Chair: Tracy Christofero

GC#3: Intent to Plan

Graduate Intent to Plan--Major or Degree

NOTE: This "Intent to Plan" form must be submitted and go through the approval process BEFORE you submit the form titled, "Request for Graduate Addition, Deletion or Change of a Major or Degree." For detailed information on new programs please see: http://wvhepcdoc.wvnet.edu/resources/133-11.pdf.

1. Prepare one paper copy with all signatures and supporting material and forward to the Graduate Council Chair.
2. E-mail one PDF copy without signatures to the Graduate Council Chair. If attachments are included, please merge into a single file.
3. ***The Graduate Council cannot process this application until it has received both the PDF copy and the signed hard copy.***

College: CITE

Dept/Division: Computer Science

Contact Person: Wook-Sung Yoo

Phone: x5452

New Degree Program Cybersecurity

Effective Term/Year Fall 20 18 Spring 20 □ Summer 20 □

Information on the following pages must be completed before signatures are obtained.

Signatures: if disapproved at any level, do not sign. Return to previous signer with recommendation attached.

Dept. Chair/Division Head	Date March 26, '18
College Curriculum Chair	Date 3/29/18
College Dean	Date 03/29/18
Graduate Council Chair	Date
Provost/VP Academic Affairs	Date
Presidential Approval	Date
Board of Governors Approval	Date

Graduate Intent to Plan--Major or Degree-Page 2

Please provide a rationale for new degree program: (May attach separate page if needed)

After the security breach associated with more than one billion Yahoo user accounts in 2013, another 500 million Yahoo user accounts were stolen in 2016. Then, Yahoo, the giant web services provider, was hacked again in 2017. We have seen a huge increase in cyber-related incidents, including big data breaches, physical infrastructure tampering, ransomware, among others. As cybersecurity continues to be a primary challenge, the market and need of cyberseurity professionals are growing at an astonishing rate. Forbes reported that the burgeoning cybersecurity market is expected to grow from $75 billion in 2015 to $170 billion by 2020. A report from Cisco puts the global figure at one million cybersecurity job openings. According to the Bureau of Labor Statistics, there are currently more than 200,000 unfilled cybersecurity positions in US alone and the rate of growth for jobs is projected at 37 percent from 2012–2022, much faster than the average (7 percent) for all other occupations. At this rate, the United States is on pace to hit a half-million or more unfilled cybersecurity positions by 2021. It is clear that there is a strong need and job market for cybersecurity professions, locally, nationally and internationally and the proposed M.S in Cybersecurity degree program is very timely. The M.S. in Cybersecurity degree program will adequately produce graduates who will fill the workforce needs in this rapidly-growing field. The proposed program is a viable low-cost program that will significantly result in increasing the enrollment and producing more tuition and program/lab fees. Along with the B.S. in Computer and Information Security program proposed recently by the Weisberg Division of Computer Science, the proposed program will educate students to better understand, prevent, mitigate and respond to cybersecurity threats. The M.S. in Cybersecurity program will also strengthen existing programs at Marshall University. Closely-related programs will greatly benefit from the addition of the M.S. in Cybersecurity degree program as this new program will create exciting and productive new paths for education and research for students in existing Marshall University undergraduate and graduate degree and certificate programs in Computer Science, Information System, Technology Management, Electrical and Computer Engineering, Management Information Systems, Criminal Justice, and Digital Forensics.

1. ADDITIONAL RESOURCE REQUIREMENTS: If your new program requires additional faculty, equipment or specialized materials, attach an estimate of the time and money required to secure these items.
NOTE: Approval of this form does not imply approval for additional resources. Enter NONE if not applicable.

2. NON-DUPLICATION: If a question of possible duplication occurs, attach a copy of the correspondence sent to the appropriate department(s) describing the request and any response received from them. Enter NONE if not applicable.

None

For catalog changes as a result of the above actions, please fill in the following pages.

Graduate Intent to Plan--Major or Degree-Page 3

5. ***New* Catalog Description**
Insert a 'clean' copy of your proposed description, i.e., no strikethroughs or highlighting included. This should be what you are proposing for the new description. (May attach separate page if needed)

See attachment

Graduate Intent to Plan--Major or Degree-Page 4

Please insert in the text box below your summary information for the Graduate Council agenda. Please enter the information exactly in this way (including headings):

Department:
New Major or Degree:
Credit Hours:
Rationale:

Department: Weisberg Division of Computer Science
New Major or Degree: Masters of Science in Cybersecurity
Credit Hours: 30 Credit Hours
Type of Change: Addition
After the security breach associated with more than one billion Yahoo user accounts in 2013, another 500 million Yahoo user accounts were stolen in 2016. Then, Yahoo, the giant web services provider, was hacked again in 2017. We have seen a huge increase in cyber-related incidents, including big data breaches, physical infrastructure tampering, ransomware, among others. As cybersecurity continues to be a primary challenge, the market and need of cyberseurity professionals are growing at an astonishing rate. Forbes reported that the burgeoning cybersecurity market is expected to grow from $75 billion in 2015 to $170 billion by 2020. A report from Cisco puts the global figure at one million cybersecurity job openings. According to the Bureau of Labor Statistics, there are currently more than 200,000 unfilled cybersecurity positions in US alone and the rate of growth for jobs is projected at 37 percent from 2012–2022, much faster than the average (7 percent) for all other occupations. At this rate, the United States is on pace to hit a half-million or more unfilled cybersecurity positions by 2021. It is clear that there is a strong need and job market for cybersecurity professions, locally, nationally and internationally and the proposed M.S in Cybersecurity degree program is very timely. The M.S. in Cybersecurity degree program will adequately produce graduates who will fill the workforce needs in this rapidly-growing field. The proposed program is a viable low-cost program that will significantly result in increasing the enrollment and producing more tuition and program/lab fees. Along with the B.S. in Computer and Information Security program proposed recently by the Weisberg Division of Computer Science, the proposed program will educate students to better understand, prevent, mitigate and respond to cybersecurity threats. The M.S. in Cybersecurity program will also strengthen existing programs at Marshall University. Closely-related programs will greatly benefit from the addition of the M.S. in Cybersecurity degree program as this new program will create exciting and productive new paths for education and research for students in existing Marshall University undergraduate and graduate degree and certificate programs in Computer Science, Information System, Technology Management, Digital Forensics and Information Assurance, Electrical and Computer Engineering, Management Information Systems, and Criminal Justice .

CYBERSECURITY, M.S.

