

# Journal of Cybersecurity Education, Research and Practice

Volume 2019 | Number 1

Article 4


June 2019

## Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach

Lucy Tsado

Lamar University, [ltsado@lamar.edu](mailto:ltsado@lamar.edu)

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/jcerp>

 Part of the [Curriculum and Instruction Commons](#), [Higher Education Administration Commons](#), [Information Security Commons](#), [Legal Studies Commons](#), [Management Information Systems Commons](#), [Other Social and Behavioral Sciences Commons](#), [Public Affairs, Public Policy and Public Administration Commons](#), [Scholarship of Teaching and Learning Commons](#), and the [Technology and Innovation Commons](#)

### Recommended Citation

Tsado, Lucy (2019) "Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2019 : No. 1 , Article 4.

Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/4>

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact [digitalcommons@kennesaw.edu](mailto:digitalcommons@kennesaw.edu).

---

# Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach

## **Abstract**

The human resource skills gap in cybersecurity has created an opportunity for educational institutions interested in cybersecurity education. The current number of schools designated by the Department of Homeland Security (DHS) and National Security Agency (NSA) as Centers of Academic Excellence (CAE) to train cybersecurity experts are not sufficient to meet the shortfall in the industry. The DHS has clearly mapped out knowledge areas for cybersecurity education for both technical and non-technical disciplines; it is therefore possible for institutions not yet designated CAEs to generate cybersecurity experts, with the long-term goal of attaining the CAE designation. The purpose of this paper is to emphasize the need for a top-driven, multidisciplinary approach to cybersecurity education especially at schools that have not yet been designated as Centers for Academic Excellence. The paper also suggests a multi-faceted approach and the important considerations needed to achieve a successful cybersecurity educational program.

## **Keywords**

Center for Academic Excellence (CAE), cybersecurity education, top-driven strategy, multidisciplinary approach, skills gap, technical disciplines, nontechnical disciplines, knowledge units

## INTRODUCTION

Cybersecurity has become an important business function in many organizations due to the rise in cyberattacks. The growth in various forms of cybercrimes and cyberattacks globally has warranted the need for cybersecurity experts who are skilled to respond, protect, defend, and prevent breaches. However, a serious cybersecurity skills gap has developed because of the limited number of experts in the field. The skills gap developed as a result of the late recognition of cybersecurity as an academic field in the late 1980s to early 2000s. Information and communications technology (ICT) proliferated widely without the appropriate accompanying security measures. The resulting cybersecurity skills gap crisis highlighted the need to create and equip institutions of higher learning to develop experts in cyberdefense to close the skills gap. Many institutions of higher learning started to create cybersecurity programs. The unsystematic development of cybersecurity programs, however, warranted some structure. The need for this structure gave birth to the National Security Agency (NSA) and Department of Homeland Security (DHS) joint sponsorship of the National Centers of Academic Excellence (CAE) designation to guide cybersecurity educational programs.

The purpose of this paper is to propose and emphasize the need for a top-driven, multidisciplinary school-wide strategy in creating cybersecurity educational programs at universities and institutions of higher learning. The second purpose of this paper is to argue that both technical and nontechnical fields need to be included in this strategy. In addition, while the CAE designation is important, it is possible for schools that do not have a CAE designation to generate cybersecurity experts in specific fields of expertise to address the skills gap and pipeline deficiency in cybersecurity. This paper provides suggestions for how an institution of higher learning can plan and execute a cybersecurity education strategy that will allow it to succeed in generating cybersecurity talent and eventually obtain a CAE designation if it so chooses. The paper discusses what schools should do to successfully implement a top-driven, multidisciplinary school-wide strategy to generate cybersecurity talent. While the discussions in this paper are limited to suggestions for schools within the United States, international schools and academic communities can adapt these suggestions to suit their educational programs. A top-driven, multidisciplinary approach to a cybersecurity educational strategy will benefit any institution in the United States or abroad. The scope of the discussions in this paper is, however, limited to the cybersecurity skills gap challenge; a description of the CAE designation in the United States; arguments for a multidisciplinary, top-driven strategy approach to

cybersecurity education; and recommended suggestions for a multifaceted approach to a cybersecurity education program.

## **THE CYBERSECURITY SKILLS GAP**

Evans and Reeder (2010), policy evaluators for the Center for Strategic and International Studies (CSIS), described the cybersecurity skills gap as a “crisis in cybersecurity” (p. v). They also stated that the critical skills gap necessitated a move to increase both the number and quality of cybersecurity experts to fill positions, as well as to provide a pipeline of experts to address the deficiency. In addition, the International Information System Security Certification Consortium (ISC)<sup>2</sup>, a nonprofit organization that trains information security (IS) experts, has been sounding the alarm regarding the acute shortage of experts needed to fill the pipeline deficiency in its periodic global studies on cybersecurity workforce issues since 2011. ISC<sup>2</sup>’s 2017 report stated that by the year 2022, the global shortfall in information security experts is projected to reach 1.8 million. This figure is up 20 percent from the shortfall figure of 1.5 million projected in the 2015 report (Center for Cyber Safety and Education and International Information System Security Certification Consortium [ISC]<sup>2</sup>, 2017).

