Mississippi Cybersecurity Labor Market and Business Analysis

March 2021

Prepared by:
Bayley Peoples, Graduate Research Assistant
Andy Kilgore, Program Director, Mississippi Defense Initiative
Craig M. Sumrall, Liaison, Mississippi Defense Initiative
Heather N. Brown, MSED, Research Analyst
Dr. Chad R. Miller, Professor of Economic Development
Tasha May, Operations Manager, Trent Lott Center

PROMOTING INNOVATION, DIVERSIFICATION AND COOPERATION IN THE MISSISSIPPI DEFENSE COMMUNITY

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

MSDEFENSE.NET

AA/EOE/ADAI UC 78138 3.18

Table of Contents

This report was prepared under contract with the National Security Technology Acceleration Support and Economic Diversification Efforts for the State of Mississippi with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the National Security Technology Acceleration Support and Economic Diversification Efforts for the State of Mississippi and does not necessarily reflect the views of the Office of Economic Adjustment.

EXECUTIVE SUMMARY

This is an update of a report investigating the outlook (supply-side) of available workforce professionals who possess cybersecurity knowledge, skills and abilities in Mississippi as compared to employer demand for these types of workers through the year 2023. The report assessed the types of cyber-related academic programs available in Mississippi, number of program graduates, companies hiring, and industry sectors dependent on cybersecurity. The following is a summary of findings:

- There is anticipated to be more demand for workers in cyber-related occupations than academic programs are graduating/completing with an average of 2,254 annual openings versus 1,016 academic program completions.
- Mississippi universities and colleges should evaluate enrollment capacities to determine if there is ample room to accommodate an increase of individuals enrolling in cybersecurity.
- Mississippi universities and colleges should consider aligning classifications of academic programs to be more specific, where applicable, to attract individuals interested in cybersecurity professions and to communicate with employers the number of graduates completing programs of study. These institutions appear to use more generic CIP code classifications rather than more specific cyber-defined CIP codes for programs of study. The more generic classification may be necessary for a variety of reasons, but also may reduce the ability of prospective employers to gauge availability of a skilled workforce.
- Cyber-related occupations are anticipated to continue growing through 2023 by 7.7% in Mississippi and by 9.5% nationally. This is reflected in 2018 employment of 24,058 jobs versus 25,903 jobs in 2023. The growth rate of 7.7% will outpace Mississippi's overall workforce growth projection of 3%.
- Military bases and installations located in Mississippi possess specialized cybersecurity personnel which the state should target to attract into civilian occupations when exiting military service. The state should also work collaboratively with the military on cyber security training opportunities.
- Nationally, entry-level cybersecurity specialists are obtaining industry-recognized certifications in adequate supply to meet employer demand. However, advanced certifications in professional and expert level credentials are not meeting the quantities needed for employer demand.

INTRODUCTION TO CYBERSECURITY

The Mississippi Defense Initiative (MDI) located at The University of Southern Mississippi conducted this cybersecurity labor study to better understand the state of Mississippi's supply and demand of cybersecurity professionals. This report assessed the types of cyber-related academic programs available in Mississippi, number of program graduates, companies hiring, and industry sectors dependent on cybersecurity. Based on the results of a desktop asset inventory and interviews with industry professionals, there appears to be a larger demand for cybersecurity professionals in Mississippi than graduates entering the workforce through 2023.

The U.S. Department of Defense (DoD) identifies cybersecurity as critical to the way the entire nation functions (Defense.gov, Cyber Strategy). DoD adopted four pillars for a cyber strategy:

- Protecting the American people, the homeland and the American way of life by safeguarding networks, systems, functions and data
- Promoting American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation
- Preserving peace and security by strengthening the ability of the U.S., its partners and allies to deter and punish those who use cyber maliciously
- Advancing American influence to extend the key tenets of an open, interoperable, reliable and secure internet

Protection of America's cyber infrastructure is so critical that as of December 31, 2017, federal defense contractors which process, store or transmit Controlled Unclassified Information (CUI) must meet the Defense Federal Acquisition Regulation Supplement (DFARS) minimum security standards.

Mississippi has a detailed multi-agency response plan in the case of cyber-related incidents in the state. All suspected cybercrimes should be reported to the FBI, as they have federal jurisdiction, a skilled investigative team, and more charging options under Federal Code. Many public sector agencies are monitored by the Mississippi Department of Information Technology Services (ITS). The private sector is not under any mandatory reporting requirements in the event of a cyber-attack. It is heavily recommended that all private sector companies maintaining personally identifiable information (PII) have a cyber insurance policy.

For the purposes of this study, the term cybersecurity refers to the technologies and processes designed to defend computer systems, software, networks, and user data from unauthorized access (onecomodo.com). Cybersecurity also addresses threats distributed through the internet by cybercriminals, terrorist groups, and hackers. Cybersecurity is about protecting devices and networks from unauthorized access or modification. The internet is not only the chief source of information, but it is a medium through which people do business.

BACKGROUND

The number of worldwide internet users in 2020 was 4.54 billion, up 7% year-on-year (We are Social, Ltd). People use the internet for a wide variety of reasons that have value to a cybercriminal. Businesses and individuals advertise and sell products in various forms, communicate with customers and retailers, and perform financial transactions. Due to this, hackers and cybercriminals use the internet as a tool to spread malware and carry out cyber-related attacks.

Cybersecurity aims to protect computers, networks, and software programs from such cyber-attacks. Most of these digital attacks are aimed at accessing, altering, or deleting sensitive information; extorting money from victims; or interrupting normal business operations.

Types of Cybersecurity:

- Information Security
- Network Security
- Application Security

Types of Cyber Security Threats		
Viruses	Identity Theft	Password Attacks
Spyware and Key loggers	Adware	Trojans
Ransomware	Ransomware: Infection Mechanism	Browser Hijacker
Zero-Day Attacks	Phishing Emails	Shady Websites
Peer to Peer File Sharing	Torrent Downloads	

Source: https://one.comodo.com/blog/cyber-security/what-is-cyber-security.php

Why is Cybersecurity Important?

Researchers estimate that as much as an immediate $300-$500 billion and 1.2 million jobs are lost every year due to the theft of intellectual property (Scott & Spaniel, 2016). Infamous cyber-attacks such as the GoldenEye and WannaCry ransomware have crippled several organizations and forced many to shut down operations (Onecomodo). In the wake of

these sophisticated cyber-attacks and security breaches, cybersecurity has a spotlight for organizations of all sizes.

New variants, new tactics, and cyber threats continue to evolve. Not only has the number of attacks increased for businesses and individuals, but the level of sophistication has increased as well. There is anticipated to be a dramatic rise in Ransomware and Malware malicious activity for hire using the dark web. It will allow anyone, no matter their technical knowledge, to easily and quickly initiate cyber-attacks.

Nevertheless, the extent of damages caused by cyber-attacks in the past has shed light and raised greater awareness about the cyber-attacks and the need for better security measures among organizations of all types. This will serve as a motivation for cybercriminals to up their game by staging new and more sophisticated attacks in the future. Therefore, there is opportunity for Mississippi to protect and grow its cybersecurity defense economy through planning of a well-qualified cyber workforce.

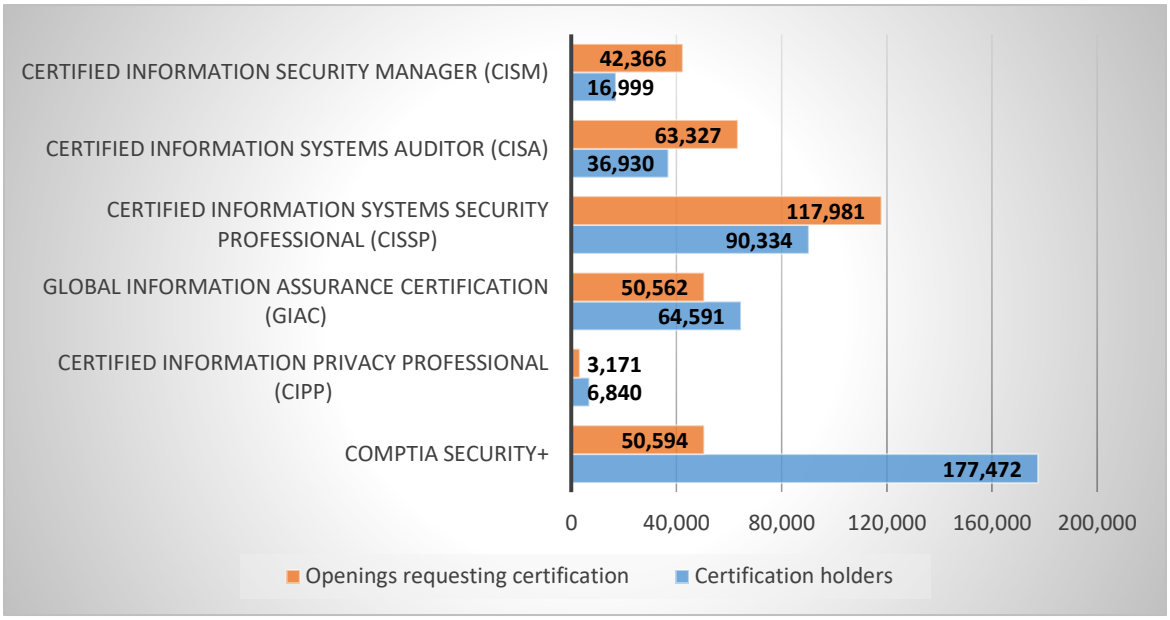
Cyber Security Education

The computer information systems industry has built a variety of professional, stackable certifications which align with the National Center for Cybersecurity Education (NICE) Cybersecurity framework as a means of responding to workforce needs. These stackable credentials generally are grouped into three categories (CompTIA.com):

- Specialist – Early career professional with 0-2 years of experience
- Professional – Early to mid-level IT professional with 2-5 years of experience
- Expert – Established IT professional with 5+ years of experience

The challenge is to encourage IT professionals to continue a journey of life-long learning that moves beyond specialist and into processional and expert-level credentials. These certifications provide baseline knowledge and skills to increase the supply of available workers to employers. One of the most commonly recognized certifications is the CompTIA Security+ with 173,162 certified specialists. While this number exceeds the job postings by a ratio of 4.8, other more advanced credentials have fewer certified professionals than posted job openings. For example, Certified Information Systems Auditor (CISA) has 33,048 certification holders as compared to job demand of 44,948. Additionally, the Certified Information Security Manager (CISM) has 13,923 certification holders compared to job openings of 29,905 (see Figure 1).

Figure 1: Holders of Common Cybersecurity-related Certifications to Job Openings Requesting Certifications, March 2021



Source: https://www.cyberseek.org

METHODOLOGY

The following sources of publicly available secondary data were used to conduct the analysis. O'Net Online was useful in defining standard occupation classification codes and training providers. EMSI economic modeling and JobsEQ were used for comparing job growth trends and graduation completion trends. BCC Research was used to understand market trends. Company and organization websites aided in describing how each contribute to the topic. The findings are heavily dependent upon secondary sources of published information and a limited number of telephone interviews for data gathering. More extensive research is needed to further quantify the extent of need for Mississippi.

SCOPE

This report will compare workforce availability *(supply-side)* for cybersecurity-related occupations in Mississippi with the expected occupational outlook *(demand-side)*. The purpose of this analysis is to highlight potential gaps that may exist in the state's ability to produce enough cyber professionals to meet employer demand. The analysis compared 2018 occupations to those anticipated through 2023.

As cyber threats continue to grow in sophistication, organizations face a persistent challenge in recruiting skilled cybersecurity professionals capable of protecting their systems against the threat of malicious actors. With cybercriminals now responsible for billions in losses per year and state-sponsored hacking groups posing an ever-greater threat, the need for individuals capable of securing networks against attackers has never been greater.

LABOR SUPPLY

This section of the report will address the supply of Mississippi's cybersecurity talent. To begin this section, a summary of key federal initiatives providing workforce frameworks was identified. On the state level, a review of academic programs being offered at universities and colleges was addressed to quantify graduates entering the workforce. From the qualitative perspective, a summary of examples was discovered regarding high school, adult training, and military initiatives investing in cyber related training. This information was helpful in determining Mississippi's overall ability to provide a supply of qualified talent meeting the demand for employers.

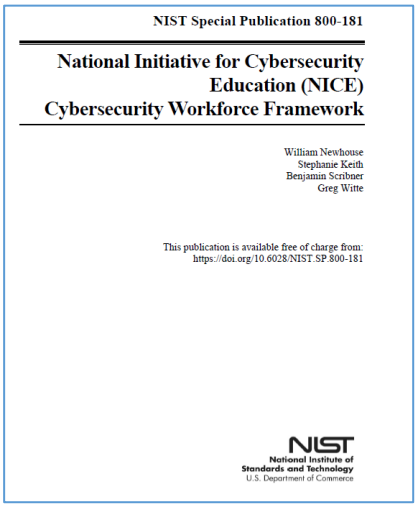
Federal Cybersecurity Workforce Framework

Three federal agencies, in particular, have been influential in leading how the nation's cybersecurity workforce is defined and trained. These agencies include:

- United States Department of Commerce
- United States Department of Labor
- United States Department of Education

Other federal agencies have provided leadership, but these three created the underlying foundations for how individuals get access to knowledge and skill development to become a cybersecurity professional.

