to develop and designate cybersecurity[1] programs at institutions of higher education as CAE IA/CD.[2] DoD CIO contracted a portion of the overall analysis of the CAE IA/CD program to the Institute for Defense Analyses (IDA) for an independent, objective assessment of the National CAE program (See Attachment 2). While DoD CIO does not fully support all of the findings and recommendations, the IDA independent assessment provided foundational input to the DoD Assessment, Findings and Recommendations, and Implementation Plan included in this report.

The IDA assessment and the overall DoD CIO effort involved a variety of data collection methods, including not-for-attribution interviews with representatives from academic institutions and stakeholder organizations of the CAE program, as well as feedback from CAE public-private (industry, academia and government) stakeholder engagements. These engagements included the annual Colloquium for Information Systems and Security Education in June 2014, and the National Institute for Standards and Technology (NIST)-hosted National Initiative on Cybersecurity Education (NICE) Conference/Exposition in November 2014. IDA also interviewed representatives from NSA IAD and DHS CS&C. Other sources of information incorporated into the assessment include input from Federal Agencies; research information from the review of academic papers relating to the CAE program; publicly available documents from agency websites such as DHS, DoD, and NSA; and recommendations from subject matter experts.

The DoD Assessment, Findings and Recommendations informed a new Implementation Plan, which is best represented by the "way-ahead presentation" given by CAE IA/CD Program leadership at the CAE Principals Meeting immediately preceding the November 2014 NICE Conference (see Attachment 3). The briefing identifies actions, including timelines and considerations, to position the CAE IA/CD Program to improve and evolve the mechanisms and

[1] The term cybersecurity will be used throughout this report to be consistent with the National Initiative for Cybersecurity Education (NICE) Workforce Framework. Using a broader label, the Department of Defense Cyberspace Workspace Strategy has identified the cybersecurity, cyber effects, information technology, and cyber intelligence workforce elements to be consistent with the NICE Workforce Framework.

[2] NSA/DHS National CAE IA/CD is the new name of the program previously called the NSA/DHS National CAE for Information Assurance in Education.

processes for developing courseware and other criteria for the CAE IA/CD program. The briefing describes a closer alignment with the NICE Program and its management and also a more interactive engagement, better considering industry and academia input. Together, the independent IDA Assessment, and the DoD Assessment, Findings, and Recommendations, and Implementation Plan provide the required responses to the Secretary of Defense tasking in section 942 of NDAA for FY 2014.

2 Department of Defense Assessment

2.1 CAE Program History and Current Status

In the late 1990s, in response to increasing threats to national security associated with vulnerabilities in IA and information technology (IT), and recognizing a need for a formal program to broaden the scope and enhance knowledge and skills in IA among professors and graduates, NSA launched the National Centers of Academic Excellence in IA Education Program (CAE/IAE). The CAE/IAE program has been an invaluable and necessary resource in enhancing the capability of our Nation's academic institutions to provide the education necessary to produce graduates with the knowledge and skill base required to provide for the cybersecurity of our Nation. Beginning with seven institutions in 1999, the program has grown to 181 two-year, four-year and graduate institutions designated as CAEs (as of June 10, 2014).[3] DHS became a CAE Program leadership partner in 2004. Original "CAE-designation criteria" was based on National Security Telecommunications and Information Systems Security Committee (NSTISSC)[4] training standards now referred to as the Committee on National Security Systems (CNSS). In late 2012, NSA announced a new Knowledge Unit (KU) and Focus Area (FA) framework to replace the outdated CNSS-based standards. NSA conducted a series of six CAE face-to-face workshops, and three webinars from January to March 2013 to socialize and evolve their KU construct. All 181 CAEs were invited to participate in the workshops and webinars, and over 70 representatives participated. CAE concerns with the KU workshop/academic input process and NSA's aggressive KU-implementation timeline led to Congressional interest (e.g., section 942 of the NDAA for FY 2014). To date, more than half of the now 181+ CAEs have mapped their courseware to the current KUs.