The “acute” skills gap in cybersecurity has created an opportunity for schools interested in cybersecurity education. It is evident from the growing shortfall identified by ISC<sup>2</sup> that the current number of Centers for Academic Excellence (CAE)—designated schools in the United States is not sufficient to generate the number of cybersecurity experts needed in the industry. This dearth was quantified by Tsado (2016), who found that only 194 (about 4 percent) of the United States’ degree-granting institutions of higher learning as defined by the National Center for Education Statistics were designated CAEs as of 2016. At the time of writing, the number of CAE-designated schools stands at 276, representing about 6 percent of the 4,583 two- and four-year degree-granting institutions of higher learning in the United States. This is still inadequate to produce the quantity of experts needed to fill the gap or provide a pipeline of experts for the field. Therefore, many institutions of higher learning can and should get involved in training cybersecurity talent.

The cybersecurity skills gap has created the need—and, more importantly, an opportunity—for as many schools as are interested to get involved, which would be beneficial to the cybersecurity community in three ways. First, it provides an opportunity for schools to become involved in the generation of cybersecurity experts. Second, it provides a unique opportunity for both technical and nontechnical students who would not otherwise be interested in cybersecurity to be trained to enter the field. Finally, it provides a short-term goal of producing

cybersecurity experts with the eventual long-term goal of more schools attaining the CAE designation. The short- and long-term goals of attaining the CAE designation are beyond the scope of this paper. However, it is pertinent to note that with cybersecurity education Knowledge Units (KUs) clearly mapped out, a cybersecurity education is now possible at institutions not yet designated as CAEs with a long-term goal of obtaining the CAE designation.

## **THE CAE DESIGNATION**

The National Centers of Academic Excellence designation is awarded through the joint efforts of the NSA and DHS. Schools are awarded the designation only after meeting certain rigorous criteria. According to the National Information Assurance Education and Training Programs (NIETP), the designation has two varieties: NSA/DHS National Center of Academic Excellence in Cyber Education (CAE-CD) and NSA/DHS National Center of Academic Excellence in Cyber Operations (CAE-CO). The CAE-CD includes two areas of expertise, Cyber Defense Education (CAE-CDE) and Cyber Defense Research (CAE-R). Any two- or four-year educational institution must fulfill specific requirements in the designated area to be awarded the designation for that area of specialization (NIETP, n.d.). The goal of the NSA and DHS is to identify educational institutions of higher learning that are interested in teaching and conducting research in the field of cybersecurity.

Although this paper does not underplay the importance of CAEs, it recognizes that not all schools have the immediate capacity and resources to meet the CAE designation criteria. In any case, schools interested in applying for the CAE designation must offer cybersecurity education for at least three years before the application (NIETP, n.d.). Therefore, obtaining the CAE designation could be a long-term goal for institutions. Appendix 1 provides a checklist for a four-year CAE application for cyber defense.

## **Cybersecurity Education Should Include Both Technical and Nontechnical Disciplines**

Cybersecurity is perceived to be a technically oriented field, but in many ways, it involves the collaboration of many disciplines and thus many different fields of study. The general myth is that the cybersecurity field is only suitable for those in the fields of information technology and computer science. This is far from the truth. Contrary to that opinion, ISC<sup>2</sup> is calling for nontechnical academic fields to get involved in the cybersecurity workforce stating “Report calls for employers to look for new recruitment channels and consider workers with more diverse skillsets and non-technical backgrounds to attract and retain cybersecurity talent” (ISC<sup>2</sup>, 2017).

ISC<sup>2</sup> has also consistently reported in its periodic surveys of those in the information security field that to be a successful IS expert, a person needs other skills in addition to technical expertise. In the 2015 survey, a clear majority of IS respondents (90 percent) stated that communication skills were vital for IS experts to be successful at their jobs. Other areas of knowledge identified as important were regulatory policy (71 percent), security policy formulation and application (70 percent), leadership skills (69 percent), and business management skills (53 percent). In 2013, ISC<sup>2</sup>'s top executives issued a report titled *A View from the Top: The (ISC)2 Global Information Security Workforce Study CXO Report*, in which 74 percent of respondents stated that they spent most of their time on governance, risk management, and compliance (ISC<sup>2</sup>, 2013). Training experts to handle these tasks would free top management to do other important managerial tasks. This indicates that these are needed skillsets that are generally nontechnical. Evans and Reeder (2010) also determined that critical thinking skills and the ability to solve everyday problems are essential in the cybersecurity field. In fact, Dupuis (2017) and McGettrick (2013) both suggested that cybersecurity education should be an integral part of every major. Their common argument rests on the consideration that cybersecurity has become an important business function of any organization using information technology and information systems.