The National Center for Cybersecurity Education (NICE), led by the National Institute for Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership among government, academia, and private sector employers that developed a framework for cybersecurity education, training and workforce development (NICE Framework, NIST SP 800-181). The framework provides a reference for educators to develop curriculum, certificate or degree programs, training programs, courses, seminars or exercises that cover knowledge, skills, and abilities of the cyber professional.


NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

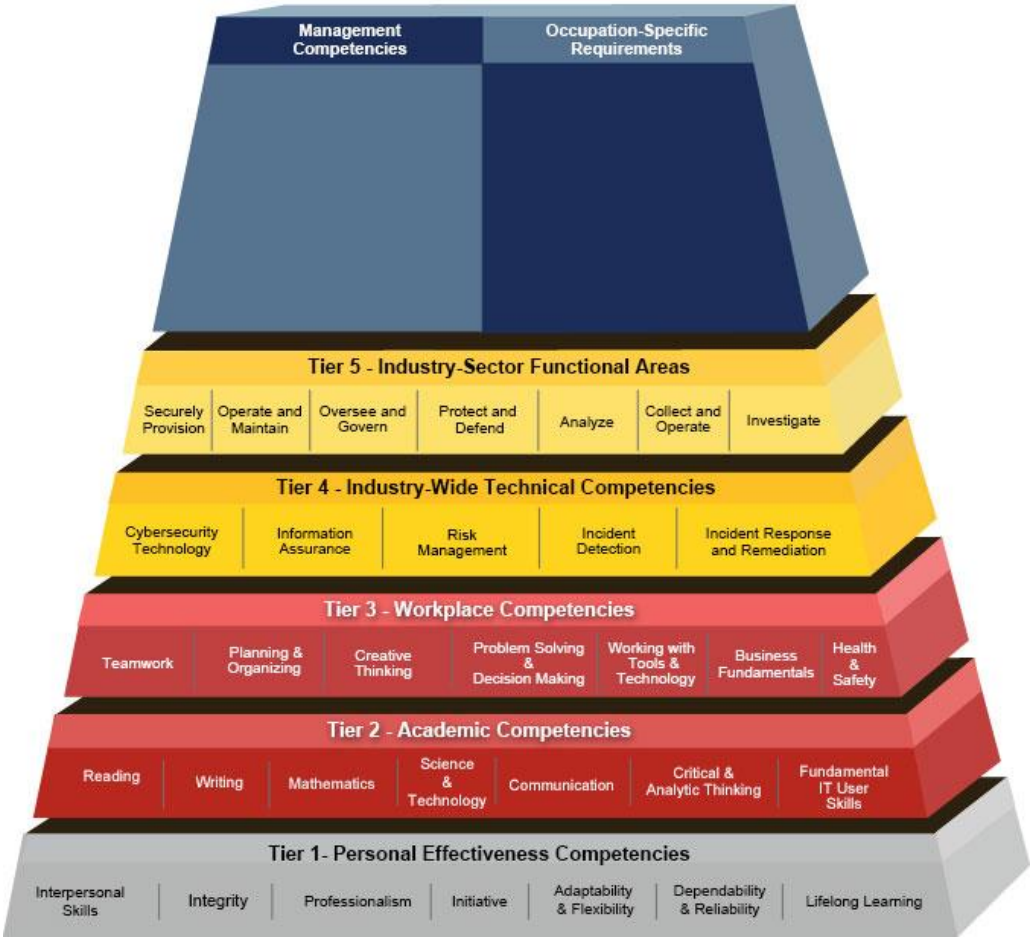
William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The U.S. Department of Labor developed the Cybersecurity Competency Model (CMMC), a 5-tiered stackable credential model, to describe the competencies needed by individuals whose activities impact the security of their organization's cyberspace. This model was built upon NICE Workforce Framework (see Figure 2). The model and associated program are designed to protect defense contractors from cyber attacks by defining the latest skill and knowledge requirements for cybersecurity professionals.

Figure 2: U.S. Department of Labor, Employment and Training Administration's Cybersecurity Competency Model, 2021



Classification of Cyber Related Instructional Programs

The U.S. Department of Education's National Center for Education Statistics developed the Classification of Instructional Programs (CIP) to provide a taxonomic scheme for accurately tracking, assessing, and reporting academic fields of study and program completion activity (Department of Education NCER). The taxonomy was first developed in 1980, and it allows new programs of study, like cybersecurity, to be formally adopted by colleges across the nation. For cybersecurity, at the most general level, there are multiple options for adopting the two-digit academic program codes such as:

- 11-Computer and information sciences and support services
- 14-Engineering
- 26-Biological and biomedical sciences
- 29-Military technologies

- 43-Security and protective services
- 52-Business, management, marketing and support services

Drilling down into more detailed, 6-digit CIP codes revealed specialty academic program definitions specific to cybersecurity. For Mississippi colleges and universities which desire to be identified with expertise in cybersecurity, it is recommended they consider adopting these cyber-specific 6-digit CIP codes including, but not limited to:

- 43.0116 Cyber/Computer Forensics and Counterterrorism
- 29.0207 Cyber/Electronic Operations and Warfare
- 11.0102 Artificial Intelligence
- 43.0304 Terrorism and Counterterrorism Operations
- 52.2101 Telecommunications Management

These cyber-specific CIP codes were not found among Mississippi's educational institutions. Therefore, this section of the report will use other similar academic classifications and will be referenced as *cyber-related programs*.

Universities and Colleges in Mississippi

Mississippi universities and colleges appear to be graduating 22% less graduates from academic programs than anticipated job demand through 2023. These completions represent a range spanning from one-year certificates through doctoral degrees. Currently, the majority of program completers predominately fall into 3 groups including General Computer and Information Sciences (CIP 11.0101); Information Technology (CIP 11.0103); and General Computer Programming (CIP 11.0201) (see Table 1).

The major change in this data from the previous study has been a been a major shift away from Information Technology and a major influx into Computer Systems Networking and Telecommunications and Management Information Systems. Computer Systems Networking increased from 32 to 237 awards from 2017 to 2019 and Management Information systems from only 2 to 92. Information Technology decreased from 242 awards to only 1.

Table 1

Cybersecurity Related Educational Programs and Number of Awards, 2019

CIP Code	Title	Certificates and 2yr Awards	4yr Awards	Postgraduate Awards	Total Awards
11.0101	Computer and Information Sciences, General	54	205	55	314

11.0901	Computer Systems Networking and Telecommunications	237	0	0	237
11.0201	Computer Programming/Programmer, General	112	0	0	112
52.1201	Management Information Systems, General	9	74	9	92
11.1003	Computer and Information Systems Security/Information Assurance	78	0	3	81
14.0901	Computer Engineering, General	5	54	0	59
11.0701	Computer Science	21	33	5	59
11.0301	Data Processing and Data Processing Technology/Technician	0	35	0	35
11.0802	Data Modeling/Warehousing and Database Administration	17	0	0	17
43.0116	Cyber/Computer Forensics and Counterterrorism	0	5	0	5
11.0801	Web Page, Digital/Multimedia and Information Resources Design	4	0	0	4
26.1103	Bioinformatics	0	0	2	2
11.1002	System, Networking, and LAN/WAN Management/Manager	0	2	0	2
11.0103	Information Technology	1	0	0	1
51.2706	Medical Informatics	0	0	1	1
	Total	538	408	75	1,021

Source: Jobs EQ

Numerous public and private post-secondary institutions across the state of Mississippi offer academic programs closely or indirectly aligned with knowledge and skill requirements of cybersecurity professionals. Seventeen academic programs were identified with core or fundamental content that could align with cybersecurity, and these programs of study occur at 32 public and private institutions.

Of these 32 institutions offering cybersecurity-related programs, the top 5 institutions accounted for about 60% of completions (see Table 2). Mississippi Gulf Coast Community College and Hinds Community College graduated 295 students (28% of total completions) with certificates or 2-year degrees in 2017 and 258 in 2019 (25% of total completions). Mississippi State University, The University of Southern Mississippi and The University of Mississippi graduated 345 students representing 33% of total completers in 2017 and 19% in 2019. These five institutions are geographically dispersed throughout the state and thus has potential to provide various educational services to the majority of Mississippi's commuter-dependent population.

Cybersecurity Completions decreased from 2017 to 2019 which can largely be attributed to the closure of Virginia College. Virginia college accounted for 45 completions or 4% of completions in 2017. It is worth noting; however, that the number of completions has not risen since 2017 to coincide with the increasing amount of job demand.

Table 2

Institutional Completions, 2017 vs. 2019

Institution	Number of Completions 2017	Number of Completions 2019
Mississippi Gulf Coast Community College	159	135
Hinds Community College	136	123
Mississippi State University	125	148
University of Southern Mississippi	123	95
University of Mississippi	96	98
Itawamba Community College	52	75
Jones County Junior College	45	32
Holmes Community College	38	43
Alcorn State University	31	15
Jackson State University	29	65
*Virginia College-Jackson	28	-
Copiah-Lincoln Community College	22	16
Northwest Mississippi Community College	21	19
East Mississippi Community College	21	30
*Virginia College-Biloxi	17	-
Mississippi College	15	20
Pearl River Community College	12	18
Delta State University	11	-
Mississippi Valley State University	11	9
Mississippi Delta Community College	9	-
Southwest Mississippi Community College	9	10

Institution	Number of Completions 2017	Number of Completions 2019
Northeast Mississippi Community College	8	-
East Central Community College	8	-
Meridian Community College	8	12
Antonelli College-Jackson	6	-
Rust College	5	8
Coahoma Community College	3	-
Tougaloo College	2	-
Antonelli College-Hattiesburg	2	-
Belhaven University	1	11
Strayer University-Mississippi	1	-
Millsaps College	0	-
	1,054	**1,016**

Source: EMSI, NCES
*Closed in 2018

It is worthy to note that Mississippi colleges and universities appear to use more generic CIP code classifications rather than more specific cyber-defined CIP codes for programs of study. The more generic classification may be necessary for a variety of reasons, but also may reduce the ability of prospective employers to gauge availability of a skilled workforce.

Mississippi's Educational Program Inventory

Jackson State University

The Department of Electrical & Computer Engineering and Computer Science offers a thirty-six credit hours master's degree. All students are required to pass the departmental Graduate Comprehensive Examination. Students can choose one of the three-degree options: Thesis, Project or Course-only option. Cybersecurity is offered as an area of emphasis.

Jackson State University has a four year, $6.0M research program under the Cooperative Research and Development Agreement (CRADA) entitled "Strategic Cyber Science, Warfare, Security, Application Development and High Performance Computing Research and Development (SCS)" with the U.S. Army Engineer Research and Development Center (ERDC). The CRADA is focused on conducting research in the areas of Computation and Data Enabled Sciences and Engineering, including the modeling of cyberspace (cyber warfare and security), improving high

performance computing applications using advanced machine architectures and data analytics.

Source: http://www.jsums.edu/compscience/

Mississippi College

Mississippi College debuted a new online graduate certificate in Cybersecurity and Information Assurance in the fall of 2017. The certificate in Cybersecurity and Information Assurance is designed to provide persons already involved in cybersecurity as well as information technology professionals desiring to be involved in cybersecurity, with the essential tools needed to identify, prevent, and mitigate cyber threats. Cybersecurity professionals will be on the front lines preventing cyber breaches and cyber-crimes. This certification complements the college's expertise in legal studies. The master's degree (10 courses) can be completed in five semesters. Classes are designed to help professionals broaden their understanding of cybersecurity issues.

Source: www.mc.edu/news/cybersecurity-program-introduced-mississippi-college

Mississippi State University

Mississippi State University was recently selected by the National Security Administration as one of four new schools to be a Center of Academic Excellence (CAE) in Cyber Operations. Mississippi State University also has cyber security capabilities that include three dedicated research centers: Center for Computer Security Research, the National Forensics Training Center, and the Critical Infrastructure Protection Center. MSU also holds national CAE designations in information assurance education and in information assurance research.

MSU Department of Computer Science and Engineering

The Department of Computer Science and Engineering is highly interactive, a research-intensive department offering undergraduate and graduate degrees in Computer Science, Software Engineering, Cyber Security and Operations, and Computer Engineering.

Computer Science	***Software Engineering***	***Cyber Security***
Bachelor of Science	Bachelor of Science	
Master of Science		Master (emphasis in Cyber Defense or Cyber Operations)
Doctorate		

The Department of Computer Science and Engineering cyber security and operations master's program is:

- One of the only degree programs in the Southeast to offer a cyber-defense and a cyber-operations concentration.
- Fixed on defeating the full spectrum of cyber-attacks, Mississippi State's NSF Cyber Corps program is the 3rd largest in the country.
- Recognized nationally for its leadership in cyber security, MSU is one of only nine schools in the U.S. to hold all three of the National Security Agency's centers of academic excellence credentials: CAE-Cyber Defense Education, CAE-Cyber Defense Research, and CAE-Cyber Operations.
- Via its nationally ranked cybersecurity program, MSU's M.S. in Cyber Security and Operations was selected by the U.S. Navy as a model curriculum.

