Institutions of higher education, in particular CAE schools, have an enormous responsibility to produce cybersecurity experts that can meet the demands of industry and government in solving perhaps the biggest national security concern we face in protecting our critical infrastructure, networks, communications, and intellectual property. Yet today, the workforce demands are many times not being met, and the delta among qualified applicants and open jobs is growing at a rapid pace. In addition, we believe that cybersecurity should not just be taught to computer engineering/science students, but in some capacity it should be taught to all students, as it most certainly impacts every one of us. Part of the communication problem that exists in government and industry today is that cybersecurity professionals "talk-past" non-cyber experts, leading to frustration, anger, and often, poor decision making.

Further, most institutions of higher learning with a cyber program generally focus on technology. They are not teaching to the intangibles of ethics, communication and leadership that liberal arts colleges; most importantly and in particular, faith-based liberal arts colleges such as Montreat College, are in a position to take a leadership role in. Simply requiring a class in cyber ethics is insufficient. We believe ethics should be woven into the curriculum at every level from kindergarten through masters. As faith based institutions stand alone with the service academies as the last remaining institutions that overtly teach to character, we believe we can and should do better.

Montreat College believes a good start for the future of cybersecurity curriculum development in the US follows these three pillars:

1. Rebalance the focus of the curriculums to put significant attention on ethics and character so that we are not "weaponizing" students with technical skills without any ethical framework for the utilization of their skillsets.

2. Create an interdisciplinary framework that teaches cybersecurity students how to communicate, write and present their ideas, challenges and needs, as well as teaches non-cybersecurity students cyber hygiene and basic fundamentals of cybersecurity to avoid communications impasses in their careers.

3. Develop CAE communities, not just schools of higher learning. Incentivize additional collaboration from kindergarten through masters by bringing together industry, academia and government. These communities of cyber excellence can pilot ideas, align STEM and other curricula with the needs of end-users, and provide government with critical solutions to national security problems in cybersecurity.

We believe, at its core, cybersecurity is principally a human problem, not just a technical one. Despite the best technology in the world, if organizations don't have trustworthy, ethical leaders, who can communicate in this space, the mission may not succeed. Developing ethical leaders who can communicate has been at the center of our Cybersecurity bachelor's degree at Montreat College and should be included in the national curriculum standards to directly address the trust and communication problems in cybersecurity.

- ***Trust problem***: Security professionals, even those designated as "certified ethical hackers" do not have the confidence of many in the business community. Business executives are hesitant to

"open the data door" to anyone they understand to be a "hacker." Even Chief Information Officers (CIOs) have significant challenges with trusting those charged with cyber defense. According to a recent national survey of Chief Information Officers, trust of ethics and character rank first among the attributes they seek in their employees.

- *Higher education must work to develop curriculums that highlight the importance of strong moral and ethical decision making in order to alter the stigma against hacking*
- *Curriculums should focus just as much on unintended and/or larger consequences of actions taken on a network as they do the technical realities to make those actions possible*

- ***Communication problem***: The two very distinct worlds of business leadership and information technology often create conflict and a tremendous gap of understanding that is rooted in the poor ability to communicate to each other. IT people often don't understand the big picture of an institution and business leadership seldom understands the technical details of their network and data security.
  - *Higher education must develop a foundational approach to operational cyber planning to better align IT staff with larger corporate visions*
  - *There must be a strong focus in building bridges across the corporate communications chasms between senior management and IT departments*
- ***Education problem:*** Current K-12 preparation to enter college and/or certificate programs for careers in cyber and its related disciplines is lacking. In addition, cyber education today is focused only on a technical curriculum. There is no educational framework for understanding character and ethics as central to addressing this problem. Universities do not teach students the notion that it is not enough to know what ***can*** be done; cyber leaders and operators must also be taught what ***should*** and ***should not*** be done.
  - *More work must be done at the k-12 level, working in conjunction with higher education, to give students practical and applied learning before college so that students can enter freshman year needing less rudimentary skills development.*
  - *Higher education must teach its students to think about their actions from an ethical and moral perspective as well as a technical*

Montreat College is of the opinion that higher education is not doing enough to address these issues and for that reason, we propose a new category of cyber sub-specialties; that of cybersecurity leadership. This category would develop the curriculum for the future - intermediaries between the technical and non-technical worlds. This would in some ways revise the CISO/CTO/CIO type of leader with skills to more effectively communicate as senior management in the following ways:

- Leaders responsible for developing the blueprints for future success with their technical teams can communicate that blueprint to non-technical audiences seamlessly.
- Manage the cyber teams from a secular but ethically driven mindset to insure the highest caliber of employees and performance.

Liberal arts colleges and universities, and in particular, faith-based liberal arts colleges are poised to affect change in developing cybersecurity leaders by reshaping cyber education. We urge the federal government to engage more with these types of institutions for fresh ideas that big, state universities have few answers for. It would be a very worthwhile endeavor, we believe, to explore how faith-based institutions' approaches to overtly teaching to character can be translated into a secular curriculum for all schools.

It may, on the surface, seem strange to combine classical character development lessons with 21st Century technical skillsets in order to create the cyber leaders of the future. The works of Plato, Kant, Aristotle, etc. are not what most people would view as part of a solid cybersecurity curriculum. However, we believe this type of learning still holds tremendous value for this environment. Ethics, leadership, and communication must be pillars of any good cybersecurity curriculum. This is due, in part, to the risk of insider threats, the current poor coordination between cybersecurity practitioners and organizational/governmental leaders, and the ever-increasing danger of cyber skills. While typically it is high-profile hacks and malware strikes that gain media attention, most data breaches are the result of insider threats, both malicious and unintentional. IBM's 2016 Cyber Security Intelligence Index found that 60% of all attacks in 2015 came from insiders, a 5% increase from 2014. And many of the most notorious breaches within the government came from insiders. These attacks can often be traced to poor ethics and negligence by employees and must be addressed.

By introducing ethics into cybersecurity education, we believe students, for the first time, will be able to demonstrate their trustworthiness to employers, along with their technical skills. And curriculum development involving professionals from industry, academia, and government ensures that issues will be approached from technical and non-technical perspectives alike. And lastly, we believe that the development of a "Cyber Hippocratic Oath" and an exploration of Just War Theory in the context of cyber is vital. Cyber is an asymmetric threat of astonishing potential, and reinforces the need to ensure character and ethics are at the heart of our educational curriculum in these areas. Just as we are careful in who has access to the nuclear codes, we similarly do not want hundreds of thousands of skilled cyber warriors with no clear foundation of ethics, character, communication, and leadership developed in their educational pathways.

Since faith-based institutions of higher education now stand alongside the U.S. military academies as the only institutions of higher learning that overtly teach to character, we believe we have an opportunity to play an important role in the solution to the cybersecurity crisis. Montreat College has chosen to rise to this challenge. We welcome any and all feedback on our proposed thoughts about the cyber curriculum requirements of the future. Thank you in advance for your consideration of our comments and for your work to help secure our nation in this emerging, dangerous landscape.