Figure 1 on the next page shows that a four-year college may choose to develop a nontechnical core as its cybersecurity educational strategy, which consists of various knowledge units: cyber threats; policy, legal, ethics, and compliance; security program management; security risk analysis; and cybersecurity planning and management. Therefore, educational disciplines such as policy and security studies, criminal justice, medical sciences, and business-concentrated majors, to mention a few, can benefit from this nontechnical core. However, it is important to note that the technical and nontechnical cores are not necessarily mutually exclusive. It is, therefore, important for institutions to approach a strategy from an interdisciplinary standpoint, as discussed later in this article.

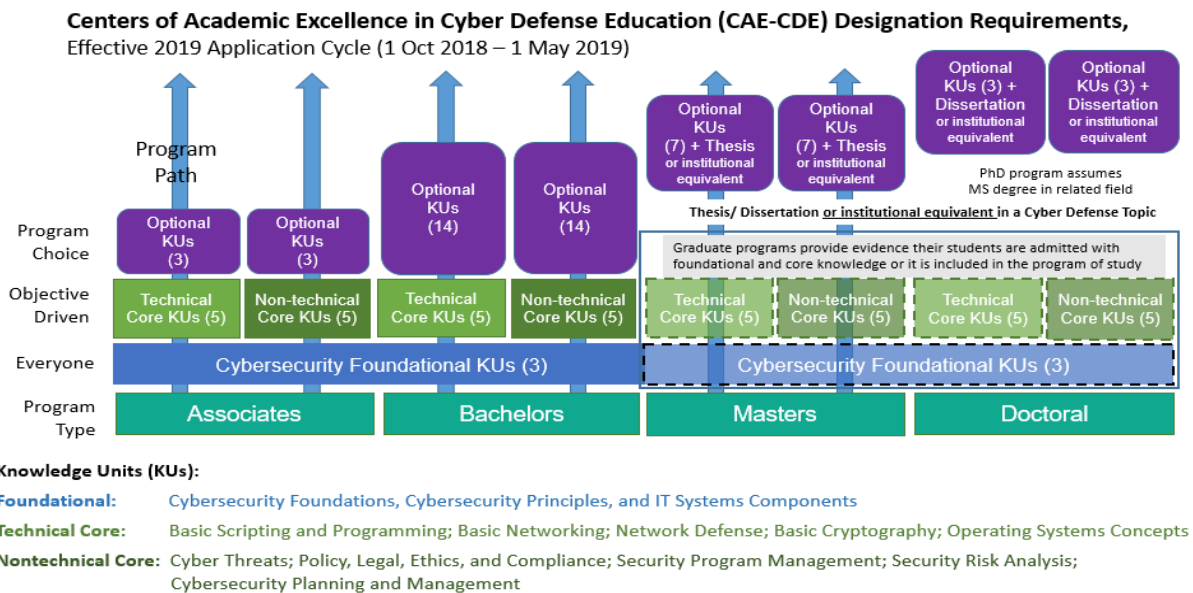


Figure 1: CAE Designation Requirements for Cyberdefense for Cycle 2018–2019.

Adapted from: National IA Educational and Training Programs at [https://www.iad.gov/NIETP/documents/Requirements/CAE-CD\\_2019\\_Knowledge\\_Units.pdf](https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf)

An interdisciplinary approach is needed to develop a successful cybersecurity educational strategy that will involve both technical and nontechnical disciplines. An assessment of cybersecurity degree programs—particularly those that lie in departments outside of computer science—bears this out. In 2014, the Ponemon Institute identified the top twelve schools for cybersecurity, and the placement of their cybersecurity degrees is telling (see Table 1). One of the major findings of this study was that cybersecurity education in these twelve CAE-designated schools cut across other disciplines apart from computer science, such as engineering, management, and policy studies. There was also an emphasis on courses that included leadership, governance, and information security policy, as well as a deliberate focus on career development and professional advancement for students.

S/No	University Identified in Ponemon Study	Department Housing Cybersecurity/Faculty
1.	University of Texas, San Antonio	College of Business
2.	Norwich University	Computer Science
3.	Mississippi State University	Computer Science and Engineering
4.	Syracuse University	Computer Science and Engineering
5.	Carnegie Mellon University	Computer Science and Engineering
6.	Purdue University	Computer Science and Information Technology
7.	University of Southern California	Computer Science
8.	University of Pittsburgh	Computing and Information
9.	George Mason University	Faculty: Engineering, Business, and Public Policy
10.	West Chester University of Pennsylvania	Computer Science
11.	US Military Academy, West Point	Electrical Engineering and Computer Science
12.	University of Washington	Institute of International Studies

*Table 1: Ponemon Institute 2014 Study: Top twelve universities for recruiting cybersecurity talent and the departmental placement of their cybersecurity degree programs*

These are all persuasive arguments that cybersecurity requires a top-driven, multidisciplinary approach incorporating a variety of disciplines within and outside the technical sphere to push forward a successful strategy at any school. There are various areas of specialization in cybersecurity education from which students in both technical and nontechnical disciplines can benefit. Therefore, involving students in nontechnical fields would not only increase the number of cybersecurity professionals, but also provide increased opportunities for a given institution to be designated as a CAE if it so chooses.