Source: www.cse.msstate.edu/cyber-security/

MSU Center for Cyber Innovation (CCI)

"MSU supports one of the most robust cyber infrastructures of any university. CCI researchers have access to state-of-the-art high performance computing assets to include petabyte scale high-speed storage. CCI has the capability to scale up laboratory research into enterprise scale cyber demonstrations and to do so in NOFORN and other restricted environments."

Source: www.cci.msstate.edu/

MSU High Performance Computing

The High Performance Computing Collaboratory (HPC²), an evolution of the MSU NSF Engineering Research Center (ERC) for Computational Field Simulation, at Mississippi State University is a coalition of member institutes and centers that share a common core objective of advancing the state-of-the-art in computational science and engineering using high performance computing; a common approach to research that embraces a multi-disciplinary, team-oriented concept; and a commitment to a full partnership between education, research, and service.

As part of its education mission, the ERC has had approximately 700 students directly involved in the research of the Center, has developed a cross-disciplinary computational engineering graduate program to allow students to integrate their study with the research of the Center, has developed graduate and undergraduate CFS courses for engineering students and others, and has developed a minor in computational engineering for undergraduate engineering students. Working with the Department of Art and the School of Architecture, the ERC facilitated the new

graduate degrees in animation and electronic visualization (MS in art) and in electronic design (MS in architecture). The ERC has programs with minority and women's institutions and works with K-12 schools.

The HPC² is comprised of eight independent centers/institutes with the common characteristics of a multi-disciplinary, team-oriented effort that is strategically involved in the application and advancement of computational science and engineering using high performance computing.

- Alliance for System Safety of UAS through Research Excellence (ASSURE)
- Center for Cyber Innovation (CCI)
- Center for Computational Sciences (CCS)
- Geosystems Research Institute (GRI)
- Institute for Computational Research in Engineering and Science (ICRES)
    - Center for Advanced Vehicular Systems (CAVS)
    - CAVS Extension (CAVS-E)
    - Institute for Imaging & Analytical Technologies (I²AT)
    - Institute for Systems Engineering Research (ISER)
- Institute for Genomics, Biocomputing & Biotechnology (IGBB)
- Northern Gulf Institute (NGI)

Computational Engineering graduate program is a versatile program unique in its cross-disciplinary emphasis because the CME program does not reside within a single academic department or college, but within the High Performance Computing Collaboratory (HPC²). It offers the opportunity to pursue programs of study and research leading to the Master of Science degree and the Doctor of Philosophy degree.

Source: www.hpc.msstate.edu/

The University of Mississippi

The University of Mississippi's School of Law specializes in cyber law. Laws regarding cybersecurity of space assets, aviation and other critical infrastructure remain in their infancy. The Center for Air and Space Law supports research in this important topic and will continue to contribute to the ongoing dialog regarding best preventive practices and procedures. It is dedicated to:

- Developing the legal foundation to bridge humanity's evolution from a terrestrial to a spacefaring species.
- Developing and fostering the implementation of standards and procedures for advancing technologies that challenge current regulatory frameworks.
- Understanding and addressing cybersecurity issues in both aviation and space.
- Promoting rule of law as a benefit for nation-states and their commercial actors operating in air and space domains.

Source: http://airandspacelaw.olemiss.edu/

The University of Southern Mississippi

USM's School of Computing Sciences and Computer Engineering (CSCE) embraces its mission in research and graduate education (discovery), undergraduate education (learning), and outreach (engagement and economic development) in Computer Science, Engineering and Technology. CSCE offers a minor in Information Security and a certificate in Applied Cybersecurity. The CSCE cybersecurity faculty is complimented by an extensive set of adjunct instructors who are active in the cybersecurity profession in both the federal and state government and private sector. CSCE partners with the Mississippi Coding Academy (MCA) to provide cybersecurity skills development, and will launch a cyber-focused MCA site in Biloxi in 2021.

USM currently offers a Bachelor of Science in Applied Technology that provides students with leadership within organizations, project management skills, complex production processing, applied business skills, and the ability to leverage information technology. Students may also take a variety of cybersecurity courses, including those that earn them a certification in Applied Cybersecurity. This degree program is targeted to students enrolling from 2 year institutions and the military, enabling them to obtain an advanced degree and skills for the workforce.

USM is also involved with K-12 education programs, and collaborates closely with MSU's Bagley College of Engineering on some of these. USM has received funding from the NSA/NSF funded GenCyber program (https://www.gen-cyber.com), and has a special offering for K-12 wheelchair users. GenCyber provides summer cybersecurity camps for K-12 students and teachers. The aim of this program is to increase interest in cybersecurity fields and diversify the workforce, help students develop good online behaviors, and improve teaching methods within the field.

Alcorn State University

Alcorn State's School of Agriculture and Applied Sciences offers a Computer Networking and Information Technology (CNIT) program. This program is

designed to prepare students to design and maintain complex computing systems and diverse environments. The program is focused on delivering real-world experience and certification with common software such as Microsoft and Cisco.

Additionally, Alcorn State offers a variety of degrees in Mathematics and Computer Science degree through the School or Arts and Sciences. Degree programs include Bachelor of Science in Computer Science and Bachelor of Science in Mathematics with Data Science emphasis. There is also a Master's of Science in Computer and Information Science. The undergraduate degrees focus on equipping students with proficiency in programming languages, data mining, cyber security, and software engineering. The Master's program emphasizes the four key areas: artificial intelligence, cyber security, database management, and programming languages.

https://www.alcorn.edu/academics

Belhaven University

Belhaven University offers a variety of degrees and certificates in cyber security related fields. Belhaven offers both a degree in Computer Science and in Computer Information Systems. Both programs are Bachelor of Science undergraduate degrees. The Computer Science program areas of study include: programming fundamentals, data science, operating systems, and cyber security.

Computer Information Systems is a similar program to Computer Science. While the Computer Science focuses on why technology works, Computer Information Systems focuses on how technology works. This program is focused solely on practical applications of computing systems that help get work done. The Computer Information Systems program also offers minors in Web Application Development, and Management Information Systems. There also a variety of certificates offered in Web Application Development, Mobile Application Development, Cyber Security and Data Science.

https://www.belhaven.edu/academics/cis/index.htm

Mississippi Valley State University

Mississippi Valley State University offers a Bachelor of Science in Computer Science through their Mathematics, Computer and Information Sciences Department. There is also a Computer Science minor available to students wishing to enter the field. The Computer Science program offers three tracks: Computer Science, Cyber Security, and Information Science. The coursework for the Computer Science program involves software engineering, programming, and database management courses.

https://www.mvsu.edu/computer-science-information-science

Accreditation Board for Engineering and Technology (ABET)

In November 2018, ABET announced the approval of its first program-specific criteria for cybersecurity at the baccalaureate level. This newly established engineering-based accreditation could provide a guiding connection for Mississippi universities to align to this national standard. Programs at the U.S. Air Force Academy, U.S. Naval Academy, Towson University and Southeast Missouri State University earned the distinction of ABET accreditation under the newly adopted criteria. ABET accreditation provides assurance that a college or university program meets the quality standards of the profession for which that program prepares graduates. With more and more institutions developing undergraduate cybersecurity programs, the Computing Accreditation Commission (CAC) of ABET identified the need to establish cybersecurity as a formal academic discipline.

Source: https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/

Community Colleges

Mississippi's 15 public community colleges offer a variety of academic and technical programs that prepare workers beyond a high school diploma but less than a bachelorette degree. A total of 13 programs are offered by 34 community colleges at 39 locations (see Table 3). The mission of the community college system is to be responsive to local employer needs. This is evidenced by recent program approvals by the Mississippi Community College Board. Examples of this include a new Network Security Technology program for Copiah-Lincoln Community College in 2019 and a new Cyber Security Technology program at East Central Community College in 2017.

Copiah-Lincoln Community College

Copiah-Lincoln Community College (Co-Lin) offers an associate's degree in computer science through their Math and Computer Science Division. The program offers students an excellent student/instructor ratio, state-of- the-art equipment and personalized instruction. The courses included in the program focus on math and computer programming.

Beginning in the Fall of 2019, Co-Lin introduced a Cybersecurity Technology program. This new program is one of the many career and technical programs offered by the school. The program is focused on developing the skills necessary to work as a computer/network security technician such as confidentiality, integrity

and information security. The two-year program also equips graduates with the qualifications needed to obtain important certifications after graduation.

https://www.colin.edu/majors-programs/career-technical/information-systems-and-business/cybersecurity-technology/

East Central Community College

East Central Community College offers an associate's degree in computer science through their Math and Computer Science Division. The program offers students the option to focus on either math or computer science. The courses included in the program focus on math, computer programming and other key skills necessary to enter the field.

As one of their career and technical education programs, East Central offers both an Information Systems Technology program and Cybersecurity Technology program. The Information Systems Technology program offers students training in network administration, network security and client/server systems. The program is designed to help students find employment at financial institutions, hospitals and state and local governments as network technicians, network administrators, etc. The Cybersecurity Technology option provides students with current knowledge and skills related to the cybersecurity field. This program focuses on identifying vulnerabilities, problem solving, and cyber prevention. Students in this program have the opportunity to obtain important certifications after graduation from the program.

https://www.eccc.edu/information-systems-technology

Hinds Community College

Hinds Community College offers an associate's degree in Computer Science. The curriculum offers a variety of courses including microcomputer applications, programming in various languages, and database management. There are a variety of options available to students to attend classes at the various campuses and online.

Hinds Community College has a number of technical programs available related to cyber security. The programs include computer networking, computer programming and cyber security. The cyber security program offers training to students in confidentiality, integrity and information security. The program is offered only at the Ranking campus and teaches students to install, design, and manage secure information technology infrastructure.

https://www.hindscc.edu/programs-of-study/career-technical/cyber-security

Jones College

Jones College offers an associate's degree in computer science through their division of Business and Technology Services. This program is designed to prepare students to achieve a Bachelor's degree in computer science related fields in the future. Students gain experience in computer programming, math, and physics.

Jones College offers a Computer Networking Technology program through the Information Systems Technology department. This department has partnerships with several large companies such as Cisco and Microsoft. The Computer Networking program is a two-year program that offers training in network design, operating systems, and client/server systems. Graduates of this program have the option to obtain cybersecurity related certificates after completion.

https://www.jcjc.edu/programs/informationtech/

Mississippi Gulf Coast Community College

Mississippi Gulf Coast Community College offers a number of academic and technical programs related to Cybersecurity at its campuses. The Harrison County Campus offers a Computer Networking Technology program that provides students with course work related to installation, maintenance, and networking of Local and Wide Area Configurations. The Harrison County Campus also offers a Cybersecurity Technology program. This program is designed to teach students skills to prevent threats to information, recognize threats, and master defense techniques. Each of these programs leads to an Associate of Applied Science Degree and prepares students for employment upon graduation. Mississippi Gulf Coast Community College also offers several associate degree opportunities with programs in computer science, computer programming, coding, data analytics, information science, simulation and game design, and computer engineering.

https://mgccc.edu

Meridian Community College

Meridian Community College has two major technical programs related to cyber security. One is the Network Security Technology program which is a two-year program that offers training in cyber security and network administration. Students also receive instruction in client/server systems. Students earn an Associate of Applied Science upon completion of the program. This program is designed to prepare graduates for careers in fundamentals of data communications, network security, network implementation, and system maintenance.

Meridian Community College also offers a program in Coding Technology. This program is designed to prepare students for jobs in the programming field. The goal is to provide in instruction in both traditional and web-based programming.

Students in the program receive training in computer operations management, web development and systems analysis. An Associate of Applied Science is earned upon completion of the program.

https://www.meridiancc.edu/programs/career_and_technical_programs/division_of_business/index.html

Table 3

Programs offered at Community Colleges

	Career/Technical Program	# of Community Colleges	# of Locations
Information Systems Technology	Computer Information Systems, Software Engineering	1	1
	Computer Network Support Technology	3	4
	Computer Network Support Technology, Wide Area Network	1	1
	Computer Network Technology	1	1
	Computer Networking Support	1	1
	Computer Networking Support Technology	1	1
	Computer Networking Technology	4	4
	Cyber Security (Network Security Technology)	1	1
	Computer Programming Technology	9	13
	Computer Servicing Technology	1	1
	Cybersecurity Technology	1	1
	Information Systems Technology	2	2
	Network Security Technology	6	7
	Database Administration Technology	1	1
Computer Servicing Technology	Computer Networking/Servicing Technology	1	1
	Computer Servicing Technology	2	2
	Electronics and Related Engineering Technology- Computer Servicing Technology	1	1
Cybersecurity	Cybersecurity Technology	1	1

Source: MS Community College Board CTE Program

Coding Academies

Base Camp Coding Academy

Base Camp Coding Academy began in 2016 in Water Valley, Mississippi with a $500,000 start-up investment championed by the FNC Incorporation and C-Spire Foundation, CoreLogic and other philanthropists. The Academy is a place where local high school graduates attend school for free, 40-hours a week, for an entire year and learn the skills necessary for an entry level job as a developer.