The Master of Science in Cybersecurity program provides students with the knowledge, skills, and professional practices needed for careers in the cybersecurity fields. The program also prepares students who desire to pursue further graduate work that leads to a Ph.D. degree. The curriculum covers several advanced topics in cybersecurity, such as; advanced cryptography, cybersecurity policy, cyber risk and vulnerability, cyber operation, wireless network security, web/mobile security, software security, security in Internet of Things (IoT), etc. These courses will be taught using the very latest, state-of-the-art security tools and technologies.

Admission and Transfer Criteria

Applicants should follow the admissions process as stated in the graduate catalog or the graduate admissions web site. Minimum requirements for admission is a four-year Bachelor's degree with GPA of 2.75 or higher out of 4.0 in Cybersecurity or any computer science related areas.

Whether a student meets the above requirements will be determined by the division chair or designee, based on the information provided in the admission application and transcripts. Applicants with a four-year bachelor degree in a major other than Cybersecurity or any computer science related area may be admitted to the program with a condition of successful completion of the following three bridge courses with a grade B or above in first two semesters of the program:

- Data Structure and Algorithms (CS 210)
- Internetworking (CS 320)
- Statistics (STA 225, STA 346, or STA 345)

Foreign nationals must score in the IELTS Band 6.5 on the TOEFL, and must have met all other admission criteria prior to registering for the first semester of courses.

M.S. Degree Requirements

The MS degree requires 30 credit hours (CR) of graduate work. At least 15 credit hours should be taken from 600 level courses.

- Core Required (12 CR):

CYBR 510	Introduction to Cybersecurity (**New**)
CYBR 530	Cybersecurity Policies and Management (**New**)
CYBR 615	Cyber Risk and Vulnerability (**New**)
CYBR 620	Cyberwarfare (**New**)

- Concentration (6 CR)

  Student must choose two courses from ONE concentration area below:

Network Security

CYBR 535	Cyber Risk (cross-listed with CYBR 435)
CYBR 542	Cyber Operations (cross-listed with CYBR 442)
CYBR 625	Applied Cryptography (**New**)

Application Security

CYBR 500	Computer Security Design (cross-listed with CYBR 400)
CYBR 535	Cyber Risk (cross-listed with CYBR 435)
CYBR 625	Applied Cryptography (listed above)

Security Management

CYBR 500	Computer Security Design (cross-listed with CYBR 400)
CYBR 542	Cyber Operations (cross-listed with CS 442)
IS 631	Information Security
IS 646	Computer Systems Security
IS 647	IT Disaster Planning & Recovery
IS 656	Communication and Network Technologies

- Thesis option or Core Electives Option (6 CR)
  The Thesis option offers a student an opportunity for serious investigation into an area of interest by completing a 3 credit research course (CYBR 680) and a 3 credit thesis (CYBR 681) course. Students must summarize their thesis work in the form of a formal written document and deliver an oral presentation. Thesis work is typically conducted over two semesters. A thesis option can be taken after the completion of 12 credit hours. The 6 CR of the thesis option courses cannot be combined in a semester.
  For the Core Electives Option, student may choose any two 600 level CYBR courses.

- Free electives (6 CR)
  Students may choose any two from following CYBR/CS/IS/ courses.

CYBR 500	Computer Security Design (cross-listed with CYBR 400)
CYBR 535	Cyber Risk (cross-listed with CYBR 435)
CYBR 542	Cyber Operations (cross-listed with CYBR 442)
CYBR 625	Applied Cryptography (listed above)
CYBR 682-84	Special Topics in Cybersecurity
CYBR 685-89	Independent Study
CYBR 698	Internship

CS 504	High Performance Computing
CS 542	Communication Networks and Distributed Systems
CS 579	Software Engineering
CS 620	Applied Algorithms.
CS 625	AI Principles and Methods.
CS 630	Machine Learning.
CS 660	Big Data Systems.

IS 624	Data Warehousing.
IS 625	Software Engineering
IS 692	Image Processing for Forensics
IS 631	Information Security
IS 646	Computer Systems Security
IS 647	IT Disaster Planning & Recovery
IS 656	Communication and Network Technologies

MARSHALL

COMPUTER SCIENCE

MARSHALL UNIVERSITY

College of Information Technology and Engineering
Weisberg Division of Computer Science

March 31, 2018

Master of Science in Cybersecurity

Effective Date: Spring 2019

By: Wael Zatar, Dean
College of Information Technology and Engineering

and

Wook-Sung Yoo, Ph.D.
Chair, Weisberg Division of Computer Science

Summary Statement

The Weisberg Division of Computer Science in the College of Information Technology and Engineering (CITE) proposes the establishment of the Master of Science (M.S.) in Cybersecurity degree program at Marshall University.

Cybersecurity is a computing-based discipline in which technology, computer science, people, and multiple processes are aligned to assure the continued operations of computer systems in the presence of risks and adversaries in cyber space. Two existing programs offered by CITE, M.S. in Computer Science and M.S. in Information Systems, cover various cybersecurity-related courses on an annual basis. The M.S. in Cybersecurity program, however, will focus on educating and training students to better understand, prevent, mitigate, and respond to cybersecurity threats. The program will raise awareness and garner interest in closely-related programs at Marshall University. Graduates of the program will contribute to West Virginia's economic development and advance its competitiveness regionally, nationally and globally.

Faculty members in the Weisberg Division of Computer Science have demonstrated expertise in the area of cybersecurity. In their Ph.D. dissertations, the Weisberg Division of Computer Science faculty have addressed cybersecurity challenges including computers security, network security, mobile and wireless networking, Internet of Things (IoT), and cloud computing.

The proposed program does not anticipate the need for additional faculty lines, major funding, or other resources to establish the program. The College of Information Technology and Engineering plans on leveraging available resources in the Weisberg Division of Computer Science to offer this timely program. The cybersecurity degree program will not only create exciting and productive new pathways for research and development, but will increase educational opportunities and inter-departmental collaborations across the campus.

The program will become viable from its first year and will grow each year. The College of Information Technology and Engineering aims at enrolling 70 students and graduating 28 students with a M.S. in Cybersecurity degree in the fifth year of the program. The projected net revenue in the fifth year is estimated at $657,315. The program will generate close to $2 million in new revenues during its first five years.

1. Program Description

Cybersecurity is an evolving discipline that encompasses several elements: the study of strategy, policy, and standards regarding the security of and operations in cyber space, the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities as they relate to the security and stability of the global information and communications infrastructure.

The proposed M.S. in Cybersecurity degree program offers Cybersecurity education with existing related graduate programs offered by the College of Information Technology and Engineering (M.S. in Computer Science, M.S. in Information Systems, and M.S. in Technology Management). The M.S. in Cybersecurity degree program prepares graduates to succeed in professional careers in a very rapidly growing Cybersecurity fields. The graduates will lead much-needed technological changes in the industry and research fields. The following sections provide additional details about the proposed M.S. in Cybersecurity degree program.