It is in the best interest of a school to adopt a top-driven, multidisciplinary, school-wide strategy to determine how to approach its cybersecurity education to include both technical and nontechnical cores.



## **ARGUMENTS FOR A TOP-DRIVEN, MULTIDISCIPLINARY APPROACH TO CYBERSECURITY EDUCATION**

Though the CAE designation is a laudable achievement, not all schools can easily or immediately attain it. Some institutions of higher learning are at a disadvantage because of failure to capitalize on the opportunities to attain this designation in the early years after its inception. Others simply did not have the resources to attain the designation. In addition, the myth that cybersecurity education is only attainable within computer science and technologically oriented fields persists today, although it is less prevalent than it once was, as evidenced by the expansion of the CAE designation to more schools. Currently, however, institutions of higher learning can still generate cybersecurity experts if they do not hold a CAE designation by having a top-driven, multidisciplinary school-wide strategy for cybersecurity education. The long-term goal of attaining the CAE designation is important because the award improves a school's status and increases the chances of attaining needed resources and funding to improve educational programs and research.

### **Top-Driven Management Support**

A top-driven strategy is important for success in cybersecurity education. The overall aim is to increase the quality and quantity of cybersecurity talent, contribute to the pool of talent to reduce the skills gap and pipeline deficiency, and provide students with a career path that is both rewarding and unique. Organizations now recognize cybersecurity as a top business function (Sherif, Pitre, & Kamara, 2016). Institutions of higher learning should give cybersecurity education the same importance.

A school with a top-driven approach to cybersecurity in both awareness and development of educational programs is well positioned to succeed at developing a successful cybersecurity program because such programs need the buy-in and support of top management who understand the importance of cybersecurity as a business function and give it the necessary attention. Sherif, Pitre, and Kamara, (2016), emphasized this when they stated that unethical behavior is prevented in organizations when the people at the top advocate strong organizational culture and leadership values that encourage ethical behavior rather than using enforcement to make people behave ethically when using information systems.

Schools should ensure that they use any resources available to them to attract and develop cybersecurity talent. Such resources should include organizations and cybersecurity professionals in their local communities who will provide internships, employment, and academic-industry partnerships that will enhance the development of a vibrant cybersecurity community. Other resources could include access to information about grants, scholarships, and competitions that can enrich the cybersecurity community within a university or college and its local environs.

### **Multidisciplinary and School-Wide Approach/Strategy**

The National Science Foundation's sponsored workshop on cybersecurity research and education identified a multidisciplinary approach as a top priority for developing cybersecurity education. The report stated that five years was an ideal time to achieve an educational program at academic institutions using a multifaceted approach. The 2014 NSF report also stated that "cybersecurity is a multi-faceted problem that requires professionals with expertise in computing, law, finance, business, psychology, medicine, epidemiology, insurance, technology, public policy, and many others" (p. 7).

In agreement, Dr. Bhavani Thuraisingham, a Louis A. Beecherl Jr. Distinguished Professor at the University of Texas at Dallas, stated that "interdisciplinary education for cybersecurity is essential. It is not only about computer science and engineering. We are working to bring together multiple programs from our university—criminology, brain sciences, statistics, ethics, healthcare, informatics, economics and risk analysis—to truly develop a comprehensive approach to security thinking" (as cited in Vireos, 2013, p. 14).

Finally, Vireos (2013) also pointed to an interdisciplinary approach as a proposed strategy, espousing the importance of a set of leading best practices necessary for cybersecurity education development. Figure 2 below shows the proposal of the promotion of a long-term approach with three major components, one of which is to collaborate within the institution, using a holistic, diverse, and interdisciplinary approach.



*Figure 2: Cybersecurity Education for the Next Generation: Emerging Best Practices.*  
 Adapted from: Marisa Vireos, available at  
[https://www.nist.gov/sites/default/files/documents/2017/01/19/d1\\_trk3\\_viveros\\_cybersecurity\\_education\\_next\\_generation.pdf](https://www.nist.gov/sites/default/files/documents/2017/01/19/d1_trk3_viveros_cybersecurity_education_next_generation.pdf)

A multidisciplinary school-wide educational strategy for cybersecurity would involve a situation where a school can identify and recruit students who would be trained in the cybersecurity field, both technical and nontechnical students can be steered to study cybersecurity, needed resources are sought to bolster a robust cybersecurity academic community, and collaborative partnerships are formed with organizations. It is more adept for an educational institution to address these issues from a top-driven, multidisciplinary approach than with a haphazard approach by individual departments within the institution.