Source: https://mississippitoday.org/2017/03/10/high-school-grads-code-their-way-to-tech-jobs/#

Mississippi Coding Academies

Mississippi Coding Academies (MCA) are a project of Innovate Mississippi and sponsored in part by Mississippi Development Authority, Mississippi State University, and several corporate partners. They operate in two locations with the goal of offering "a non-traditional path to create new and diverse software professionals." The project is focused particularly on disadvantaged and underserved communities.

The Jackson-based academy is in downtown Jackson in the center of the emerging "innovation hub" on State Street near the Old Capitol Museum. The Golden Triangle Campus-based academy is located in Starkville, MS.

MCA recently opened two remote classrooms for coders in collaboration with the Columbus Municipal School District and the Mississippi Band of Choctaw Indians. This was made possible by the TechShare program which is funded by a USDA grant and Appalachian Regional Commission (ARC) support. The goal of these new classrooms is to connect rural communities with instructors at the Jackson and Starkville campuses.

Source: https://mscoding.org/

High School Initiatives

Three benchmark initiatives introduce students to the world of cyber education and serve as pilot programs for high school students. These include the GirlsGoCyberStart initiative, C-Spire Software Development Pathway, and Keesler Air Force Base's Duck-Con Seminar.

Girls Go Cyber Start

In 2018, GirlsGoCyberStart became a new innovative cybersecurity training partnership between the SANS Institute and the state of Mississippi. This

training is a free online game where every Mississippi high school girl can discover her talents in cybersecurity and learn about the field.

"The GirlsGoCyberStart program is an excellent and fun opportunity for students who think they may be interested in cybersecurity to determine if they have the passion and aptitude to pursue it as a career," said Governor Bryant.

Students from Mississippi who excel in the GirlsGoCyberStart game will have the opportunity to win prizes and complete in national competitions.

Source: www.wtok.com/content/events/469362503.html

C Spire Software Development Pathway

Mississippi State University's newest K-12 cyber education initiative was launched and targeted both teachers and high school students. The Center for Cyber Education will build upon the MSU Research and Curriculum Unit's longstanding work in K-12 computer science education, teacher training and teacher recruitment. Its first project is the C Spire Software Development Pathway.

The $550,000 program, which will be fully funded in the first year and partially funded the second and third years by C Spire, will train 30 teachers. It will also support computer science job opportunities for 150 students from selected schools after two years of specialized course work in high school and one year community college.

Source: www.rcu.msstate.edu/Communications/Newsroom/CCE.aspx

Keesler Air Force Base High School Duck-Con Seminar

The 333rd Mad Ducks from Keesler Air Force Base conduct seminars for area high school students on concepts such as coding, password selection, and wireless technology security. Duck-Con featured five specialized seminars for students with plans to expand the program to other area schools in the future.

Source: http://www.wlox.com/story/38005924/keesler-promotes-cyber-security-careers-to-high-school-students/

Cybersecurity Conferences, Workshops, and Forums

There are several reoccurring events and meetings hosted around Mississippi pertaining to cyber security. This is not an exhaustive list but rather a summary of the events identified during the desktop review process.

- BSidesJackson - Targeted cyber security enthusiasts for a day of presentations, workshops and trainings conducted by local professionals and professors.

- Mississippi Annual Cybersecurity Summit - Government officials and academics convene every October at Jackson State University's Mississippi e-Center to discuss security awareness.
- Mississippi Digital Government Summit - This event informed state government managers from non-tech backgrounds about IT issues such as computer security.
- Jackson Area Web and App Developers - A networking group that meets monthly
- JXNtech: Meets monthly to discuss entrepreneurial endeavors in the capital's tech community
- Mississippi InfraGard - Joining InfraGard entails an FBI background check due to members working with the FBI to protect Mississippi's physical and virtual infrastructure from malicious hacks.
- Mississippi College Cybersecurity Summit - The annual Mississippi College Cybersecurity Summit is designed to engage, educate, and raise awareness about cybersecurity across the nation. The 2019 Summit was held on 10 April 2019. Topics included: Cybersecurity Best Practices, Financial Inclusion, Artificial Intelligence, Internet of Things, Cyber Insurance, Reputation Management, Cryptojacking and Biometric Breaches.
- University of Southern Mississippi – Gulf Park Campus hosted a discussion on cybersecurity and cyberattacks as a free and open public forum with keynote speaker, Major Jason C Hillman, cyber strategist at the U.S. Army Cyber Institute.

Cyber related instructional programs are a promising, yet undeveloped pipeline in Mississippi's economy. While there is a slow and steady growth in the region for cyber related occupations, academic institutions should be encouraged to recruit more students to fill the 22% gap in meeting the job demand through 2023. This should happen concurrently with these same institutions making a push to achieve high completion rates in order to reduce the 60% dependency rate it currently has on the Top 5 performing institutions producing graduates. Lastly, each instructional program should be encouraged to use the U.S. Department of Education's National Center for Education Statistics' Classification of Instructional Programs (CIP) codes to accurately track, assess, and report the newly identified 6-digit CIP codes relating to cybersecurity. This will allow cybersecurity programs to be formally adopted by colleges and universities across the nation.

LABOR DEMAND

This section of the report studied labor demand anticipated by Mississippi employers for cybersecurity professionals through the year 2023. Overall, the cybersecurity market is growing, and the trickle effect is anticipated to have positive job growth for Mississippi. It is arranged from the broadest cybersecurity market trends in the United States; followed by types of industry sectors that employ cyber professionals; and then by occupation trends within those industry sectors.

Cybersecurity Market Trends through 2023

The national demand for cybersecurity professionals was investigated to determine the types of employers needing talent including public-sector, private employers and defense personnel. The North American cyber security market should grow from $51.6 billion in 2018 to $82.5 billion by 2023 at a compound annual growth rate (CAGR) of 9.8% (see Table 4). Banking, financial services and insurance market sectors should grow from $12.8 billion to $20.8 billion during the same timeframe, a CAGR of 10.3%. Similarly, telecommunications and information technology markets should grow from $9.3 billion to $15.6 billion, a CAGR of 10.8% (BCC Research, Cyber Security: North American Markets).

Table 4

North American Cyber Security Market, by Industry Vertical, Through 2023
($ millions)

Industry Vertical	2018	2023	CAGR% 2018–2023
Banking, financial services and insurance (BFSI)	12,781.80	20,835.60	10.3
Government	10,573.00	17,397.40	10.5
Telecom and IT	9,316.60	15,591.70	10.8
Retail	4,928.10	7,775.20	9.5
Defense and intelligence	5,472.60	7,503.10	6.5
Healthcare	4,372.40	7,024.90	9.9
Others	4,177.50	6,324.10	8.6
Total	**51,622.00**	**82,452.00**	**9.8**

Source: BCC Research

Trends in Cyber Security Sub-Markets

The market breakdown of types of cyber security include: network security, endpoint security, wireless security, content security, cloud security, and application security. Cloud security is expected to grow the highest percentage rate at 12.8% by 2023 followed by Wireless security at 10.9% (see Table 5).

Table 5

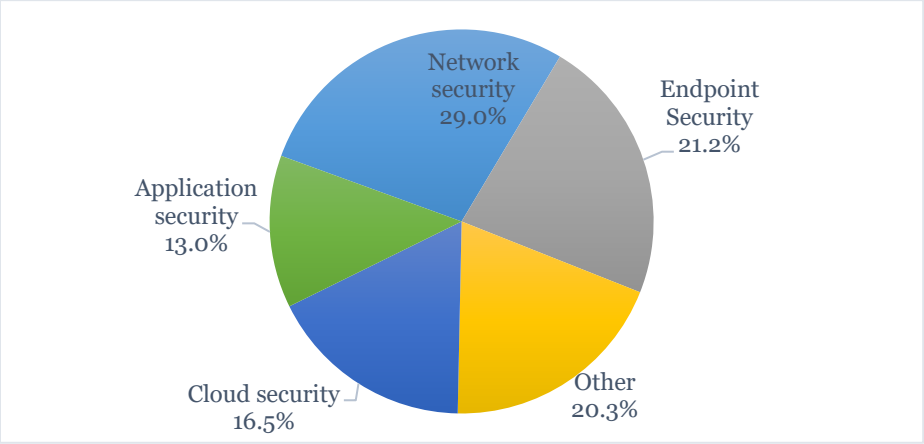
North American Cyber Security Sub-Market, by Type, Through 2023 ($ millions)

Types of Sub-markets	2017	2018	2023	CAGR% 2018–2023
Network security	$20,909.00	$22,806.90	$34,662.80	8.7
Endpoint security	8,549.70	9,455.80	15,377.30	10.2
Wireless security	6,016.30	6,697.60	11,254.70	10.9
Content security	4,977.20	5,474.00	8,657.50	9.6
Cloud security	3,325.90	3,764.10	6,868.20	12.8
Application security	3,065.80	3,423.60	5,631.50	10.5
Total	**46,843.90**	**51,622.00**	**82,452.00**	**9.8**

Source: BCC Research

Of the total North American market, Network Security currently is the largest sub-segment at 29.0% of the total cyber security market (see Figure 3), but it is anticipated to grow more slowly at 8.7% than other sub-segments.

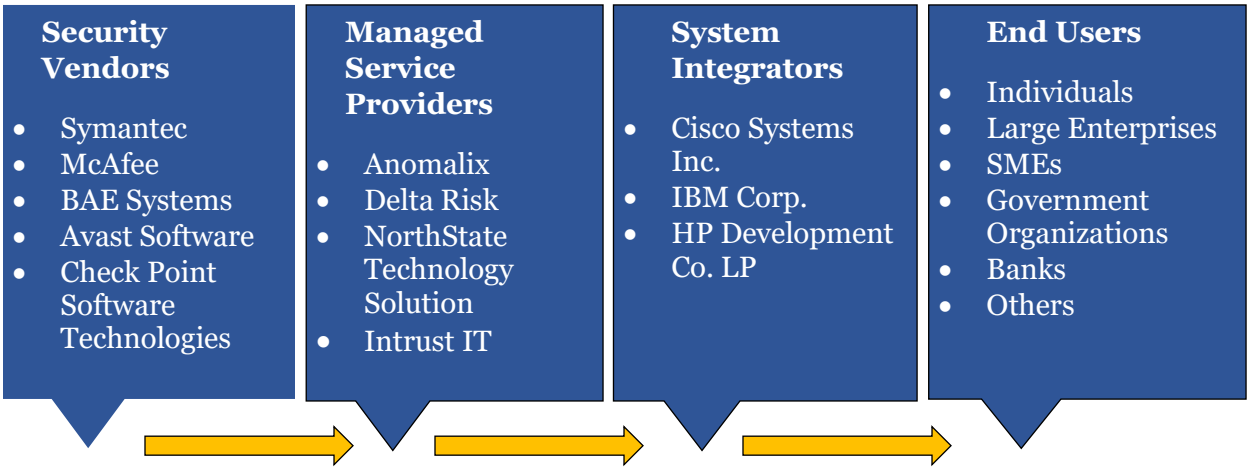
Figure 3. USA Cyber Security Market Shares by Type



Source: BBC Research

Market segments of cyber security exist as a supply chain of related activity ranging from 'upstream' security vendors like Symantec and McAfee to 'downstream' end users like individuals, banks, government and others (see Figure 4).

Figure 4: Cyber Security Ecosystem



Industry Sectors Supporting Cybersecurity Occupations

Eight industry sectors were identified as the most common in employing cyber professionals. These are defined by North American Industry Classification Code (NAICS) and can be further studied to determine quantities and types of occupations inclusive of cybersecurity (see Table 6). Additional descriptions for these industry sectors are provided in Appendix A. Because cybersecurity occupations have a presence in a wide variety of industry sectors, it was important to identify which of those sectors have a larger concentration of cyber jobs.

Mississippi is a rural state and contains a smaller share of its total population employed in cyber-related jobs as compared to the nation. This concentration of occupations in a given population can be measured using a *Location Quotient* (LQ) ratio. The average LQ for cyber-related industries and occupations in Mississippi is 0.37 and 0.41, respectfully, compared to the nation's LQ of 1.0. The state is, therefore, less likely to have a specialization in cybersecurity as compared to the nation.[1]

[1] A location quotient of 1.0 means that the region and the nation are equally specialized; while an LQ higher than 1.0 means that the region has a higher concentration. This also has the adverse meaning for LQs lower than 1.0, which means that there is no regional specialization.

Table 6

NAICS codes for industries closely aligned with cybersecurity

NAICS	Description	2017 Location Quotient	2019 Location Quotient
518210	Data Processing, Hosting, and Related Services	0.34	0.32
541511	Custom Computer Programming Services	0.21	0.19
541512	Computer Systems Design Services	0.46	0.48
541513	Computer Facilities Management Services	0.41	0.38
541611	Administrative Mgmt. and General Mgmt. Consulting Services	0.13	0.14
541618	Other Management Consulting Services	0.10	0.09
541690	Other Scientific and Technical Consulting Services	0.69	0.74
561621	Security Systems Services (except Locksmiths)	0.59	0.59

Source: EMSI, Industry Table

Mississippi is anticipated to outpace the nation between 2018 and 2023 in *competitiveness effect* particularly in two of the eight industry sectors studied: Computer Systems Design Services (NAICS 541512) and Other Scientific & Technical Consulting Services (NAICS 541690) with competitiveness measures of 276 and 179, respectively.[2] Additionally, these eight industry sectors pay average annual earnings of $75,665 which is well above the state's average. Contrary, however, Mississippi is anticipated to be less competitive in Custom Computer Programming Services (NAICS 541511) and Administration Management and General Management Consulting Services (NAICS 541611) with competitiveness values of -130 and -158, respectively (EMSI, Industry Table, 2018 to 2023). The higher positive value means the more competitive a region is likely to perform compared to the nation (see Table 7).