[3] Maconachy, Vic Dr., History of the CAEs: Part of a Broader Cyber Defense Stratagem. Paper, September 15, 2011
[4] The NSTISSC is the predecessor to the current Committee on National Systems Security, which comprises voting members from 21 U.S. Government Executive Branch departments and agencies. In addition, 14 official Committee Observers represent additional organizations outside of the executive Branch. The CNSS protects National Security Systems by developing operating policies, procedures, guidelines, directives, instructions, and standards. http://www.cnss.gov.CNSS/about/structure.cfm.

2.2 National CAE Program

One of the strengths of the program is that the existing National CAE mission and objective remain valid in today's dynamic cyber world:

> **Mission:** The purpose of the National CAE designation program is to promote higher education in IA and CD and prepare a growing number of IA/CD professionals to meet the need to reduce vulnerabilities in the Nation's networks.[5]
>
> **Objective:** Through partnerships with government, academia, and industry, NSA's IA mission advocates improvements in IA education, training, and awareness.[6]

NSA and DHS jointly sponsor the CAE/IAE, Two-Year IA Education, and IA Research programs. Many students attending CAE IA/CD-Education and -Research institutions are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal CyberCorps: Scholarship for Service program. Designation as a CAE does not carry a commitment for funding from NSA or DHS. CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.[7]

2.3 Maturity of IA as an Academic Discipline and the Role of the Federal Government in the CAE Program

IA as a cybersecurity discipline, while evolving, remains a relatively immature, multi-disciplinary field of study. Over the last 15 years the government, private sector, and higher education institutions in the United States and across the globe have greatly expanded their understanding of cybersecurity and their programs to train and educate the cybersecurity workforce. The bodies of knowledge and the variety of roles in cybersecurity are continuing to expand in response to an increasingly sophisticated and pervasive threat environment, new technologies, and changing laws and policies.

Government should continue to lead the CAE Program; there are currently no industry/academic organizations volunteering and/or qualified to lead a CAE-like designation program/process. There is a relatively new (July 2014) public-private initiative called the Cyber Education Project (CEP)[8] that is exploring "cyber science" accreditation. While there is positive discussion in CEP on the need for a high-level cyber field of study, development of "cyber science" educational objectives necessary to move forward is just starting. Some form of "cyber" accreditation is at least two to three years away and another two to three years for implementation. Other recent

[5] https://www.nsa.gov/ia/academic_outreach/nat_cae/
[6] https://www.nsa.gov/ia/academic_outreach/index.shtml
[7] https://www.iad.gov/NIETP/
[8] www.CyberEducationProject.org

studies exploring the need for professionalization of the cyber workforce are using the analogy of the many professions in the broad medical profession.[9] The KU/FA framework is one mechanism for schools to begin this process for cybersecurity workforce development. In the future, when the academic program accreditations are mature and congruent with the array of important roles in cybersecurity, the IA/CD CAE Program should re-evaluate the need to offer its designations.

2.4 Alignment with NICE

The CAE Program is currently investigating closer connectivity to the NIST-led National Initiative on Cybersecurity Education (NICE). The NICE Workforce Framework is a national resource that categorizes, organizes, and describes cybersecurity roles. NICE developed the Workforce Framework to provide educators, students, employers, employees, training providers, and policy makers with a systematic way for organizing the way we think and talk about cybersecurity work and what is required of the cybersecurity workforce. The NICE Workforce Framework and the new DoD Cyberspace Workforce Strategy[10] are congruent in their recognition of the broad and diverse nature of the workforce needed in this field. The CAE program's current KUs are designed for a narrower, but critically important focus on the cybersecurity technical workforce.

3 Findings and Recommendations

3.1 Scope

Finding: The CAE IA/CD Program's KU-construct currently focuses on education related to the more technical aspects of the cybersecurity workforce. While critical, these technical specialties, competencies, and knowledge, skills, and abilities do not fully consider the broadly described cybersecurity workforce identified in the NICE Workforce Framework. The CAE Program should retain a focus on technical aspects of cybersecurity as well as expand to align with the roles of the broader workforce and their higher educational needs.