In addition, a school-wide multidisciplinary approach has many advantages: the ability to search for resources and funds as a unit that will benefit the whole school rather than just one department; the efficient, effective, and collective use of resources; and the ability to cast a wide net to identify cybersecurity talent rather than within a few specific disciplines. Moreover, this is one of the checklist questions in Appendix 1: "Does the institution have an officially established entity (either physical or virtual) serving as the focal point for its cyber educational program? The center shall provide the following services: program guidance and oversight; general cyber defense information; and collaboration and

outreach opportunities among students, faculty, and other institutions. Additionally, the center must be supported by a website that is dynamic, current, and visible within the institution and the external community at large” (NIETP, n.d.). Appendix 1 is an example of a checklist for a school applying for a CAE designation for cyber defense.

The second consideration for institutions of higher learning starts with conducting a school-wide cybersecurity awareness program for all members of its academic community. Coffey, Haveard, and Golding (2018) stated that many regulations govern the use of information at schools, but a lack of cybersecurity awareness remains an obstacle to a successful university approach to cybersecurity. They further stated that cybersecurity and the laws that govern information use need to be incorporated in the cybersecurity awareness programs of all schools. Their research highlighted the importance of training to reduce end user errors in the use of information systems that would likely lead to breaches. These laws govern the use of information, exercising the three basic principles of information security: confidentiality, integrity, and availability. The research of Coffey et al. highlights just one example of issues arising from the lack of a university-wide cybersecurity agenda. Such a policy is one of the requirements for a CAE designation. An aspiring CAE school should have a successful campus-wide cybersecurity awareness program that involves consistent up-to-date training of staff involved in the production and use of information.

## **Recommended Suggestions for a Multifaceted Approach to a Cybersecurity Education Program**

In 2014, the National Science Foundation funded a workshop held in Washington, DC, organized by George Washington University, with participants drawn from various fields in both government and private institutions. Participants assessed and developed convincing common approaches to advancing cybersecurity educational programs in United States’ educational institutions. One pertinent finding of the workshop was that cybersecurity education needs a multifaceted approach for success.

Clearly, an approach to a CAE designation would need a top-driven, multidisciplinary, school-wide strategy that would entail sustaining a successful cybersecurity educational program. The possibility of attaining the CAE designation as a long-term goal is also possible if a vibrant cybersecurity eco-community can be developed. Some essential and specific approaches are therefore important considerations when contemplating a cybersecurity educational program:

1. Educational institutions should take steps to identify nearby industries and organizations willing to hire cybersecurity talent (McGettrick, 2013). It is important that the needs of the industry be considered before embarking on specific programs. This would not only help a school to rapidly achieve success for its cybersecurity program, but would also open doors to other opportunities, such as internships and academia–practitioner relationships (see Appendix 1).
2. Institutions must identify which knowledge unit mapping strategies are required to meet the industry’s cybersecurity needs. The NSA and DHS have defined the KUs necessary for various cybersecurity programs (see Figure 1 on page 5). Any school interested in starting a cybersecurity program should also identify which KUs will benefit the industry it is targeting. This will benefit the targeted industry as well as the school and its students. Figure 1 gives an example, showing the KU requirements for a four-year cyberdefense education. Note that the requirement includes both technical and nontechnical KUs.
3. It is essential to identify the resources needed to deliver the identified KUs’ mapping and curricula. These resources may include computer labs, hands-on cybersecurity learning programs, software, and qualified faculty to teach cybersecurity courses. Academic–practitioner partnerships should also be explored as a resource (McGettrick, 2013).
4. For continuity, it is important that institutions invest in K–12 education in nearby school districts by partnering with educators to provide exposure to cybersecurity programs, such as by sponsoring cybersecurity programs, competitions, and scholarships to attract future cybersecurity talent. This will be yet another way to identify schools that will feed into the colleges, as well as to recognize future cybersecurity talent while at the same time enabling a steady flow of identified talent into the schools’ cybersecurity programs (see Appendix 1).
5. Educational institutions must strive to develop and sustain a cybersecurity eco-community that will ensure that all stakeholders within the community are involved in the development of cybersecurity talent. This will ensure that there is a continuous flow of talent to reduce the skills gap and ensure a decrease in the pipeline deficiency in the long run.