There were an estimated 2,509 payrolled businesses in these eight industry sectors in Mississippi in 2018, with Computer Systems Designs Services total nearly half at 1,206 businesses. Its growth rate of 22% is anticipated through 2023 with average annual earnings of $80,081 offering positive indicators of growth potential for the state. The eight industry sectors' combined increase of 14% growth in jobs will add an estimated 1,362 additional jobs in the state through 2023.

[2] Competitiveness Effect, also known as shift share analysis, is a measure that isolates regional-specific growth from other growth effects occurring by the nation or by the industry sector.

Table 7

Industry Comparison, 2018-2023

NAICS	Description	Competitive Effect	2018 - 2023 Change	2018 - 2023 % Change	2018 Jobs	2023 Jobs	Avg. Earnings Per Job	2018 Payrolled Business Locations
541512	Computer Systems Design Services	276	837	22%	3,890	4,727	$80,081	1,206
541690	Other Scientific and Technical Consulting Services	179	278	21%	1,315	1,593	$66,349	431
541618	Other Management Consulting Services	12	19	23%	84	103	$70,538	23
541513	Computer Facilities Management Services	1	49	19%	255	304	$64,449	16
561621	Security Systems Services (except Locksmiths)	(4)	55	9%	620	675	$47,610	78
518210	Data Processing, Hosting, and Related Services	(38)	55	6%	863	918	$70,710	98
541511	Custom Computer Programming Services	(130)	93	6%	1,635	1,728	$91,428	397
541611	Administrative Management and General Management Consulting Services	(158)	(26)	(3%)	773	747	$68,251	261
	Total	**139**	**1,362**	**14%**	**9,434**	**10,796**	**$75,665**	**2,509**

Source: EMSI, Industry Table, 2018 to 2023 Comparison

Occupation Outlook

Across all industry sectors in Mississippi, there were an estimated 24,058 total cyber related jobs in 2018, up from 2012. These occupations are anticipated to continue to grow by 7.7% through 2023 to 25,903, as compared to the nation's slightly higher growth of 9.5%. Education Pipeline reports from EMSI show 1,845 new jobs will be added through 2023. Job posting announcements indicate an average annual number of job openings are anticipated to be approximately 2,254, representative of attrition, job promotions, and other job-transition reasons. This represents slightly more demand for workers than academic programs are completing, 2,254 openings versus 1,054 completions.

Across all industry sectors, the highest percentage increases in occupations were found in Software Developers, Application (SOC 15-1132) and Market Research Analysts (13-1161) with percentage changes of 22% and 13%, respectively *(see Table 8)*. Occupations for Computer Programmers (15-1131) and Computer Network Architects (15-1143) are anticipated to remain stagnate or decline slightly.

Table 8

Occupation Comparison between Mississippi and United States, 2018-2023

		Mississippi					United States	
Standard Occupation Code	Description	2018 Jobs	2023 Jobs	2018 - 2023 Change	2018 - 2023 % Change	Annual Openings	2023 Jobs	2018 - 2023 % Growth
11-3021	Computer and Info Sys Mgrs	1,360	1,453	93	7%	121	426,220	9%
13-1111	Management Analysts	2,201	2,363	162	7%	227	937,125	8%
13-1199	**Business Operations Specialists, All Other**	**3,702**	**3,973**	**271**	**7%**	**396**	**1,116,444**	**6%**
13-1161	Mrkt Research Analysts and Specialists	2,081	2,361	280	13%	266	742,019	14%
15-1121	**Computer Systems Analysts**	**2,275**	**2,398**	**123**	**5%**	**177**	**664,311**	**7%**
15-1122	**Information Security Analysts**	**436**	**489**	**53**	**12%**	**42**	**135,636**	**15%**
15-1131	**Computer Programmer**	**960**	**953**	**(7)**	**(1%)**	**66**	**270,803**	**0%**
15-1132	Software Developers, Applications	1,243	1,519	276	22%	142	1,068,467	17%
15-1133	**Software Developers, Systems Software**	**1,051**	**1,143**	**92**	**9%**	**89**	**452,611**	**8%**
15-1134	**Web Developers**	**629**	**682**	**53**	**8%**	**57**	**185,677**	**10%**
15-1141	**Database Admin**	**525**	**551**	**26**	**5%**	**40**	**131,743**	**8%**
15-1142	**Network and Computer Systems Admin**	**1,595**	**1,663**	**68**	**4%**	**117**	**415,874**	**6%**
15-1143	**Computer Network Architects**	**800**	**807**	**7**	**1%**	**57**	**176,043**	**5%**
15-1151	Computer User Support Specialists	3,125	3,345	220	7%	280	770,611	8%
15-1152	**Computer Network Support Specialists**	**1,059**	**1,109**	**50**	**5%**	**91**	**225,293**	**6%**
15-1199	**Computer Occupations, All Other**	**1,016**	**1,093**	**77**	**8%**	**86**	**379,528**	**7%**
	TOTAL	**24,058**	**25,903**	**1,845**	**7.7%**	**2,254**	**8,098,405**	**9.5%**

Note: Occupations in **bold print** represent those referenced in the NICE Cybersecurity Workforce Framework
Source: EMSI Occupation Report

Mississippi has one of the nation's fewest numbers of cyber-related professionals encompassing 24,058 in 2018. However, the anticipated increase of occupation growth of 7.7% will outpace the state's expected job growth of 3% through 2023.

Mississippi Employers in Cybersecurity

An inventory of Mississippi employers which appear to employ cyber security professionals among its workforce was compiled to identify company name, location, website address, and description of services (see Appendix B). These companies promote the ability to conduct cyber-related work or possess cyber-related expertise. These companies were identified from desktop internet searches using keywords to connect to company-owned websites. This inventory of companies will be updated as new information becomes available.

Mississippi Cyber Initiative

Modeled after the Georgia Cyber Center in Augusta, the Mississippi Cyber Initiative (MCI) will create a statewide ecosystem to address cybersecurity issues in the State and for our nation. MCI's mission will be to provide state-wide leadership that prepares Mississippi's future economy through unparalleled collaboration and innovation in cybersecurity.

The MCI will focus on three missions: (1) meet the cybersecurity training needs at Keesler Air Force Base, (2) provide statewide leadership in addressing cybersecurity and workforce needs for Mississippi into the future, and (3) attract innovative cyber and advanced technology industries.

The goals of the MCI are to: (1) promote economic development for the Gulf Coast region and the State, (2) deliver timely cybersecurity workforce training and education, (3) address complex cybersecurity issues for the State, and (4) increase public awareness through outreach.

The MCI will execute the mission through a multi-disciplinary approach utilizing powerful collaborations, education, infrastructure, and real-world applications to advance innovation and produce real-world solutions.

The MCI is a statewide effort led by Mississippi State University (MSU) with implementing partners from Keesler Air Force Base (Keesler AFB), Mississippi Gulf Coast Community College (MGCCC), and the University of Southern Mississippi (USM). Keesler AFB has direct responsibility for training the Air Force and Department of Defense's cyber force and as a key partner, anchors this initiative and creates a unique opportunity for our state, region, and nation. MSU is the state's leading university for cyber education, technology, and research. MGCCC has well established cyber and IT academic and certification programs essential in preparing a cyber workforce and the leading provider of workforce training and education in the gulf coast region. University of Southern Mississippi (USM) also has a growing cyber program and will play a key role utilizing well established partnerships across the state associated with the Mississippi Defense Initiative (MDI).

While the lead implementing partners are tasked with jump starting the MCI, success will be based on strong partnerships and collaboration among all stakeholders by leveraging the collective expertise among academia, the private sector, state, federal and local government, law enforcement, Department of Defense, and MS National Guard.

The MCI will be headquartered in a new, state-of-the-art facility located in Biloxi, adjacent to Keesler AFB, known as the Mississippi Cyber Technology Center (MCTC). The MCTC will serve as the heart of the statewide MCI ecosystem. The second key location will be on the MGCCC Harrison County campus. Having the MGCCC location creates unique opportunities for meeting training requirements at Keesler AFB. In addition to these foundational sites, the MCI ecosystem will connect current and future physical assets and human capital throughout the State that belong to partners and collaborators.

The MCTC will offer the full scope of services necessary to prepare the workforce and address partner cyber challenges. As the headquarters for the Mississippi Cyber Initiative, the MCTC becomes a hub for constantly updating and developing curricula to meet training and professional development requirements of stakeholders. It will include space to house a state-of-the-art cyber range allowing stakeholders to practice cyber defense, operations, and research that is not possible in 'live' computing environments. The facility will also have a Secured/Controlled space to hold sensitive information, conduct advanced training and education, and allow collaboration on the most current cyber threats and mitigation efforts facing all stakeholders. It will also serve as a technology incubator for private sector development.

As the MCI concept moves into the execution phase more opportunities will be identified. Again, the success of the MCI will be based on strong partnerships and collaboration among all stakeholders. As the MCI matures, capabilities and vulnerabilities from across the state will be captured. Working together, the MCI

collaboration will focus on leveraging statewide capabilities to strengthen cyber security, promote innovation and opportunity, while addressing the workforce development needs of the state.

CONCLUSION

Cyber related instructional programs are a promising, yet undeveloped asset for Mississippi's economy. There is a slow and steady growth in the region for cyber related occupations so academic institutions should be encouraged to recruit more students to fill the 22% gap in the anticipated job demand through 2023. Since five institutions in the state currently account for about 60% of the cyber completions, more institutions should be encouraged to develop cyber programs. Lastly, each instructional program should be encouraged to use the U.S. Department of Education's National Center for Education Statistics' Classification of Instructional Programs (CIP) codes to accurately track, assess, and report the newly identified 6-digit CIP codes relating to cybersecurity. This will allow cybersecurity programs to be formally adopted by colleges and universities across the nation.

All suspected cybercrimes should be reported to the FBI, as they are best equipped to properly handle the investigation and prosecution of cyber criminals. Many public sector agencies are monitored by the Mississippi Department of Information Technology Services (ITS). It is heavily recommended that all private sector companies maintaining personally identifiable information (PII) have a cyber insurance policy.

References

Berente,N.,Howison, J.,King, J.L.,Ahalt,S.,Winter,S. (2018). Organizing the Cyberstructure Workforce. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3260715

California: Building a Supply Chain for Cyber Skills https://businessfacilities.com/2017/01/california-building-a-supply-chain-for-cyber-skills/

Certifications https://help.comptia.org/hc/en-us/articles/360000036626-What-to-Know-About-Stackable-Certifications-

Cyber Degrees https://www.cyberdegrees.org/listings/mississippi/

Cyber Jobs www.cyberseek.org

DOE Intends to Fund Establishment of Energy Manufacturing Cybersecurity Institute https://blog.executivebiz.com/2017/02/doe-intends-to-fund-establishment-o-energy-manufacturing-cybersecurity-institute/

High School Grads https://mississippitoday.org/2017/03/10/high-school-grads-code-their-way-to-tech-jobs/#

Information Assurance and Cyber Security Degrees in Mississippi: https://cybersecuritydegrees.com/degrees-by-state/mississippi/

National Institute of Standards and Technology. DFARS Cybersecurity Requirements. https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance

NICE Cybersecurity Workforce Framework: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Scott, J. & Spaniel, D. (2016). *China's Espionage Dynasty: Economic Death by a Thousand Cuts*. Institute for Critical Infrastructure Technology.

U.S. Bureau of Labor Statistics - https://www.bls.gov/ooh/computer-and-information-technology/computer-programmers.htm#tab-6

U.S. Department of Defense. Cybersecurity Strategy. https://www.defense.gov/explore/story/Article/1648425/dods-cyber-strategy-5-things-to-know/

U.S. Department of Labor. Cybersecurity Competency Model. www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

We Are Social, "2018 Global Digital Suite of Reports", New York, New York.