1.1 Program Mission

Marshall University provides innovative undergraduate and graduate education programs that contribute to the development of the individual and their role in society. An important goal of the M.S. in Cybersecurity degree program is to equip students with a strong foundation in the theory and practice of cybersecurity. This foundation builds on Marshall's mission, where it is stated "to actively facilitate learning through the preservation, discovery, synthesis, and dissemination of knowledge". The proposed program will cover the fundamental concepts of cybersecurity and provide opportunities to apply the technical knowledge and skills to produce viable solutions for protecting and defending cyber space. Graduates from the M.S. in Cybersecurity degree program will achieve competency in the following four Program Educational Objectives (PEO):

After graduation, students will be able to:

PEO 1*: be employed in Cybersecurity or related technical areas*

PEO 2*: be engaged in life-long learning and professional development through self-study, continuing education or graduate and professional studies*

PEO 3*: become effective communicators, collaborators and innovators*

PEO 4*: practice professional ethics with social responsibility addressing social, technical and business challenges*

The M.S. in Cybersecurity program will strive to ensure that its graduates are placed in cybersecurity jobs or closely related fields within the professional practice. The graduates are trained to contribute to the evolving technology at their work place, identify opportunities for breakthrough research, and assume reasonable responsibilities in the decision-making process. The M.S. in Cybersecurity degree program aligns well with the mission of the College of Information Technology and Engineering (CITE):

- CITE will be a recognized leader in practice-oriented teaching and applied research.
- CITE is committed to serve the lifelong educational needs of students, new graduates, working professionals, and employees.
- CITE builds on combined traditions of student-focused education, entrepreneurship, and funded research and service emphasis.
- CITE provides education when and where needed, incorporating technology-enhanced methods, by full-time, dedicated faculty complemented by expert adjunct faculty from industry and government.

1.2 Program Features

The M.S. in Cybersecurity degree program will make Marshall University a recognized leader in education, research and practice in cybersecurity fields. The program will attract traditional and non-traditional students from West Virginia, the Tri-State Region and the surrounding states. The M.S. in Cybersecurity degree program will promote collaboration with industries, government agencies, and educational institutions by:

- developing partnerships and alliances with external corporate and industry organizations for pursuing joint educational and research opportunities in cybersecurity
- pursuing research and grant opportunities in cybersecurity related areas
- coordinating availability of cybersecurity coursework to assist not only West Virginia, but the rest of the nation to meet the demand for cybersecurity professionals
- providing outreach opportunities to interested parties and organizations

The catalog description of the proposed M.S. in Cybersecurity degree program is shown in the following two pages.

CYBERSECURITY, M.S.

The Master of Science in Cybersecurity program provides students with the knowledge, skills, and professional practices needed for careers in the cybersecurity fields. The program prepares students who desire to pursue further graduate work that leads to a Ph.D. degree. The curriculum covers several advanced topics in cybersecurity, such as; advanced cryptography, cybersecurity policy, cyber risk and vulnerability, cyber operation, wireless network security, web/mobile security, software security, security in Internet of Things (IoT), etc. These courses will be taught using latest and state-of-the-art security tools and technologies.

Admission and Transfer Criteria

Applicants should follow the admissions process stated in the graduate catalog or the graduate admissions web site. Minimum requirements for admission is a four-year Bachelor's degree with GPA of 2.75 or higher out of 4.0 in Cybersecurity or computer science related programs.
Whether a student meets the above requirements will be determined by the Chair or designee of the Weisberg Division of Computer Science, based on the information provided in the admission application and transcripts. Applicants with a four-year bachelor degree in a major other than cybersecurity or computer science related program may be admitted to the program with a condition of successful completion of the following three bridge courses with a grade B or above in the first two semesters of the program:

- Data Structure and Algorithms (CS 210)
- Internetworking (CS 320)
- Statistics (STA 225, STA 346, or STA 345)

Foreign nationals must score in the IELTS B and 6.5 on the TOEFL, and must have met all other admission criteria prior to registering for the first semester of courses.

M.S. Degree Requirements

The MS degree requires 30 credit hours (CR) of graduate work. At least 15 credit hours should be taken from 600 level courses.

- Core Required (12 CR):

CYBR 510	Introduction to Cybersecurity (**New Course**)
CYBR 530	Cybersecurity Policies and Management (**New Course**)
CYBR 615	Cyber Risk and Vulnerability (**New Course**)
CYBR 620	Cyberwarfare (**New Course**)

- Concentration (6 CR)
  Student must choose two courses from ONE concentration area below:

Network Security

CYBR 535	Cyber Risk (cross-listed with CYBR 435)
CYBR 542	Cyber Operations (cross-listed with CYBR 442)
CYBR 625	Applied Cryptography (**New Course**)

Application Security

CYBR 500	Computer Security Design (cross-listed with CYBR 400)
CYBR 535	Cyber Risk (cross-listed with CYBR 435)

CYBR 625	Applied Cryptography (Also listed in the Network Security Concentration)

Security Management

CYBR 500	Computer Security Design (cross-listed with CYBR 400)
CYBR 542	Cyber Operations (cross-listed with CS 442)
IS 631	Information Security
IS 646	Computer Systems Security
IS 647	IT Disaster Planning & Recovery
IS 656	Communication and Network Technologies

- Thesis option or Core Electives Option (6 CR*)*

  The Thesis option offers a student an opportunity for serious investigation into an area of interest by completing a 3 credit research course (CYBR 680) and a 3 credit thesis (CYBR 681) course. Students must summarize their thesis work in the form of a formal written document and deliver an oral presentation. Thesis work is typically conducted over two semesters. A thesis option can be taken after the completion of 12 credit hours. The 6 CR of the thesis option courses cannot be combined in a semester.

  For the Core Electives Option, student may choose any two 600 level CYBR courses.

- Free electives (6 CR)

  Students may choose any two from following CYBR/CS/IS courses.

CYBR 500	Computer Security Design (cross-listed with CYBR 400)
CYBR 535	Cyber Risk (cross-listed with CYBR 435)
CYBR 542	Cyber Operations (cross-listed with CYBR 442)
CYBR 625	Applied Cryptography (Also listed in the Network Security Concentration)
CYBR 682-84	Special Topics in Cybersecurity
CYBR 685-89	Independent Study
CYBR 698	Internship

CS 504	High Performance Computing
CS 542	Communication Networks and Distributed Systems
CS 579	Software Engineering
CS 620	Applied Algorithms.
CS 625	AI Principles and Methods.
CS 630	Machine Learning.
CS 660	Big Data Systems.