## CONCLUSION

There are various issues that need to be considered before a successful cybersecurity education program can be realized. A school-wide, top-driven, multidisciplinary approach is best suited to planning and implementing a successful cybersecurity education program. It is also important during the planning process for a school to identify the KUs that would benefit industries in the school's region, along with the necessary resources to carry out a successful cybersecurity education program. There are other important factors, such as academia–industry and K–12 education partnerships. Academia–industry partnerships will open doors for career development initiatives such as internships, competitions, and conference sponsorships, as well as real-world learning experiences. K–12 partnerships will provide a steady inflow of identified secondary school talent into schools of higher learning.

Subsequently, it will be possible for institutions of higher learning to generate cybersecurity talent with the long-term goal of attaining a CAE designation. A multidisciplinary approach is required to develop a cybersecurity education plan that involves both technical and nontechnical disciplines. This strategy would benefit from a top-driven, university-wide cybersecurity awareness program. The long-term goal should be to attain a CAE designation.

## REFERENCES

- Center for Cyber Safety and Education and International Information System Security Certification Consortium (ISC)<sup>2</sup>. (2017). *Global Information Security Workforce Study (GISWS)*. Retrieved from <https://iamcybersafe.org/gisws/>.
- Coffey, J. W., Haveard, M., & Golding, G. (2018). A case study in the implementation of a human-centric higher education cybersecurity program. *Journal of Cybersecurity Education, Research and Practice*, 2018(1). Retrieved from <https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/4>
- Dupuis, M. J. (2017). Cyber security for everyone: An introductory course for non-technical majors. *Journal of Cybersecurity Education, Research and Practice*, 2017(1). Retrieved from <https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss1/3>
- Evans, K., & Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters*. A Report of the Center for Strategic & International Studies Commission on Cybersecurity for the 44th Presidency. Retrieved from <https://www.csis.org/analysis/human-capital-crisis-cybersecurity>
- International Information System Security Certification Consortium (ISC)<sup>2</sup>. (2017). *Global cybersecurity workforce shortage to reach 1.8 million as threats loom larger and stakes rise*

- higher*. Retrieved from <https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage>
- McGettrick, A. (2013). Toward curricular guidelines for cybersecurity: Report of a workshop on cybersecurity education and training. National Science Foundation. Association for Computing Machinery. Retrieved from Association for Computing Machinery at <http://www.acm.org/education>.
- National Center for Education Statistics (NCES). (n.d). *Fast fact: Educational institutions*. Retrieved from <https://nces.ed.gov/fastfacts/display.asp?id=84>
- National IA Education and Training programs (NIETP). (n.d). *CAE requirements and resources*. Retrieved from <https://www.iad.gov/NIETP/CAERRequirements.cfm>
- National IA Education and Training programs (NIETP). (n.d). *What's new? CAE naming convention*. Retrieved from <https://www.iad.gov/NIETP/index.cfm>
- National Science Foundation. (2014). *Cybersecurity education workshop*. Workshop Report, Directorates of Computer and Information Science and Engineering (CISE), and Education and Human Resources (HER). Arlington, VA. Retrieved from [https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW\\_FinalReport\\_040714.pdf](https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf)
- Ponemon Institute. (2014). *2014 best schools for cybersecurity: Study of educational institutions in the United States*. Traverse City: Ponemon Institute.
- Sherif, K., Pitre, R., and Kamara, M. (2016). Why do information system controls fail to prevent unethical behavior? *VINE Journal of Information and Knowledge Management Systems* 46(2), 251–266. Retrieved from <https://doi.org/10.1108/VJIKMS-04-2015-0028>
- Suby, M. (2013). *A view from the top: The (ISC)<sup>2</sup> global information security workforce study CXO report*. Mountain View, CA: Frost and Sullivan and International Information System Security Certification Consortium (ISC)<sup>2</sup>.
- Suby, M. (2013). *The 2013 (ISC)<sup>2</sup> global information security workforce study*. Mountain View, CA: Frost and Sullivan and International Information System Security Certification Consortium (ISC)<sup>2</sup>.
- Suby, M, & Dickson, F. (2015). *The 2015 (ISC)<sup>2</sup> global information security workforce study*. Mountain View, CA: Frost and Sullivan and International Information System Security Certification Consortium (ISC)<sup>2</sup>.
- Tsado, L. K. (2016). *Analysis of cybersecurity threats and vulnerabilities: Skills gap challenges and professional development*. (Doctoral dissertation). Texas Southern University, Houston, TX.
- Vireos, M. (2013). Cybersecurity education for the next generation: Emerging best practices. *Presented at the 2013 NIST/NICE Workshop Gaithersburg, Maryland*. Retrieved from [https://www.nist.gov/sites/default/files/documents/2017/01/19/d1\\_trk3\\_viveros\\_cybersecurity\\_education\\_next\\_generation.pdf](https://www.nist.gov/sites/default/files/documents/2017/01/19/d1_trk3_viveros_cybersecurity_education_next_generation.pdf).