What is cybersecurity? https://one.comodo.com/blog/cyber-security/what-is-cyber-security.php

Appendix A

North American Industry Classification System Number and Description

NAICS	NAICS Description
518210	**Data Processing, Hosting, and Related Services** This industry comprises establishments primarily engaged in providing infrastructure for hosting or data processing services. These establishments may provide specialized hosting activities, such as Web hosting, streaming services, or application hosting (except software publishing), or they may provide general time-share mainframe facilities to clients. Data processing establishments provide complete processing and specialized reports from data supplied by clients or provide automated data processing and data entry services.
541511	**Custom Computer Programming Services** This U.S. industry comprises establishments primarily engaged in writing, modifying, testing, and supporting software to meet the needs of a particular customer.
541512	**Computer Systems Design Services** This U.S. industry comprises establishments primarily engaged in planning and designing computer systems that integrate computer hardware, software, and communication technologies. The hardware and software components of the system may be provided by this establishment or company as part of integrated services or may be provided by third parties or vendors. These establishments often install the system and train and support users of the system.
541513	**Computer Facilities Management Services** This U.S. industry comprises establishments primarily engaged in providing on-site management and operation of clients' computer systems and/or data processing facilities. Establishments providing computer systems or data processing facilities support services are included in this industry.
541611	**Administrative Management and General Management Consulting Services** This U.S. industry comprises establishments primarily engaged in providing operating advice and assistance to businesses and other organizations on administrative management issues, such as financial planning and budgeting, equity and asset management, records management, office planning, strategic and organizational planning, site selection, new business start-up, and business process improvement. This industry also includes establishments of general management consultants that provide a full range of administrative, human resource, marketing, process, physical distribution, logistics, or other management consulting services to clients.
541618	**Other Management Consulting Services** This U.S. industry comprises establishments primarily engaged in providing management consulting services (except administrative and general management consulting; human resources consulting; marketing consulting; or process, physical distribution, and logistics consulting). Establishments providing telecommunications or utilities management consulting services are included in this industry.
541690	**Other Scientific and Technical Consulting Services** This industry comprises establishments primarily engaged in providing advice and assistance to businesses and other organizations on scientific and technical issues (except environmental).
561621	**Security Systems Services (except Locksmiths)** This U.S. industry comprises establishments primarily engaged in (1) selling security alarm systems, such as burglar and fire alarms, along with installation, repair, or monitoring services or (2) remote monitoring of electronic security alarm systems.

Appendix B

Mississippi Employers with Cybersecurity Services or Expertise

Company	Location	Website	Description of Services
BeyondTrust	Ridgeland	Beyondtrust.com	BeyondTrust (formally Bomgar Corporation) is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access. Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralized management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments. BeyondTrust give organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 100, and a global partner network.
BKD	Jackson	Bkd.com	The BKD Cyber team can help you develop a plan to protect against unforeseen attacks. BKD is ready to assist with: Cyber Risk Assessment; Penetration Testing; Access Analyzer; Regulatory Compliance; Incident Response; BKD Red Team; BKD WhiteHat Services; SOC for Cybersecurity; Payment Card Industry (PCI) Compliance
Circadence	Tupelo	Circadence.com	Powered by a culture of innovation and the demands of an evolving cyber landscape, Circadence offers cyber range solutions and cybersecurity learning platforms that leverage artificial intelligence and custom content to address critical security challenges for enterprise, government, and academic institutions. Our unique approach to cybersecurity learning stems from the power of gamification and active-learning models. These strategies are then amplified by our leading-edge capabilities that leverage Artificial Intelligence, Natural Language Processing, and Machine Learning to augment and automate the cybersecurity capabilities of our customers. Advancements in data science further elevate our autonomous systems, which augment cyber workforces and alleviate industry challenges. *Project Ares* (Software solution)-Project Ares is a "gamified" product created by Circadence that allows cyber teams from across enterprise, government, and

Company	Location	Website	Description of Services
			academic institutions to automate and augment the cyber workforce by providing immersive, gamified cyber range learning environments that emulate company networks. Realistic scenarios engage teams in immersive, mission-specific virtual environments using real-world tools, network activity and a large library of authentic threat scenarios. This software can be used to enhance the academic training within coding academies and academic institutions who offer cybersecurity related programming.
C-Spire	Ridgeland		C Spire's security team has more than 30 years of experience partnering with companies across multiple industries to make their environments more secure and meet compliance regulations. • Cybersecurity Testing & Consulting • Assurances & Certifications • Security-as-a-Service
Defense Point Security	Kiln	Defpoint.com	Defense Point Security has the proven track record and expertise to perform all needed Computer Network Defense (CND) capabilities. Our knowledgeable staff of security analysts have experience in performing monitoring, analysis, and incident response capabilities for a wide range of customers. DPS understand the Cyber Security challenges faced by our customers, particularly pertaining to the ever-present threat landscape that has continually increased over the past several years. DPS has the operational and management expertise needed to provide 24x7x365 support for all Security Operation Center (SOC) responsibilities, including a specialized focus in the following areas: • Monitoring and Analysis • Incident Response • Malware Analysis • Crowd Sourced Intelligence Our CND capability also includes providing vulnerability assessment and other key security operations focused services.
Horne Cyber	Ridgeland and Starkville	Hornecyber.com	Horne's anticipatory cyber resilience services help minimize the impact of these vulnerabilities on your organization in the future. By taking an offensive approach to cybersecurity, they are able to collaborate with their client's IT team to strengthen their cyber resilience and protect their organization from the negative impacts of a cyber-incident. An overview of Horne's cyber resilience building services include:

Company	Location	Website	Description of Services
			Advanced Penetration Testing, Digital Forensics, Incident Response, Industry Regulatory Compliance, IT Governance, Risk, and Compliance, Managed Threat Hunting, SOC Suite of Services, M&A IT Services, Threat Hunting.

Pileum Corporation	Jackson		PILEUM network security services feature our expertise in the area of network security, threat, and vulnerability assessments to help our clients by providing practical, cost-effective solutions to safeguard vital information.
			• Security and Risk Architecture Development
			  ○ Initiate or advance cybersecurity risk management (e.g. NIST, COBIT, ISO, etc.)
			  ○ Address regulatory compliance gaps (e.g. PCI-DSS, HIPAA, IRS1075, SOC2, etc.)
			• Risk Assessments
			• Maturity Assessments, Readiness Reviews and Gap Analysis
			• Technical Security Assessments (Vulnerability and PEN Testing, Application Security Assessment, Ethical Hacking, etc.)
			• Business Impact Analysis, Business Continuity Planning and Disaster Recovery Planning
			• Security Incident Response Planning

Schellman	Jackson	Schellman.com	All of Schellman's services are centered on independent assessments or readiness based on specific industry standards. They do not and will not provide management consulting, implementation, technology, or managed services that would present themselves with any self-serving motive or conflicting interest other than serving our clients with the highest independence and quality. In April of 2017, the AICPA introduced its cybersecurity risk management reporting framework as an essential addition to the System and Organization Controls (SOC) suite of service offerings. SOC for Cybersecurity reports include a description of your cybersecurity risk management program and a set of benchmarks that we will evaluate your program against. SOC for Cybersecurity reports are designed to help organizations communicate meaningful information about the effectiveness of their cybersecurity risk management program and controls, in the form of a CPA firm's independent attestation report. SOC for Cybersecurity report users may include senior

Company	Location	Website	Description of Services
			management, boards of directors, analysts, investors and business partners.
UIC Government Services	Vicksburg	Bowheadsupport.com	Headquartered in Alexandria, VA, UIC Government Services established an office in Vicksburg, MS and structured an Information Technology team that uses methodologies, frameworks, and processes, such as ITIL, RMF, CMMI to gain efficiencies and high productivity. We begin with people that are dedicated and passionate about their profession – people who stay abreast of current technology trends, have deep knowledge of various tools and products, and have the ability to be vendor neutral when looking for solutions that best meet customer requirements. In addition, their people must be a cultural fit with the company and their customers, working together as a team to solve IT issues from the most complex down to the most mundane. Cyber Security capabilities: • Cybersecurity policy and procedures • Cyber incident response services • Intrusion detection and surveillance • Risk identification and mitigation
Vectrus	Vicksburg	Vectrus.com	As one of the largest partners supporting deployed Department of Defense missions, Vectrus provides robust command, control, communications, and computer support. Our enterprise approach to systems engineering is tailored to meet customer requirements for surveillance, reconnaissance, and fused information. We provide mission-critical anomaly resolution, cyber defense, software maintenance, database development, computer engineering and programming, open-system engineering, integrated logistics support, depot maintenance, and IT support development and life-cycle solutions.
BAE Systems	Vicksburg	Baesystems.com	BAE Systems Inc. is the U.S. subsidiary of BAE Systems plc, which is an international defense, aerospace and security company. BAE systems Inc. provides support and service solutions for current and future defense. This company is one of the leading providers of cyber, intelligence and security capabilities to government agencies and growing providers of cyber and network security capabilities to commercial customers.
Silver Hammer Systems	TBD	silverhammersystems.com	Silver Hammer Systems is a company currently based in Georgia looking to expand into Mississippi. They provide cybersecurity services for companies such as early warning services, consulting and staff enablement. They have also worked with IHL to develop cybersecurity programs for universities.

Government Support	Description	Source
Military		
Keesler Air Force Base	Keesler and the 333rd Training Squadron are home to the Air Force's second-largest initial cybersecurity skills training pipeline. Keesler has implemented three main lines of effort: 1. Create the most revered cyber instructors in the Defense Department 2. Rapidly develop and produce operationally relevant curriculum to support warfighters 3. Generate the most lethal cyber operators in the world.	PowerPoint presentation at the International Homeland Defense and Security Summit in Biloxi, MS, April 2017
Keesler AFB 333d Training Squadron – Undergraduate Cyber Training	Undergraduate Cyber Training (UCT) at the 333d Training Squadron (TRS) is the Initial Skills Training Pipeline for United States Air Force Cyber Operations Officers. UCT is located at Keesler Air Force Base in Biloxi, Mississippi. UCT is "America's Finest Cyber Schoolhouse." The 333d TRS is the officer cyberspace tech school and enlisted cyberspace advanced skills training. The squad also develops and revises instructional training to support current global operations through the projection of cyber capabilities.	https://www.squadronposters.com/product/keesler-afb-333d-training-squadron-undergraduate-cyber-training/
Keesler AFB 85th Engineering Installation Squadron	Keesler Air Force Bases' 85th Engineering Installation Squadron has 188 personnel, of which 156 are military and 32 are civilians. This squadron's mission is to provide worldwide, contingency and peacetime engineering and installation of cable, antenna, radio, radar, airfield and secure cyber systems infrastructure	Lovette, D.A. (2018, December) Briefing about Keesler Air Force Base at the Association for Defenses Communities' Regional Forum
Mississippi National Guard Cyber Operations Overview	The Army National Guard (ARNG) authorized the building of 41 Cyber Protection Teams (CPT). Each team consists of 39 members: 7 officers, 16 warrant officers, 16 enlisted officers. Mississippi is listed under CPT 178 which also includes Texas and Louisiana. CPT 178 is based at the Mississippi State University High Performance Computing Collaboratory (HPC²) Starkville, MS. Each team is trained to act both offensively and defensively to help boost state and federal cyber defense capabilities of critical infrastructure. These teams are staffed by part time and full time National Guard soldiers to provide surge ability to support defensive cyberspace operations which can be mobilized for state or federal duty. CPT also participates in the Army deployment cycle and can be deployed in support of other major operations. CPT 178 provides support to: • Develop partnership with MS Attorney General's Office to become a part of the Cyber Crime unit. • FBI fusion cell integration • Currently working toward building a mobile and distributed cyber range capability that would allow deployment of the team to support training with partners, incident response, and remote participation in exercises. • MS Secretary of State Election support • Future plans is to host a Cyber Shield exercise at Camp Shelby, MS that utilizes Engineer Research Development Center (ERDC) in Vicksburg, MS as the host site for content distributed to Camp Shelby to power the exercise	https://www.nationalguard.com/careers/cyber-career