Recommendation: In collaboration with higher education institutions and their subject matter experts, and representatives of government and industry, the managers of the CAE IA/CD

[9] (1) Libicki, Martin C., Senty, David, and Pollak, Julia. (June 17, 2014) "H4ckers5 Wanted: An Examination of the Cybersecurity Labor Market". RAND Corporation National Security Research Division. (2) National Research Council. "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision Making". Washington D.C: The National Academies Press, 2013 (3) Spidalieri, Francesca, Kern, Sean. (August, 2014) "Professionalizing Cybersecurity: A path to universal standards and status". Pell Center for International Relations and Public Policy.

[10] Department of Defense Cyberspace Workforce Strategy (2014). Signed 4 April 2014.

Program should broaden its educational scope to include the cybersecurity workforce roles identified in the NICE Workforce Framework.

3.2 Governance/ Stakeholders

Finding: The scope, focus, and criteria of the IA/CD CAE Program do not adequately reflect the full spectrum of the perspectives of stakeholders in the federal government, academia, and industry about the cybersecurity workforce needed by the nation.

Recommendation: Broaden the governance structure and stakeholder engagement to focus on the national cybersecurity workforce by including more government stakeholders in addition to DHS and DoD/NSA, possibly National Science Foundation (NSF), NIST, or others, as well as representatives of academia and industry.

3.3 Designation Criteria and Process

Finding: The newly implemented CAE IA/CD designation criteria KUs were developed to influence cybersecurity courseware of higher education. While the KU construct is endorsed by the CAE IA/CD community as a valid replacement for the previous CNSS coursework criteria, the current KUs consist of technical topics of uneven quality and depth, and are focused towards lower level learning outcomes. Also of concern are: 1) the requirement that four-year and graduate programs map to the very basic KUs of two-year programs, and 2) the overemphasis on technical depth required of programs that prepare graduates for roles in, for example, information management and leadership, law enforcement, and information risk management/economic impacts of cyber effects.

Recommendation: To meet the needs of the national workforce comprised of knowledgeable and competent experts in a wide variety of cybersecurity roles, the CAE IA/CD Program needs to collaborate with higher education, government, and industry to review and refine the KUs and FAs to enable institutions to develop and offer cybersecurity academic programs of high quality. This process should be informed by curriculum guidelines such as the Institute of Electrical and Electronics Engineers (IEEE)/Association for Computing Machinery (ACM) December 2013 *Computer Science* Curricular Guidelines for topics and higher level learning outcomes.[11]

3.4 CAE Designation Process vs. Cybersecurity Accreditation

Finding: The current process, mechanics, and deadlines by which higher education institutions must apply for CAE IA/CD Program designations are labor intensive, lack clarity in courseware criteria, and demand a multitude of artifacts, often with short timelines. A better understanding

[11] The Joint Task Force on Computing Curricula ACM/IEEE Computer Society. "Computer Science Curricula 2013 Curriculum Guidelines for Undergraduate Degree Programs in Computer Science." Page 138. December 20, 2013.

of academic processes, schedules, and institutional governance would be beneficial. Site visits are considered essential and were promised, but were conducted only by exception as a result of 2013 furloughs and limited resources. Accreditation for Cybersecurity is not a near-term prospect; however, efforts to pursue accreditation have begun independent of the CAE IA/CD Program.

Recommendation: The managers of the CAE IA/CD Program should engage with representatives of the CAE IA/CDs to refine and streamline the designation processes, mechanics, and schedules. Consider methods to pursue site visits or other methods of direct engagement despite budget restraints. CAE IA/CD Program leadership should engage in ongoing cyber accreditation initiatives.

4 Assessment of the DoD IA Scholarship Program (IASP)

In addition to CAE Program questions, DoD was asked to examine the IA Scholarship Program (IASP).

4.1 IASP Overview

The IASP serves as a mechanism to build the nation's IA infrastructure through grants to colleges and universities designated by the NSA and DHS as CAE IA/CD. It is designed to increase the number of new entrants (recruits) to DoD who possess key IA and IT skill sets; as well as to serve as a vehicle to develop and retain well-educated military and DoD civilian personnel who support the Department's critical IT management and infrastructure protection function.