IS 624	Data Warehousing.
IS 625	Software Engineering
IS 692	Image Processing for Forensics
IS 631	Information Security
IS 646	Computer Systems Security
IS 647	IT Disaster Planning & Recovery
IS 656	Communication and Network Technologies

The Weisberg Division of Computer Science plans on offering the five new courses (four core and one concentration courses) in the curriculum of the M.S. in Cybersecurity once a year:

CYBR 510	Introduction to Cybersecurity
CYBR 530	Cybersecurity Policies and Management
CYBR 615	Cyber Risk and Vulnerability (pre-requisite: CYBR 510)
CYBR 620	Cyberwarfare (pre-requisite: CYBR 615)
CYBR 625	Applied Cryptography (pre-requisite: CYBR 510)

Appendix A includes brief description of five new cyber security courses.

Other courses, shown in the following list, could be added should there be a demonstrated growth of the program and an ability to teach them following a cost-effective mechanism.

CYBR 630	Network Security
CYBR 635	Secure Software Engineering
CYBR 640	Security in Internet of Things
CYBR 650	Cybersecurity Data Analytics
CYBR 655	Cloud Security

1.3 Program Delivery

The delivery of the M.S. in Cybersecurity program will be following classical instructional mechanisms. The Cybersecurity lab, housed in the Arthur Weisberg Family Applied Engineering Complex, provides a first class hands-on experience to students in the M.S. Cybersecurity degree program. Effective utilization of the Cybersecurity lab, will enable designing, implementing, and administering the security of computer systems by embracing the concepts learned.

2. Program Needs and Justification

2.1 Existing Programs

2.1.1 M.S. in Cybersecurity Degree Programs in West Virginia

The M.S. in Cybersecurity program is not currently offered by any public university in West Virginia. In order to provide a broad overview of the information assurance and biometrics fields, West Virginia University currently offers Graduate Certificate programs in: (1) Computer Forensics, and (2) Information Assurance and Biometrics (Table 1).

Table 1: Cybersecurity or Related Graduate Programs in West Virginia

Institution	Degree	Public College	Distance from MU	CAE/CD	ABET Accredited
West Virginia University	Graduate Certificate in - Computer Forensics - Information Assurance and Biometrics	Yes	207 miles	Yes	No

However, West Virginia University has recently approved new B.S. and M.S. degree programs in cybersecurity.

2.1.2 B.S. in Cybersecurity Degree Programs in West Virginia

Three B.S. in Cybersecurity degree programs are offered by private institutions and colleges in West Virginia (Table 5). For example, Salem International University, a small, for-profit college, is about 157 miles away from Marshall University, and offers a *Bachelor of Science in Information Technology - Cyber Security*. The University of Charleston, a private university located in Charleston, offers a *Bachelor of Science in Cyber Security*. The American Public University System, a private, for-profit online learning institution located about 370 miles away from Marshall University, offers a *Bachelor of Science in Cybersecurity* and other related degree programs (Table 2).

Table 2: Cybersecurity or Related BS programs in the State of West Virginia

Institution	Degree	Public College	Distance from MU	CAE-CD	ABET Accredited
Salem International University	B.S. in Information Technology - Cybersecurity	No	157 miles	No	No
University of Charleston	B.S. in Cyber Security	No	53 miles	No	No
American Public University System	B.S. in Cyber Security	No	370 miles	No	No

The University of Charleston has six students enrolled in the fall semester of 2017 in their B.S. degree program in cybersecurity; their tuition is substantially higher than Marshall University. As previously mentioned, West Virginia University has recently approved new B.S. and M.S. in Cybersecurity program.

2.1.3 Cybersecurity Degree Programs in the Surrounding States

Few educational institutions within the surrounding 200 miles of Marshall University offer cybersecurity-related degrees or certificates (Table 3).

Table 3: Cybersecurity or related program in Tri-state Area within 200 miles

Institution	B.S.	MS	Distance from MU	Type
Kentucky				
Eastern Kentucky University	M.S. in Network Security and Electronics		130 miles	Public
Kentucky State University	M.S. in Computer Science (Computer Information Security Option) Cyber Security Certificate	M.S. in Computer Science Technology (Cybersecurity Option)	148 miles	Public
Northern Kentucky University	Certificate in Corporate Information Security Cybersecurity Certificate Secure Software Engineering Certificate		141 miles	Public

Ohio				
Franklin University	M.S. in Cybersecurity		135 miles	Private
Ohio State University	M.S. in Computer Science and Engineering (focus on Information Security) M.S. in Computer and Information Science (focus on Information Security)		136 miles	Public
University of Cincinnati	Cyber Operations Certificate		151 miles	Public
Wright State University	Cybersecurity Analytic Certificate	M.S. in Cyber Security	164 miles	Public

Similar to most institutions of higher education in the United States, these cybersecurity-related programs are incorporated in existing programs as either an area of emphasis or a concentration. Most of these cybersecurity-related programs have modest enrollments and are relatively new, although the national demand of cybersecurity workforce is extremely high. The enrollment of Secure Software Engineering certificates in the Department of Computer Science at Northern Kentucky University is reportedly non-existent as of fall 2017.

Cybersecurity threats constitute a universal challenge that affects all of modern society. Combined with technical knowledge/skills and business/management acumen, the M.S. in Cybersecurity degree program will be attractive to a diverse student population. The program will attract West Virginia residents, non-residents and international students.

2.2 Program Planning & Development

2.2.1 Clientele and Need

The need for cybersecurity expertise is clearly evident. For example, the security breach associated with more than one billion Yahoo user accounts in 2013, and another 500 million accounts were illegally obtained in 2016. The dominant web services provider, suffered yet another cyber attack in 2017.

Within the last few years, we have seen a substantial increase in cyber-related incidents including big data breaches, physical infrastructure tampering, ransomware. As cybersecurity continues to be a primary challenge, the need for trained experts continues to grow at an astonishing rate. More than 200,000 cybersecurity positions are currently unfilled. The Bureau of

Labor Statistics predicts employment growth of 37 percent within the information security industry over the next 10 years, with four out of every five cybersecurity jobs requiring a degree. At this rate, the United States is predicted to reach an astounding half-million or more unfilled cybersecurity positions by 2021.