Federal Government		
U.S. Army Corp of Engineers	High Performance Computing Modernization Program (HPCMP) - (Vicksburg, MS) - HPCMP is a technology-led, innovation-focused program committed to extending high performance computing (HPC) to address the Department of Defense's (DoD's) most significant challenges, because they have seen its impact: in research, where HPC enables DoD to explore new theories and evaluate them well beyond what is practical using experiment alone; in acquisition, through the use of validated applications in design and testing, which significantly reduce the time and cost of developing weapon systems, and improve the quality of their designs; and in operations, where real-time calculations produce just-in-time information for decision makers on the battlefield. High performance computing amplifies the creativity, productivity, and impact of the DoD Research, Development, Test and Evaluation (RDT&E) community by giving them access to insight about the physical world, and human actions within it, that would otherwise be too costly, too dangerous, or too time-intensive to obtain through observation and experiment alone. HPCMP is accomplishing its vision today as the DoD's central resource for expertise in the application of high-end computing to the Department's most challenging problems. The High Performance Computing Modernization Program (HPCMP) provides the people, expertise, and technologies that increase the productivity of the DoD's RDT&E community: World-class computational resources - The HPCMP develops and fields the most advanced computing technologies available for routine use by the RDT&E community in the DoD through an architecturally-diverse, routinely-refreshed base of supercomputers and storage systems deployed at its five supercomputing centers across the nation. DoD-leading software application - The HPCMP is modernizing the base of DoD science and engineering applications by: providing vision, funding, and expertise to develop advanced physics-based computational analysis capabilities through the Department's network of laboratories and warfare centers; by developing, demonstrating, and maturing world-class, large-scale scientific software development capabilities within the Department; and by injecting the latest university and industrial research into the computational practices of the RDT&E community. Nationwide research and engineering network - The HPCMP manages the DoD's premiere RDT&E network, the Defense Research and Engineering Network (DREN). As a component of the Global Information Grid (GIG), the DREN provides high-bandwidth, low-latency connectivity among DoD RDT&E, and computational research communities and DoD supercomputing centers. DREN serves as a proving ground for new networking and cybersecurity technologies and fully supports IPv6 and multicast. HPCMP is assuring the DoD's success tomorrow by instilling computational literacy within the next generation S&T	https://www.hpc.mil/2013-08-29-16-01-36/about

	workforce and future military leaders through our leadership in the national HPC community.	
Department of Energy to Fund Establishment of Energy Manufacturing Cybersecurity Institute	The Department of Energy plans to release a funding opportunity for an institute to develop methods and tools to secure manufacturing processes in the energy sector. DOE will support the establishment of a Clean Energy Manufacturing Innovation Institute to examine cybersecurity risks to energy efficiency systems and share information with U.S. manufacturers. "As the sector-specific agency for cybersecurity in the energy sector, it is our job to make sure energy technologies across the board are best prepared against cyber threats," said Mark Menezes, undersecretary for energy. The Office of Energy Efficiency and Renewable Energy plans to issue an FOA in the second quarter via the EERE Exchange portal and may include two technical areas of interest in the announcement.	https://blog.executivebiz.com/2017/02/doe-intends-to-fund-establishment-o-energy-manufacturing-cybersecurity-institute/
U.S. Department of Homeland Security (DHS)	The Department of Homeland Security works to improve the security of the United States. DHS has two agencies that work to specifically target cybersecurity threats with the Cybersecurity and Infrastructure Security Agency (CISA) and Office of Intelligence and Analysis. CISA is a crucial agency in maintaining the security of U.S. cyberspace. This agency works to provide warnings, analysis, vulnerability reduction, mitigation and information sharing for the information systems in the country. CISA is also responsible for preparation and response to cyber threats at the state, local, tribal and territorial government level. Often, CISA will collaborate with the Department of State on the resolution of issues. The Office of Intelligence and Analysis has assigned an Intelligence Officer with departmental and national intelligence authorities in the State. This office provides a medium to report cyber security threats to the U.S. Intelligence community and Federal Government.	Homeland Security | Home (dhs.gov)
Department of Justice/ Federal Bureau of Investigation (FBI)	The combination of the Department of Justice and FBI are the leaders in the country in investigating and prosecuting cyber criminals. The FBI uses its resources to investigate, disrupt and prosecute cyber intrusions as quickly as possible. There is close collaboration between these agencies and the private sector to detect and stop cybercrime.	Welcome to FBI.gov — FBI
United States Secret Service (USSS)	The USSS is involved with the investigation of financially motivated cybercrime. In 2001, the PATRIOT Act mandated that the USSS establish Electronic Crimes Task Forces around the country. Many Cyber Fraud Task Forces have already been established nationwide to increase resources, skills and vision for state, local and federal agencies. The USSS is currently in the process of creating a Cyber Fraud Task Force in Jackson, Mississippi to harness the resources of multiple agencies such as The National Computer Forensic Institute, Cyber Intelligence Section, Computer Emergency Response Team, and Global Investigations Operations Center.	Home | United States Secret Service
State Government		
Enterprise Security Program	To fulfill the statutory requirements in Mississippi Code Ann. 25-53-201 for cybersecurity, the state of Mississippi will have a comprehensive cybersecurity program (the Enterprise Security Program) to provide coordinated oversight of the	https://www.its.ms.gov/Services/Pages/Enterprise%20Security%20Program.aspx

	cybersecurity efforts across all state agencies, including cybersecurity systems, services and development of policies, standards and guidelines.	
Mississippi Department of Information Technology Service (ITS)	ITS aims to provide trusted information technology and telecommunications services to stakeholders in the Mississippi government. ITS is responsible for administering the Enterprise Security Program. ITS works to provide insight to all cybersecurity efforts around the state including cybersecurity systems, services, and development of policies.	Overview (ms.gov)
Mississippi Office of Homeland Security (MOHS)	MOHS is a leading multi-agency task force that works to ensure the state government is prepared to deal with terrorism. MOHS partners with federal, state, and local emergency response personnel to prevent, protect and respond to threats, both man-made and natural disasters, within the state. These threats could include cyber incidents which is why MOHS continues to foster partnerships across professional response disciplines. This ensures the state is well prepared if a cyber attack were to occur. MOHS also works to educate citizens through awareness and outreach programs.	Home | Mississippi Office of Homeland Security (MOHS) (ms.gov)
Mississippi Analysis and Information Center (MSAIC)	The purpose of MSAIC is to provide centralized information gathering, sharing, and analysis for the state of Mississippi. The goal is to aid in the prevention of criminal activity such as acts of terrorism. MSAIC allows for easy information sharing between both private and public sector agencies. MSAIC also enhances law enforcement and public safety agencies ability to detect, prevent and apprehend criminals and terrorists during all attacks including cyber.	MISSISSIPPI ANALYSIS AND INFORMATION CENTER | Mississippi Office of Homeland Security (MOHS) (ms.gov)
Mississippi Emergency Management Agency (MEMA)	MEMA aims to protect Mississippi's citizens by promoting preparedness and providing timely disaster response. MEMA works to prepare for all emergency scenarios within the state.	Mississippi Emergency Management Agency | MEMA (msema.org)
Security Training Opportunities		
Enterprise Security Awareness Computer-Based Training	The state of Mississippi Enterprise Security Policy (ESP) requires each state agency to implement a security awareness program for all agency employees; trusted partners; and individuals authorized to operate, manage, or use state of Mississippi assets. Security awareness programs include training to help change user behavior through a series of short tutorials that educate users on how to improve their cybersecurity posture. ITS has developed a collaborative solution for ensuring state agencies have easy access to computer-based security awareness training.	
Federal and National Security Training	**Cybersecurity education and training is an essential component in protecting the State's IT assets. In addition to the training activities that agencies provide to their staff, ITS encourages agencies review the training resources outlined below.**	
Federal Virtual Training Environment	The Federal Virtual Training Environment (FedVTE) is a flexible, multimedia, e-learning environment that Federal, State, Local, Tribal and Territorial (SLTT) government personnel can access anywhere, anytime. Users enhance their job-related skills through videotaped lectures, demos, and hands-on labs. The environment is accessible from any Internet-enabled computer and is available to Federal and SLTT personnel.	https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

TEEX Cybersecurity Courses	As a founding member of the National Cybersecurity Preparedness Consortium, Texas A&M Engineering Extension Service (TEEX) offers a wide range of federally funded online cybersecurity training opportunities. For those new to cybersecurity, non-technical introductory courses create basic awareness and explore cybersecurity in a community context by building basic terminology and identifying fundamental cyber threats, vulnerabilities and countermeasures. The web-based courses are offered through three discipline-specific tracks: general, non-technical computer users; technical IT professionals; and business managers and professionals.	https://teex.org/Pages/Program.aspx?catID=607&courseTitle=Cybersecurity
United States Department of Defense Security Education & Training	The United States Department of Defense, Center for Development of Security Excellence provides online security education and awareness courses using a collaborative learning environment. This training is designed raise awareness about security principles and concepts and is available to government employees.	https://www.its.ms.gov/Services/Pages/Security-Training-Opportunities.aspx
Cyberterrorism Defense Initiative Training – Free Training	The Cyberterrorism Defense Initiative (CDI) is a comprehensive, integrated series of courses that incorporates best practices, procedures, and methodologies for a variety of systems. Because information technology is an integral part of the infrastructure and modern-day workflow of all critical infrastructure, CDI is meant to address concerns common to a broad spectrum of disciplines. Training is designed to meet the needs of a broad but focused demographic of public and private sector technical personnel, ensuring that critical capabilities reach all levels of management and field response. All CDI courses utilize a blended learning approach that balances classroom lecture, hands-on laboratory exercises, and online supplemental material. "The Cyberterrorism First Responder" is for skilled technical personnel and will utilize cyberterrorism response tools against simulated cyberterror attacks that are targeted at national network infrastructure targets. "The Comprehensive Cyberterrorism Defense" and "The Cyberterrorism First Responder" courses also teaches participants not only how to combat cyberterrorism, but also how to preserve and collect critical evidence logs, primarily to assist law enforcement in resolving an event and apprehending perpetrators. A core component of CDI is preparing critical infrastructure technical personnel with thorough policy and planning mechanisms for recovering and rebuilding critical infrastructure harmed by a cyberterrorist event. Using the leave-behind materials, manuals, and resources produced by CDI, graduates can ensure that the lessons learned are sustained and administered throughout their individual agencies. Classes are held in easily accessible and centralized locations throughout the United States.	http://www.cyberterrorismcenter.org/index.html

Appendix C

Mississippi Cyber Initiative Executive Plan

Why the Mississippi Cyber Initiative?

Digital and cyber operations involve a complex infrastructure that impacts all aspects of our economy and our lives. We are dependent on cyber-related processes, systems, information sources, and situational awareness. Sensitive information critical to stakeholders is stored and transferred digitally every minute, requiring protection at all levels as rapidly evolving cyber technologies have increased the nation's vulnerability to cyberattacks. As our dependence on cyber capabilities continues to grow, so will the need to protect critical information and infrastructure. Many of the systems that facilitate these societal functions are vulnerable to technological exploitation. The Mississippi Cyber Initiative (MCI) is needed to meet these challenges of the cybersecurity reality in the state and around the nation and will position Mississippi as a leader in a field that will be of critical importance in the years and decades ahead.

Vision:

The MCI will create a statewide ecosystem to address cybersecurity issues in the State and our nation. The MCI will advance innovation while developing a workforce that will create economic opportunities.

Mission:

The mission of MCI will be to provide state-wide leadership that prepares Mississippi's future economy through unparalleled collaboration and innovation in cybersecurity. The MCI will be an economic development catalyst leveraging the collective expertise among academia, the private sector, state, federal and local government, law enforcement, the U.S. Department of Defense, and the Mississippi National Guard.

The MCI will focus the mission in three areas:

- Meet the cybersecurity training needs at Keesler Air Force Base
- Provide statewide leadership in addressing cybersecurity and workforce needs for Mississippi into the future
- Attract innovative cyber and advanced technology industries

Goals of the Mississippi Cyber Initiative:

- Promote economic development for the Gulf Coast region and the State
- Deliver timely cybersecurity workforce training and education
- Maximize collaboration with state's diverse cyber community to strengthen capabilities and address vulnerabilities
- Increase public awareness through outreach
- To support defense companies supply chain

Background:

- Modeled after the Georgia Cyber Center in Augusta, GA.
  - The Georgia Cyber Center is a public/private collaboration among academia, state, federal and local government, law enforcement, the U.S. Army and the private sector.
  - Augusta is also home to the United States Army's Cyber Command (Fort Gordon), the US Army Cyber Center of Excellence and the National Security Agency (NSA), making Augusta the destination for cyber professionals in any stage of their career.
  - The state's investment of $100 million provided two adjacent buildings totaling 332,000 square feet.

  - Facilities serve as a hub for technology startups and includes leasable space available to firms and organizations supporting the state's cybersecurity ecosystem who can leverage the center's resources and the convenience of co-location with state, federal and other industry associates.
  - It is also home to certificate, undergraduate and graduate level programs in cybersecurity and cyber sciences offered by Augusta University and Augusta Technical College.
  - The facility also features a cutting-edge cyber range, a 390-seat auditorium, an incubator/accelerator to foster innovation and entrepreneurship and classrooms.
  - In FY2019, the Georgia Cyber Center hosted 12,000 visitors from 18 countries, 15 states, and every county in Georgia.

- A team from Mississippi visited the Georgia Cyber Center in March 2020 that included representatives from Mississippi State University, the University of Southern Mississippi, Mississippi National Guard, and Keesler Air Force Base. It was during this visit that leaders among the group began considering the idea of a similar facility in Mississippi since Keesler AFB is the home of Air Force and Space Cyber Training.

Location:

The MCI will be headquartered in a new, state-of-the-art facility located in Biloxi, adjacent to Keesler AFB, known as the Mississippi Cyber & Technology Center (MCTC).

- The MCTC will serve as the heart of the statewide MCI ecosystem with complimentary capabilities across the state. It will serve as a focal point to promote and integrate Cyber and Technology capabilities and talent.
- The second key location will be on the Mississippi Gulf Coast Community College Harrison County campus. With new construction on their campus, MGCCC will serve as a major artery for the MCI. Having the MGCCC location creates unique opportunities for meeting training requirements at Keesler AFB.
- In addition to these foundational sites, the MCI ecosystem will connect current and future physical assets and human capital throughout the State that belong to partners and collaborators.
- The MCI will help to connect cybersecurity efforts and initiatives from across the entire state. The MCTC provides a facility where cyber experts from across the state, region, and nation can gather to collaborate on how best to meet cybersecurity demands that impact federal, state, private, and public entities.

The MCTC will offer the full scope of services necessary to prepare the workforce and address partner cyber challenges.