## **Appendix 1: Example of Checklist – Four Year College Application for Cyber Defense:**

### **NSA/DHS National Centers of Academic Excellence in Cyber Defense Applicant Checklist CAE-CDE Designation**

The CAE-CDE Program is open to current regionally accredited four-year colleges and graduate-level universities. All institutions must hold current regional accreditation as outlined by the Department of Education (<http://ope.ed.gov/accreditation>).

- Applicants must identify a specific curriculum path and demonstrate that individual students will receive a minor, degree, concentration or other recognized program completion. Curriculum in this path must map to the seventeen core Knowledge Units plus five optional required for the CAE-CDE designation.
- Applicants must demonstrate compliance with program criteria, including demonstration of program outreach and collaboration, center for CD education, a robust and active CD academic program, CD multidisciplinary efforts, practice of CD at the institution level, and student and faculty CD efforts.

Qualifying applicants will be designated as CAE-CDE for a period of five academic years, after which they must successfully re-apply in order to retain the designation. Designation as a CAE-CDE does not carry a commitment of funding from NSA or DHS. CAE institutions with designations that will expire in 2018 must submit no later than 15 January 2018 and are not required to submit this checklist.

- ☐☐☐ Applicants that already have a CAE application account and have been actively gathering information may continue with their submission and submit by 15 January 2018 for possible designation in June or by 15 April 2018 for possible designation at the NICE Annual Conference in November 2018.
- ☐☐☐ Applicants that are new to the CAE process or those who wish to receive assistance should complete an Applicant Checklist to ascertain readiness to apply. Applicants have the opportunity to receive mentorship. Application Assistance with a mentor is being offered as a benefit to the institution and is designed to help applicants understand the depth of program and designation requirements.
- ☐☐☐ Applicants that opt to receive support will have their checklists reviewed and will be referred to one of two assistance paths:
  - Program Development: Institutions needing further development of programs and/or curriculum, or those with programs that have not reached maturity, will be referred to a CAE Regional Resource Center for assistance. In this phase, the applicant will have access to workshops, seminars and an advisor to help in their preparation for designation. Schools in this phase will also be invited to programs and events hosted by the CAE Community ([www.caecommunity.org](http://www.caecommunity.org)) and have access to other resources offered by the Program Office only for the CAE audience.
  - Application Assistance: Institutions assessed to be within 12 – 18 months of meeting curriculum and programmatic criteria will be referred to the Application Assistance path for mentorship. The CAE Program Office requires the endorsement of the mentor to process applicants that have chosen this path.



Submissions must be received no later than 15 April 2018 or a subsequent designation cycle.

- ☐☐☐ Applicants that choose to opt out of Application Assistance must acknowledge the last page of this New Applicant Checklist.

Yes, I opt to receive support via the CAE Application Assistance Program Please complete the checklist and follow submission instructions. (If opt in, then applicant will complete Application checklist and not the “Application Assistance Opt Out” section on the last page)

No, I opt out of the CAE Application Assistance Program (checklist is not required, please proceed to last page) (if opt out, then applicant will only complete the “Application Assistance Opt Out” section on the last page)

Contact the Program Office at [askcaeiae@nsa.gov](mailto:askcaeiae@nsa.gov) for further information

NSA/DHS National Centers of Academic Excellence in Cyber Defense Applicant Checklist  
**CAE-CDE Designation**

\*Institution Name: (Fillable character field)

POC Name: \*First: (Fillable character field) \*Last: (Fillable character field)

\*POC Phone: (Fillable character field) Alt. Phone (Fillable character field)

\*POC Email (must be .edu): (Fillable character field)

\*POC Mailing Address: Street: (Fillable character field) State: (2 character drop down)

\*Title: (drop down?)

Zip: (Fillable character field)

\*Curriculum Path (dropdown: certificate, minor, concentration, degree, other) Please describe other (fillable character

field) Name: (Fillable character field)

\*Department that houses the Path: (Fillable character field)

Dean or Above Name: \*First (Fillable character field) \*Last: (Fillable character field) \*Title: (drop down?) \*Phone: (Fillable character field)

1. \*Regional Accreditation - required for designation: (drop down list of accrediting bodies) – if regionally accredited not selected, then message saying “not eligible for CAE-CD submission” and rest of application is not available to complete

2. Provide the course number, name and a short description of the courses in your identified curriculum path that you believe map to the CAE CDE Core KUs plus 5 Optional KUs.  
 EXAMPLE: Course #: ITS222 Course name: Enterprise Security.  
 Course Description: The Enterprise Security Seminar is designed so that you understand the critical components of network security. The course covers physical security and devices as well as software and organizational components. This course covers the material recommended as preparation for the ComTIA Security + certification examination. Exercises and assignments are geared toward practical skills needed as a Network Manager.