IBM's Chairman, President and CEO Ginni Rometty stated, “Cyber-crime is the greatest threat to every company in the world”. Over 60 percent of the United States companies and numerous governmental agencies have been victims of cyber-attacks. The World Economic Forum recently reported that: (1) Cyber-crime damage costs will hit $6 trillion annually by 2021, (2) Cybersecurity spending will exceed $1 trillion, (3) Attacks to personal data/accounts will reach four billions by 2020 (Microsoft estimated that four billions will be online—twice the number of online people now), (4) Global ransomware damage costs are predicted to exceed $5 billion in 2017, which is up from $325 million in 2015 (15 times increase in two years), and (5) Attacks to healthcare organizations will quadruple by 2020. The political disagreement presented during and after the 2016 elections clearly magnified the criticality of addressing all cybersecurity challenges as these threats may compromise our national security and the prosperity of the American citizens.

The Integrated Post-secondary Education Data System (IPEDS) reported that the number of students enrolled in post-secondary institutions has been in a continuous decline since 2010 (two million less students between 2010 and 2015). Many states, including West Virginia, have systemically reduced their financial support to higher education, thus forcing more yearly budget cuts; therefore, the establishment of new programs to significantly increase enrollment rates and produce tuition revenues is vital to the growth of Marshall university. The M.S. in Cybersecurity degree program will be a viable, low-cost program that will significantly result in increased enrollment and the production of more tuition and program/lab fees. The M.S. in Cybersecurity degree program will effectively produce graduates who will fill the workforce needs in this rapidly-growing field.

2.2.2 Employment Opportunities

The proposed M.S in Cybersecurity degree program is timely for West Virginia, the nation, and the world. For example, Forbes reported that the burgeoning cybersecurity market is expected to grow from $75 billion in 2015 to $170 billion by 2020. A report from Cisco estimates the global figure at one million cybersecurity job openings. Morever, the demand for these positions will rise to six million globally by 2019, with a projected shortfall of 1.5 million. According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 37 percent from 2012–2022, which is a much faster rate than the average (seven percent) for all other occupations. According to the U.S. Bureau of Labor Statistics, the mean annual salary for private sector cybersecurity analyst jobs is $96,400. The U.S. News and World Report ranked the career in information security analysis 8th on its list of the 100 best jobs for 2015. CNN Money ranked the career of an Information Assurance Analyst 9th in 2015 and 5th in 2017 in Top 100 best jobs. Cybersecurity workers can also command an average salary premium increase of nearly $6,500 per year, or nine percent more than other IT workers, according to the Job Market Intelligence. It is clear that there is a strong need and job market for cybersecurity professions, locally, nationally and internationally.

A search of indeed.com for cybersecurity jobs in West Virginia showed advertisements for 41 different positions (https://www.indeed.com/jobs?q=cybersecurity&l=WV). About half of these jobs are in the IT industry including Amazon Web Services, Inc., NetCentrics Corporation, Pragmatics, and Rockwell Collins. The other half of the jobs are for commercial banks, the healthcare and manufacturing sectors, engineering firms, and federal and state government law enforcement. As reported by many industrial leaders, a substantial percentage of IT and Cybersecurity jobs in West Virginia are filled by graduates from out-of-state and foreign institutions. For example, many cybersecurity and technical support technician positions offered by Toyota Motor Manufacturing, West Virginia, Inc. were partially filled by local students in 2017 due to the lack of training/education in the area. Local companies such as State Electric Supply Co. or Strictly Business Computer Systems, Inc. have had similar experiences. The proposed M.S. in Cybersecurity degree program has received the full support of many local companies and letters of support are included in Appendix B.

2.3 Program Impact

The Weisberg Division of Computer Science currently houses three programs (B.S. in Computer Science degree program, M.S. in Computer Science degree program, and M.S. in Information

Systems degree program). The Division has taken the steps to start a B.S. in Computer and Information Security degree program in the fall 2018 semester, along with the M.S. in Cybersecurity. Currently, various cybersecurity courses are offered that relate to technology, people, and process, including all required Information Systems (IS) courses for the *Graduate Certificate in Information Security* of the College of Information Technology and Engineering. The M.S. in Cybersecurity degree program will strengthen existing programs at Marshall University while creating new pathways for education and research. Closely related existing Marshall University undergraduate and graduate degree and certificate programs (such as Information Systems, Technology Management, Digital Forensics and Information Assurance, Electrical and Computer Engineering, Management Information Systems, and Criminal Justice), will have the option of enhancing their offerings by incorporating Cybersecurity courses. The students in these programs will have many opportunities to participate in undergraduate and graduate research projects. These projects will provide students with research experience in innovative cybersecurity fields. The program's faculty will create partnerships with other universities and research institutions.

2.4 Cooperative Arrangements

The proposed M.S. in Cybersecurity program will incorporate an internship option in the curriculum. Currently, the Weisberg Division of Computer Science has strong partnerships with several industry partners and state government agencies. The proposed Cybersecurity program already has the strongest support from many local, state and tristate industries and employers. The advisory board members of the Weisberg Division of Computer Science have been very excited about this much needed degree program and have committed themselves to providing suitable employment opportunities for enrolled students as well as graduates of this proposed degree program. In addition, the advisory board members have committed to forming less formal relationships earlier in the students' curriculum through field experiences, internships, and co-ops beginning in the sophomore year.

2.5 Alternatives to Program Development

The M.S. in Cybersecurity degree program will be one of the the first established M.S. in Cybersecurity degree programs in a public institution in West Virginia. The regional, national and international shortage of qualified graduates in this specialized field have shaped the process of identifying and developing the program learning outcomes and curriculum. Currently, There is not an alternative to the proposed M.S. in Cybersecurity degree program.

3. Program Implementation Projected Resource Requirements

The program does not require additional resources in its initial stage and can be sustainable for two years by leveraging already existing resources available at the Weisberg Division of Computer Science. Additional resources might be added either when the number of students reaches 50 students or during the third year of the program. Even with these additional resources, the program will remain cost-effective. The program will provide multiple benefits at a low cost to the institution. Scenarios that examine the Return on Investment (ROI) of this timely program have shown it to be a lucrative addition to Marshall University.

3.1 Program Administration

The Weisberg Division of Computer Science of the College of Information Technology and Engineering will house the M.S. in Cybersecurity degree program. The Chair of the Weisberg Division of Computer Science will supervise and manage the program with oversight by the Dean of the College of Information Technology and Engineering. The college does not project changes in the administration of the division with the addition of this new degree program.

3.2 Program Projections

Based upon the number of student inquiries and interest of the proposed degree, it is conservatively estimated that the M.S. in Cybersecurity program will have 20 full time equivalent (FTE) students in its first year, with 20 percent annual growth and 80% retention in the following five years (Table 4). Twenty-eight students will graduate from the program in the 5th year.