4.2 IASP Benefits

There are several benefits associated with the IASP. There is a commitment of new IA/cybersecurity personnel through service obligation, direct selection of new IA/cybersecurity personnel to meet critical needs, continuous flow of top IA/IT talent educated to CAE requirements, strengthened IA/cybersecurity capability of the DoD IT/IA (cyberspace) workforce, and curriculum and research development at CAEs.

4.3 IASP Assessment

Since its inception in 2001, the IASP has been directly tied to CAE-designated institutions. To date, the IASP has employed 593 (366 recruitment/227 retention) students, and has enabled CAEs with 180 capacity-building grants. In today's environment, the cost of education is on the rise and resources are constrained. The capacity to meet the current and future demand of a high quality IA/cybersecurity workforce is dependent on the resources allocated to support the IASP program. Additionally, the success and quality of an IASP student's education is dependent on

the academic institution and the caliber of the CAE program requirements. The IASP continues to be a beneficial program. Current DoD funding for the IASP continues to be a challenge due to budget constraints and DoD is exploring the potential for an IASP-like program in DoD in coordination with other governmental cyber education programs.

5 Implementation Plan

The NSA/DHS leadership team for the CAE Program provided an update on the program at the November 4, 2014, CAE Principals Meeting held the day before the Annual NICE Conference. The update included a morning plenary presentation and an afternoon "workshop/discussion" with numerous CAE representatives. See Attachment 3 for the briefing slides.

Per the briefing, the CAE Program leadership team will undertake the following activities to continue to evolve the program:

- Pursue alignment with the broader government initiatives, such as NICE, and seek more effective partnerships with CAE Program stakeholders in industry and academia.
- Pilot a new CAE "collegiate" sub-group under the NICE Working Group structure in 2015.[12] The working group will include government, industry, and academic stakeholder representatives (possibly 3 each per community). The working group will provide input to KU management (selection, criteria, and implementation timelines) and other CAE community issues.
- Conduct a series of face-to-face meetings and webinars in 2015, discussing CAE way ahead planning.
- Establish a better web-presence in the pursuit of a more transparent process and more effective two-way communication.
- Complete the migration of CAEs to the new (and evolving) KU construct as existing CNSS-based designations expire. CAE Program Leadership reported that roughly half of the CAEs had adopted the new KU construct thus far. The last of the designations awarded under the original CNSS-based criteria expire in 2017.

6 Conclusion

The National CAE IA/CD program's mission remains vital to protecting our nation's security. The demand for the designation has grown over the years in part because of the growing global

[12] The NICE Working Group was established in January 2015 by the Cross-Sector Cyber Security Working Group, an advisory body operating under the auspices of the Critical Infrastructure Partnership Advisory Council.

attention to cybersecurity and a strong demand signal from academic institutions who want to prepare their students to join the cyber workforce. However, as the cybersecurity field has evolved, awareness of the areas of knowledge needed has outpaced the growth and direction of the program. Additionally, the Federal Government has developed a broader approach to address the cyber workforce needs through efforts such as NICE and the DoD Cyberspace Workforce Strategy. It is DoD's intent to better align the National CAE program with these two efforts, for the greater understanding of the complex and dynamic Cyber academic and job market of the federal government and private sector. It is also important to establish and maintain robust community and stakeholder engagement in both NICE and the CAE program to develop courseware and processes for CAE designations.

Acronyms

ACM	Association for Computing Machinery
CAE	Centers for Academic Excellence
CAE/IAE	National Centers of Academic Excellence in IA Education
CD	Cyber Defense
CEP	Cyber Education Project
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CS&C	Cybersecurity and Communications
DHS	Department of Homeland Security
DoD	Department of Defense
FA	Focus Area
IA	Information Assurance
IAD	Information Assurance Directorate
IASP	Information Assurance Scholarship Program
IDA	Institute for Defense Analyses
IEEE	Institute of Electrical and Electronics Engineers
KU	Knowledge Unit
NICE	National Initiative on Cybersecurity Education
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee

Department of Defense Report on the National Security Agency and Department of Homeland Security Program for the "National Centers of Academic Excellence in Information Assurance Education Matters"

In Response to Section 942 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66)

DoD CIO
3020 Defense Pentagon
Washington, DC 20301-3020

Distribution Statement A: Approved for public release when Attachment 2 is removed