Multiple Courses containing the following fields:

☐ ☐ \*Course#: (Fillable character field)

☐ ☐ \*Course name: (Fillable character field)

☐ ☐ \*Course Description: (Fillable character field)

3. Please indicate 'Yes or Done', 'No or None', or 'Unknown/Unsure' to the questions below and submit the checklist; you will be contacted with information on how to continue.

*\*Denotes required field*

**NSA/DHS National Centers of Academic Excellence in Cyber Defense Applicant Checklist  
 CAE-CDE Designation**

Criteria Name	Criteria Description	Yes or Done	No or None	Unknown or Unsure
0. Letter of intent	Please acknowledge this requirement. Once assigned to the application assistance path, applicants will need to obtain a letter containing POC information, institutional support, regional accreditation information, cyber center support and accomplishments in the field of Cyber Defense.			
1. Cyber Defense Curriculum Path	Is there a Curriculum path that meet the all of the mandatory Knowledge Units (KUs) plus 5 Optional KUs?			
	Has the stated curriculum path been in existence for at least 3 years and have 1 year of students that have completed the curriculum path with recognition of completion?			
	Are there at least 1 year of students that have graduated with the curriculum path included in their degree program?			
2. Student Scholarly Skill Development	Do courses in the curriculum path require students to write papers or complete projects or presentations?			
	Do courses in the curriculum path require lab			

	assignments for hands-on learning?			
	Do students participate in cybersecurity competitions?			
	Are students provided with access to cybersecurity practitioners such as guest lecturers working industry or government, internships, etc?			
3. "Center" for Cyber Education	Does the institution have an officially established entity (either physical or virtual) serving as the focal point for its Cyber educational program? The center shall provide the following services: program guidance and oversight; general cyber defense information; and collaboration and outreach opportunities among students, faculty, and other institutions. Additionally, the center must be supported by a website that is dynamic, current and visible within the institution and the external community at large.			
	Not required but beneficial - Does the department that houses the Cyber "Center" have an external board of advisors, local industry professionals, to provide programmatic guidance over the activities of the center and the program as a whole?			
4. Program Faculty	Is there adequate faculty available to teach Cyber related courses in the curriculum path at the institution?			
	Is there someone with overall responsibility for the program?			
	Are Cyber faculty contributing to the field of Cybersecurity? Do they publish, present at conferences, write books and/or make major contributions to professional societies?			
	Are faculty supporting Cyber Student activities? Clubs, Competitions, etc.?			
5. Cybersecurity Practice is Multidisciplinary	Are non-technical/non-CD students introduced to CD through modules in existing non-CD courses, such as information security included in business, health courses incorporating HIPAA regulations, etc?			

NSA/DHS National Centers of Academic Excellence in Cyber Defense Applicant Checklist  
**CAE-CDE Designation**

	Are papers or projects or test questions required that demonstrate knowledge of security concepts or awareness in non-CD courses ?			
6. Institution IS Security	Is there an Information System Security Plan in place? A plan must provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. NOTE: For the final application, evidence of such a plan must be			

	provided.
	Does the institution have an ISSO to oversee Security throughout?
	Does the institution have in place a means to encourage cybersecurity awareness throughout the campus?
	Does the institution share cyber related curriculum or faculty beyond the boundaries of the institution, such as materials provided to high schools or technical schools, or faculty serving on another institution's development committee?
7. Outreach/Collaboration	Does the institution have transfer of credit agreements from other academic institutions offering a cyber-concentration, area of study or track?
	Does the institution sponsor cybersecurity-related community events such as cybersecurity education workshops, homeland security events, first responder workshops, computer diagnostic check-ups, etc?
	Does the institution collaborate with other CAE schools on research projects, grants, etc? Business/Industry?

Reviewer Name: \*First: (Fillable character field) \*Last: (Fillable character field)

Reviewer Notes: (Fillable character field with date of note associated with it – allow for multiple notes on multiple dates?)

#### NSA/DHS National Centers of Academic Excellence in Cyber Defense Applicant Checklist **CAE-CDE Designation**

##### Application Assistance Opt Out

I, name of POC (fillable field), from name of institution (fillable field), acknowledge that I have been given the opportunity to receive application assistance and work with a mentor to complete my application for possible designation as a NSA/DHS National Center of Academic Excellence in Cyber Defense Education. I understand that this process is an opportunity to receive program development and application assistance prior to submitting an application. I acknowledge that if my application does not meet requirements, the assistance of a mentor is a requirement to submit an application in a future cycle. If at any time I require Application Assistance I may complete the new applicant checklist and request assistance with the understanding that it may move my submission to a subsequent cycle.

By “Submitting agree to the above term” with associated date of submission  
Head of the Department that houses the Curriculum path email address: (Fillable character field)  
After form is complete and applicant presses “submit” - form will be sent to:  
[askCAEIAE@nsa.gov](mailto:askCAEIAE@nsa.gov)