Table 4: Student Enrollment Projection

Student Enrollment	1st year	2nd year	3rd year	4th year	5th year
Enrollment of 1st year students	20	16			
Enrollment of 2nd year students		24	19		
Enrollment of 3rd year students			29	23	
Enrollment of 4th year students				35	28
Enrollment of 5th year students					42
Estimated Total Student Enrollment	**20**	**40**	**48**	**58**	**70**

3.3 Faculty Instructional Requirements

The College of Information Technology and Engineering has the administrative system and necessary faculty to support the M.S. in Cybersecurity degree program. The Weisberg Division of Computer Science's faculty acquired terminal degrees in their fields, have demonstrated excellent research and publication records, and possess the technical expertise to support the program. Dissertations and past research projects of the faculty have focused on security in mobile and wireless networking, Internet of Things (IoT), intrusion detection, cybersecurity, and cloud computing.

Recent staffing changes in the College of Information Technology and Engineering (CITE) have provided the college's administration with an opportunity to reshape the future of the Weisberg Division of Computer Science. CITE Dean has implemented an aggressive plan to address systemic obstacles, enhance the efficiencies of program delivery, and modernize the offerings of the Division through hiring very promising faculty who possess the latest knowledge in the fields of computer science and cybersecurity. The Division has successfully hired five talented tenure-track assistant professors in the last couple of years. These hires were tasked with teaching courses in the existing programs and developing research programs in their areas of expertise. Student engagement in faculty research projects is not only a key component to the success of the program, but also essential for faculty retention, promotion and tenure.

Each of the five new faculty received a three-credit-hours release per semester in the first year to develop the research program. The five faculty will collectively teach an additional 30 credit hours beginning in the fall semester of 2019, which will eventually result in covering the new cybersecurity courses. Out of the ten full-time faculty of the Weisberg Division of Computer Science, five faculty will teach the new cybersecurity courses (Table 5).

Table 5. New Cybersecurity Courses and Faculty Assignment

New Cybersecurity Courses	Term	Course starts	Faculty
CYBR 510 - Introduction to Cybersecurity	SP	2019	Dr. Cong Pu
CYBR 530 - Cybersecurity Policies and Management	SP	2019	Dr. Wook-Sung Yoo
CYBR 615 - Cyber Risk and Vulnerability	FA	2019	Dr. Paulus Wahjudi
CYBR 620 - Cyberwarfare	SP	2020	Dr. Husnu Narman
CYBR 625 - Applied Cryptography	SP	SP	Dr. Tianyi Song

Based on the estimated number of students shown in Table 4 and the number of computer science and cybersecurity courses in the M.S. in Cybersecurity degree program, one full-time faculty time from current faculty body and one adjunct faculty will cover courses needed in the program's curriculum in second year. 1.25 full-time faculty and 2 adjunct faculty will teach few more computer science sections needed for the students enrolled in the program from the third year of the program. CITE Dean anticipates the addition of a tenure-track faculty line to support the program's growth starting from the third year of the program. More faculty and adjuncts could be added as the program continues to grow. Table 6 displays the projected revenue generation over the first five years of delivering the program.

3.4 Library Resources and Instructional Materials:

Marshall University Libraries have the majority of the resources needed to support the proposed M.S. in Cybersecurity degree program. Few additional library collections may be added over time to adequately complement the library resources currently available for the Computer Science programs.

3.5 Support Service Requirements

A dedicated cybersecurity lab system administrator and two part-time graduate students (lab assistants) will be needed after the program acquires a critical mass (probably after three years from the starting of the program).

3.6. Facilities Requirements

Marshall University Computing Services currently supports all user computing needs of the users on Marshall campuses. The College of Information Technology and Engineering has recently added multiple state-of-the-art computer labs and classrooms within its magnificent Arthur Weisberg Family Applied Engineering Complex (WAEC) to support the various programs of the Weisberg Division of Computer Science. The Weisberg Division of Computer Science houses a cybersecurity lab, Computer Science Project lab, and Computer Graphics lab. These spaces are shared amongst the existing programs in the Weisberg Division of Computer Science and will support the addition of other programs in the division, including the proposed M.S. in Cybersecurity degree program. The cybersecurity lab has a built-in internal network for testing and developing various cybersecurity-related projects without compromising the Marshall University network. The Cybersecurity lab currently supports existing courses of Internetworking and Cybersecurity. The M.S. in Cybersecurity program will have access to the available computer workstations and Wi-Fi in WAEC. As the program continues to grow, another cybersecurity specialized lab/classroom will be needed. The cost of the additional equipment is estimated at $250,000 (to acquire additional powerful computers, servers, and network facilities).

3.7. Operating Resource Requirements

As an integral part of the Weisberg Division of Computer Science, the M.S. in Cybersecurity degree program will share the operating resources with the other programs offered by the Division. Table 6 shows the estimated revenue generated by the proposed program during its first five years (based on the estimated number of students in Table 4). Table 7 provides a summary of the operating resource requirements.

Table 6. Revenue Generated by the Proposed Program in 5 years

	Tuition & Fee	1st Year		2nd Year		3rd Year		4th Year		5th Year	
	Yearly	FTE	Revenue	FTE	Revenue	FTE	Revenue	FTE	Revenue	FTE	Revenue
Resident of WV (50%)	$9,188	10	$91,880	20	$183,760	24	$220,512	29	$266,452	35	$321,580
Metro resident (20%)	$16,040	6	$96,240	12	$192,480	14	$224,560	17	$272,680	21	$336,840
Out of State (30%)	$21,222	4	$84,888	8	$169,776	10	$212,220	12	$254,664	14	$297,108
Total		**20**	**$273,008**	**40**	**$546,016**	**48**	**$657,292**	**58**	**$793,796**	**70**	**$955,528**

Table 7: Five-Year Projection of Total Operating Resources Requirements

	First Year 2018	Second Year 2019	Third Year 2020	Fourth Year 2021	Fifth Year 2022
A. FTE POSITIONS					
1. Administrators	0.125	0.125	0.125	0.25	0.25
2. Full-time Faculty	0.5	1	1.25	1.25	1.25
3. Adjunct Faculty	0	1	2	2	2
4. Graduate Assistants	0	0	2	2	2
5. Other Personnel:					
a. Clerical Workers	0	0	0	0	0
b. Professionals	0	0	1	1	1
B. OPERATING COSTS					
1. Personal Services:					
a. Administrators	$18,750.00	$18,750.00	$18,750.00	$37,500.00	$37,500.00
b. Full-time Faculty	$53,125.00	$106,250.00	$132,812.50	$132,812.50	$132,812.50
c. Adjunct Faculty	$-	$4,500.00	$9,000.00	$9,000.00	$9,000.00
d. Graduate Assistants	$-	$-	$6,400.00	$6,400.00	$6,400.00
e. Non-Academic Personnel:					
Clerical Workers	$-	$-	$-	$-	$-
Professionals	$-	$-	$62,500.00	$62,500.00	$62,500.00
Total Salaries	$71,875.00	$129,500.00	$229,462.50	$248,212.50	$248,212.50
2. Current Expenses (Recurring)	$10,000.00	$15,000.00	$20,000.00	$30,000.00	$40,000.00

3. Repairs and Alterations (Lab)	$-	$-	$5,000.00	$5,000.00	$5,000.00
4. Equipment:					
Educational Equip.	$5,000.00	$5,000.00	$5,000.00	$5,000.00	$5,000.00
Library Books	$-	$-	$-	$-	$-
5. Nonrecurring Expenses: (Lab)	$-	$-	$250,000.00	$-	$-
Total Costs	$86,875.00	$149,500.00	$509,462.50	$288,212.50	$298,212.50
C. Sources					
1. General Fund Appropriations	$273,008.00	$546,016.00	$657,292.00	$793,796.00	$955,528.00
D Net Revenue	$186,133.00	$396,516.00	$147,829.50	$505,583.50	$657,315.50

The program and lab fees will be sufficient to cover additional operating budget needs, and will ensure the program's financial viability.

3.8. Source of Operating Resources

The source of the program's operational support will be a combination of: (1) sharing the operating budget of the Weisberg Division of Computer Science, and (2) program and lab fees that will specifically be collected from the students in this program.

References

- Andrew McGettrick, (2013) "Toward Curricular Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training", ACM Advanced Computing as a Science and Professions.
- Burley, Diana, et al, (2016) "Special Session: ACM Joint Task Force on Cyber Education," Proceedings of the 47th ACM Technical Symposium on Computing Science Education, ISBN: 78-1-4503-3685-7.
- Special Session: ACM Joint Task Force on Cyber Education by Bureau of Lab Statistic (2017). Retrieved from http://escholarship.org/uc/item/0624q2sj
- "One Million Cybersecurity Job Openings In 2016," by Steve Morgan (2016), Forbes/Tech, Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#3717836827ea.
- "Cybersecurity could be WV's next big growth area, leaders say" by Brad McElhinny, MetroNews (2017), Retrieved from http://wvmetronews.com/2017/08/05/cybersecurity-could-be-wvs-next-big-growth-area-leaders-say/.
- CNN/Money, "100 Best Jobs in America", Retrieved from http://money.cnn.com/pf/best-jobs/
- Occupational Outlook Handook by Bureau of Lab Statistic (2017), Retrieved from https://www.bls.gov/ooh/
- National Centers of Academic Excellence in Cyber Defense (2017), Retrieved from https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/.
- ABET, Computing Accredited Commission, Retrieved from http://www.abet.org/about-abet/governance/accreditation-commissions/computing-accreditation-commission/.

Appendix A: Course Description in Cybersecurity Program

CYBR 510 - Introduction to Cybersecurity. 3 hrs.
This course covers concepts and issues in physical and cyber security; technological vulnerabilities found in operating systems, database, Web servers, Internet, and local area networks.

CYBR 530 - Cybersecurity Policies and Management. 3 hrs.
This course covers topics of risk management, integrating continuous monitoring and real-time security solutions with information system to improve situational awareness and deployment of countermeasures.

CYBR 615 - Cyber Risk and Vulnerability. 3 hrs.
This course focuses on the complete cycle of Enterprise security from identifying vulnerabilities, detecting application exploitation and post exploitation mitigations and analysis for an enterprise level cyber infrastructure.

CYBR 620 – Cyberwarfare. 3 hrs.
The course covers both offensive and defensive techniques pertaining to cyber security from techniques to find vulnerabilities and analysis on the likelihood of an attack to developing solutions to secure cyber infrastructure.

CYBR 625 - Applied Cryptography. 3 hrs.
This course covers critical topics in cryptography, including the classical ciphers and cryptanalysis, Shannon's perfect secrecy, Feistel ciphers and DES, SPN's and AES, linear and differential cryptanalysis, public-key crypto (RSA, Discrete Log), secure hash, elliptic curves.

Appendix B: Letter of Support

STATE OF WEST VIRGINIA
DEPARTMENT OF ADMINISTRATION
OFFICE OF TECHNOLOGY
State Capitol
Charleston, West Virginia 25305

Jim Justice
Governor

John A. Myers
Cabinet Secretary

John D. Dunlap
Chief Technology Officer

October 6, 2017

To whom it may concern:

As a cyber security expert serving the Department of Defense and the State of West Virginia, I have been exposed to the stark reality of the cyber security threat. Our world has fully integrated technology and the resulting interdependence has created a serious situation. The rapid advancement and integration of new technology, technology inheritably vulnerable, coupled with the lack of a skilled cyber workforce presents a situation that is likely to get worse before it becomes better. A key component to answer this threat is a strong dedication to the cyber workforce development.

The importance of developing a cyber workforce cannot be understated, but it should also be noted the development programs must be designed and implemented with an understanding of the cyber threat issue. Educational programs must account for the desperate need of technical-minded experts, trained with the skills to solve complex problems. Core education should start and delve deep in to computer science fundamentals. In addition, programs must recognize the need to teach practical skillsets in hands-on environments. Finally, cyber workforce programs can serve to help fill the workforce gap sooner, rather than later through internship and apprenticeship programs offering mutually beneficial opportunities.

In conclusion, I recommend Marshall University strongly consider implementing a strong cyber security program for the undergraduate and graduate levels with a curriculum foundation in computer science.

Respectfully,

//SIGNED//
Joshua D. Spence, CISSP
Chief Information Security Officer
West Virginia Office of Technology

City Holding Company

Wook-Sung Yoo, Ph. D.
Professor and Chair, Weisberg Division of Computer Science,
College of Information Technology and Engineering,
WAEC 3101A,
Marshall University
Huntington, WV 25755

Dear Dr. Yoo,

I'm very excited about the prospect of a Cybersecurity program at Marshall University. As an alumnus of Marshall University's Computer Science program, it's encouraging to see progress and growth. It seems I read an article weekly describing what is believed to be a cyber security professional shortage by 2019. What better time than now to begin providing students with an education that will allow them to take full advantage of this dynamic job market.

Throughout the country, financial institutions have identified cyber-threats as their top priority for 2017. This issue has been moved to the forefront of bank-board meeting agendas, and senior managers must act fast to mitigate these growing threats to banks. Cyber-threats have the power to wipe out huge swathes of business value in a matter of moments, and banks need to address this growing risk through resource budgeting. Radical change needs to be made. One way of incorporating cost-effective solutions will be by enlisting the help of specialized external cybersecurity teams along with building strong internal staffing expertise. The traditional approach to IT solutions and tools is not going to be enough to tackle this problem, which changes shape every moment. Skilled expert knowledge will be required to effectively tackle the fast-paced dynamics of threats—and even then because of the speed of technological development, it will be hard to keep up.

I'm sure City National Bank will be challenged in our market(s) to find qualified candidates to fill the security analyst positions that will be needed. We already are! Educate them and we'll find a place for them.

Sincerely,

Jeff D Legge

Jeffrey D. Legge
Chief Information and Administrative Officer
City Holding Company

strictly
BUSINESS
COMPUTER SYSTEMS

848 4th Avenue, Suite 200
Huntington, WV 25701
(304) 529-0401
www.sbcs.com
info@sbcs.com

Wook-Sung Yoo, Ph.D.
Professor and Chair, Weisberg Division of Computer Science,
College of Information Technology and Engineering,
WAEC 3101A,
Marshall University
Huntington, WV 25755

Dear Dr. Yoo,

I am writing in support of your proposed plan to create a Bachelor of Science in Cybersecurity program at Marshall University.

Given the recent news of a massive security breach and the possible leak of millions of customer records at Wells Fargo, it should come as no surprise that the field of Cybersecurity is tremendously important to our personal privacy interests as well as a major contributor to the protection of our national security interests. As such, the formation of a degree program in Cybersecurity is not only timely, but vital.

I believe the Weisberg Division of Computer Science is well positioned to take advantage of this opportunity as they have the resources in place to begin this program very quickly.

As the principal of a technology company that works with both industry and the Federal Government, I see daily, the demand for, and growing shortage of, professionals to manage cybersecurity initiatives nationwide, and am completely confident that graduates of Marshall's program will have little trouble finding rewarding careers as well as making significant contributions to the field.

As an employer of technology professionals, I am also confident that we will be the first in line to consider hiring a graduate of this important program.

With best regards,

Ml G Owens, SR,

Michael G. Owens, Sr.
President
Strictly Business Computer Systems Inc.

1900 Kanawha Boulevard, East, Building 6 • Charleston, WV 25305
Steven L. Paine, Ed.D., State Superintendent of Schools
wvde.state.wv.us

October 13, 2017

Wook-Sung Yoo, Ph.D.
Professor and Chair, Weisberg Division of Computer Science
College of Information Technology and Engineering
Marshall University
WAEC 3101A
Huntington, WV 25755

Dear Dr. Yoo,

Thank you for providing me with an overview of the proposed Bachelor of Science in Cybersecurity (BSCY) degree program currently under consideration at Marshall University. The program appears to be a rigorous course of study designed to prepare graduates to effectively prevent and mitigate emerging and evolving threats while maintaining high standards of ethical professional practice. I am pleased to support your efforts.

The need for trained experts in Cybersecurity has never been more pressing. According to the Identity Theft Resource Center,[1] the United States has experienced more than 1,000 confirmed data breaches to date in 2017, with at least 163 million individual records being exposed to unauthorized parties. Over the past 12 years, nearly 8,000 confirmed data breaches have exposed more than one billion records. In perhaps the most shocking breach so far, the credit reporting company Equifax revealed earlier this month that approximately 143 million credit records for more than 200,000 people were accessed by hackers who exploited a vulnerability in the company's website. Breaches and other security incidents seem to be becoming commonplace.

West Virginia's K-12 education system has so far been fortunate in avoiding major data breaches that threaten our students' information. However, we know that the risk is ever present and constantly growing. Agencies like the West Virginia Department of Education and our districts need highly skilled professionals with expertise to identify and stop threats before they become incidents and to respond quickly when breaches do occur.

[1] Identity Theft Resource Center. (2017, September 14). 2017 Data Breaches. Retrieved from http://www.idtheftcenter.org/2017-data-breaches.html

Threat environments evolve and change quickly. Cybersecurity professionals need adaptive skills and excellent critical thinking processes to be able to respond effectively and decisively. Marshall University's proposed BSCY program is designed to cultivate those technical and professional skills and to ensure that graduates will collaborate successfully to improve their employers' security postures in support of organizational missions.

Technology is a powerful tool for change. Through my leadership roles in West Virginia's education sector and in initiatives like the Partnership for 21st Century Skills, I have seen directly how effective technology implementation can provide a strong foundation for student achievement. West Virginia's educators have long recognized the great promise technological tools and advancements hold for helping our students cultivate the knowledge and skills they need to build bright futures. Every day, I see our educators working to find ways to harness the promise of technology and connected learning environments while simultaneously trying to avoid potential harm to their students. The ability to collaborate with trained Cybersecurity professionals, such as those who will graduate from the BSCY program, will enhance our educators' confidence that they are acting in the best interests of their students while adopting new innovations for improvement.

We must use every available tool and technology to prepare our students for their futures, and we must do so while respecting and protecting the security of their personal information. I look forward to watching the BSCY program at Marshall University further evolve as plans are finalized and implemented. I hope that, in the near future, we may see Marshall's BSCY graduates working with educators to keep our students safe.

Sincerely,

Steven L Paine

Steven L. Paine, Ed.D.
State Superintendent of Schools

SLP:GHW:csm

MARSHALL APPALACHIAN TRANSPORTATION INSTITUTE

CBER CENTER FOR BUSINESS AND ECONOMIC RESEARCH

Wook-Sung Yoo, Ph.D.
Professor and Chair, Weisber Division of Computer Science,
College of Information Technology and Engineering
WAEC 3101A
Marshall University
Huntington, WV 25755

Dear Dr. Yoo,

I am writing in support of the proposed Bachelor of Science, Cybersecurity program at Marshall University. As a research arm of Marshall University, we work directly with the public and private sectors who are increasingly concerned about cyber-threats.

This year alone we have seen an alarming number of cybersecurity breaches within the Federal Government, an onslaught of ransomware attacks and the Equifax data breach that compromised as many as 143 million consumers. Given the surge in cyber-attacks it is vital to the nation's security interest that we start developing a workforce that can combat these types of attacks.

I believe the Weisburg Division of Computer Science would be doing a great service to our community and nation by the creation of a Bachelor of Science Degree in Cybersecurity.

Sincerely,

Robert H. Plymale

Robert H. "Bob" Plymale,
Marshall University Research Corporation
Associate Vice President for Economic Development
COO, Appalachian Transportation Institute
COO, Center for Business and Economic Research