- As the headquarters for the Mississippi Cyber Initiative, the MCTC becomes a hub for constantly updating and developing curricula to meet training and professional development requirements of stakeholders.
- It provides a conduit for advanced IT education, awareness, and innovation.
- It will house coordination efforts for all relevant state agencies in cybersecurity.
- It provides a center for tech workshops & innovation hubs to the community.
- It will serve as a technology incubator for private sector development in cybersecurity.
- The facility will also have a Secured/Controlled space to hold sensitive information, conduct advanced training and education, and allow collaboration on the most current cyber threats and mitigation efforts facing all stakeholders.

Focus Areas:

- Cybersecurity, Cyber Forensics, and Innovation
- Education and Certificate Training
- Economic and Workforce Development
- State and Federal Government, and Public, Private Partnerships
- Research and Development

Execution (Lead Partners):

The MCI partnership is led by Mississippi State University (MSU) with implementing partners from Keesler Air Force Base (Keesler AFB), Mississippi Gulf Coast Community College (MGCCC), and the University of Southern Mississippi (USM). While MSU, MGCCC, Kessler AFB, and USM serve as lead implementing partners, the success of the MS Cyber Initiative will be based on strong partnerships and collaboration among all stakeholders by leveraging the collective expertise among academia, the private sector, state, federal and local government, law enforcement, Department of Defense, and MS National Guard.

- **Mississippi State University** is one of the leading cybersecurity research and education universities in the nation and Mississippi's premier cyber institution.
  - MSU is one of only 10 universities in the U.S. to hold all three academic certifications awarded by the National Security Agency (NSA). Led by the Bagley College of Engineering Computer Science and Engineering departments, these designations include the Center of Academic Excellence (CAE) CAE-Cyber Defense Education, CAE-Cyber Defense Research, and CAE-Cyber Operations.
  - The MSU Center for Cyber Innovation (CCI) collaborates with the NSA providing DoD 8570- compliant commercial cyber certification training across the Department of Defense.
  - Mississippi State University offers the following degrees and certifications in Cybersecurity:
    - M.S. in Cyber Security and Operations
    - B.S. in Cybersecurity
    - Information Assurance Professional Certificate
    - Graduate Certificate in Cyber Operations
  - MSU's Bachelor of Applied Science (BAS) degree program allows military and civilian students to transfer up to 60 hours of credits (15 hours of general education core and 45 hours of technical credits) earned from a community college or the military to a bachelor's degree at MSU. Delivered online, the BAS programs are offered in more than 30 career fields including several fields related to cyber, information systems, and data science. Thus, permanent party and graduates of Keesler AFB can apply Community College of the Air Force credits to a BAS program related to their area of expertise.
  - MSU is committed to supporting service members, veterans and their dependents and is consistently recognized as a top 10 Military Friendly school.

- **Keesler AFB** has direct responsibility for training the Air Force and Department of Defense's cyber force graduating approximately 8,700 cyber professionals per year. As a key partner, Keesler AFB anchors this initiative and creates a unique opportunity for our state to enhance collaborations with federal partners across the state, region, and nation.
  - Keesler's training mission is the responsibility of the 81st Training Group. The 81st Training Group annually provides training to more than 28,000 officers, airmen and civilian employees of the Air Force, Air Force Reserve, Air National Guard, Army, Navy, Marine Corps, other DOD agencies and DOD contractors, as well as allied nations. On any given day, more than 2,800 students attend classes in one of over 160 courses in a wide variety of career fields.
  - Accredited by the Commission of the Southern Association of Colleges and Schools, the group is a Community College of the Air Force institution.
  - Technical resident courses include career fields such as personnel, information management, air traffic control, finance, manpower, religious affairs, command and control, cyber training to include computer operation, maintenance and programming, weather, meteorology, and Precision Measurement Equipment Laboratory. Three other locations provide additional training, including postal operations, nuclear command and control, and visual/broadcast information.

- **Mississippi Gulf Coast Community College** has well-established cyber and IT academic and certification programs essential in preparing a cyber workforce and is the leading provider of workforce training and education in the gulf coast region.
  - MGCC's current and planned facilities provide immediate capabilities and opportunities to support Keesler AFB and advance the MCI. The MGCCC Center for Security and Emerging Technology (CSET) provides a platform to transform workforce training for economic expansion, innovation, and societal growth with requisite training in emerging technologies (e.g., Cybersecurity, Coding, Artificial Intelligence (AI), Virtual Reality (VR)/Augmented Reality (AR), and Simulation/Game Design) that can make the Gulf Coast region an international leader in the high-tech sector.

- **University of Southern Mississippi (USM)** has a growing cyber program and will also play a key role utilizing well established partnerships across the state associated with the Mississippi Defense Initiative (MDI).
  - The University of Southern Mississippi also offers a minor in information security, with cybersecurity coursework offered across it four undergraduate majors (information technology, computer science, computer engineering, and electronics & computer engineering technology) and graduate programs in computer science and computational science.
  - USM, in collaboration with the City of Biloxi and the Mississippi Coding Academies (MCA), will launch a cybersecurity academy in Biloxi MS in spring 2021. This workforce development program will enable under-served persons

in the Gulf Coast area to develop skills aligned with the NICE Cybersecurity Workforce Framework including the roles of Cyber Defense Analyst, Cyber Defense Incident Responder, and Cyber Defense Infrastructure Support Specialist. This MCA Cyber Academy will utilize the Appalachian Regional Commission funded Mississippi Cyber Range through partnership with MSU's Bagley College of Engineering. All cyber range use that is not in an ARC county will be paid through MCA.

Execution Phases and Current Initiatives

- **Immediate:** - Support to Keesler AFB
  - Course and Curriculum Support
    - Initial Focus on Cyber and Meteorology
  - Instructor Support
    - Information Sharing
    - Instructor Swaps
  - Recruiting and Accessions
  - Technology Integration & Training Techniques
  - Continuing Education
  - Bachelor of Applied Science Program Awareness
  - Academic Access to Information – Larger knowledge base
  - Warfighting Training Simulations
  - Talent Management - Internships
  - Workforce Development in Cyber Security
  - K-12 Cyber Education/Awareness Program on Coast
- **Near Term:**
  - Cyber Infrastructure
    - Systems Operations Lab
    - Cyber Range
    - Cyber Forensics Lab
    - Cyber Certifications
  - Provide defense industry assistance for national cybersecurity compliance
  - Collaboration facility at MGCCC to enhance instructional requirements at Keesler
- **Long Term** - Full MCTC operational capability

Stakeholder Engagement Plan - Initial Stakeholders and collaborators:

As mentioned above, success will be accomplished through strong partnerships and collaboration among all stakeholders by leveraging the collective expertise among academia, the private sector, state, federal and local government, law enforcement, Department of Defense, and MS National Guard. An aggressive engagement plan will be executed to inform potential stakeholders and promote statewide collaboration.

- Statewide Education Partners

  - Universities
  - Community Colleges
  - Coding Academies
  - K-12 Schools
- Federal Partners:
  - Keesler AFB
  - Stennis Space Center
  - NASA
  - NOAA
  - Naval Construction Battalion Center
  - Army Corp of Engineers and Engineering Research & Development Center (ERDC)
  - Camp Shelby
  - U.S. Coast Guard
  - Department of Homeland Security
  - FBI
  - Other military installations located across the state
- State Agencies
  - Mississippi Development Authority
  - Department of Public Safety (MBI, Homeland Security, others)
  - MS National Guard
  - MS Attorney General
  - Department of Information Technology Services
  - Emergency Management Agency
  - Mississippi Gaming Commission
  - Department of Education
  - Municipal Partners
- Potential Private Industry Partners
  - Defense
  - Cyber
  - IT
  - Transportation
  - Communications
  - Utilities
  - Health Care
  - Financial Institutions
  - Manufacturing
  - Aerospace
  - Shipbuilding
  - Ports
  - Oil & Gas, Chemical

How will the MCTC be built and MCI managed?

Organization: MSU was selected to lead the MCI effort and building of the MCTC based on the strength of its nationally recognized cyber program and experience

managing the largest university research and economic development park in Mississippi. The Mississippi State University Research & Technology Corporation (MSU-RTC) is a 501(c)(3), non-profit corporation formed and approved pursuant to Mississippi Code Annotated Section 37-147-15, the purpose of which is to promote, develop and administer enterprises arising from research and technology innovations in order to take advantage of opportunities of scientific, educational and economic development.

The MSU-RTC manages and develops the Thad Cochran Research, Technology & Economic Development Park, a 272-acre park with approximately 1,700 employees located in Starkville, MS. MSU-RTC owns, manages and leases 7 buildings to industry and university partners, representing 207,000 square feet: 5 in Starkville and 2 on the Mississippi Gulf Coast, including a building at the John C. Stennis Space Center. This represents over $100 million in infrastructure investment, over $104 million in private capital investment, and a FY19 economic impact from private tenants that exceeds $62 million.

Why the Mississippi Gulf Coast?

Biloxi is home to Keesler AFB and the 81st Training Wing (TRW). Keesler AFB has direct responsibility for training the Air Force and Department of Defense's cyber force and, as a key partner, anchors this initiative and creates a unique opportunity for our state, region, and nation.

- The 81st Training Wing is host to 2nd Air Force, the 403rd Wing (AF Reserve), Air Combat Command cyber training detachments, and is the single largest employer on the Mississippi Gulf Coast.
- Keesler trains more than 28,000 students annually with an average daily student load of more than 2,700. The 81st TRW is a lead Joint Training Installation, instructing not only Air Force, but Army, Navy, Marine Corps, Coast Guard and civilian federal agency personnel.
- Keesler AFB is the second largest technical training center in the Air Force and produces leaders in innovative forecasting trends in learning and on cutting-edge of training technology.
- Keesler's training mission is the responsibility of the 81st Training Group -- the largest electronics training group in the world. On any given day, more than 2,700 students attend classes in one of over 160 courses.
- In Keesler AFB's FY 2018 Economic Impact Statement, their adjusted economic impact was $1.59 billion dollars. This includes a workforce of over 11,500 with over 3,400 jobs created.

The U.S. Military impact on South Mississippi is significant. The Mississippi Gulf Coast is home to all branches of the military – Keesler Air Force Base, Naval Construction Battalion Center, the U.S. Navy at John C. Stennis Space Center, the U.S. Coast Guard, and Air and Army National Guard locations all call South Mississippi home. These include missions such as the Hurricane Hunters, Cyber Training Center of Excellence, Riverine Warfare, Forward Theater Infrastructure Construction, Ocean Modeling and Weather Prediction for the U.S. Fleet. The military presence on the Gulf Coast accounts for over $817 million in payroll with employment of over 19,900 personnel.

Through the Mississippi Defense Initiative (MDI), strong relationships exist among all military installations across the entire state. We will leverage the partnerships MDI has formed to create new opportunities for collaborations to enhance joint capabilities include:

- Advanced cyber training and support
- Workshops and conferences
  - Exercises in self-contained secured area/rooms
  - Teaches advance cyber, computer sciences, etc.
- Innovation centers for Autonomy, Artificial Intelligence, Virtual Reality, and Gaming labs
- Commercial and Industrial certifications

The Mississippi Coast Alliance for Economic Development
(http://mscoastalliance.com/)

- Strategically located at the center of the northern Gulf of Mexico and along Interstate 10, the Mississippi Gulf Coast provides industry access to 55% of the nation's population within a day's drive. The Mississippi Coast is a 3-county region abutting the central coast of the northern Gulf of Mexico. It is known for its unique location with many geographic advantages and ease of access.

- With a population of nearly 400,000 people and a strong and supportive business environment, the region's expertise is in autonomy, shipbuilding, aerospace and defense, advanced manufacturing, energy, and petrochemical industries.
- All the Gulf Coast's primary industries require robust cybersecurity capabilities and a trained workforce to meet current and future demands. The MCI will provide the statewide ecosystem for collaboration to meet demands and accelerate our economic development.

Research, Innovation, and Economic Opportunity - Mississippi is nationally recognized in the areas of High-Performance Computing, Autonomy, Artificial Intelligence, Virtual Reality, Advanced Manufacturing, Machine Learning, Modeling and Simulation, and more. Cyber security is the primary component for advancing these technologies. The MCI collaboration will strengthen cybersecurity, accelerating research and innovation and creating economic opportunities for the entire state.

As the MCI concept moves into the execution phase more opportunities will be identified. The success of the MCI will be based on strong partnerships and collaboration among all stakeholders. As the MCI matures, capabilities and vulnerabilities from across the state will be captured. Working together, the MCI will focus on leveraging statewide capabilities to strengthen cyber security, promote innovation and opportunity, while addressing the workforce development needs of the state.

THE UNIVERSITY OF SOUTHERN MISSISSIPPI
TRENT LOTT NATIONAL CENTER

Mississippi Defense Initiative is a Service of the Trent Lott National Center

Services Offered by The University of Southern Mississippi College of Business and Economic Development and Trent Lott National Center for Economic Development and Entrepreneurship

The College of Business and Economic Development offers graduate education in economic development through the Master of Science in Economic Development (MSED) program and a Graduate Certificate in Economic Development. The Trent Lott National Center partners with the MSED program to further the students experience by working with economic developers, communities, companies, and non-profit organizations through five main approaches:

1. University Economic Development researchers provide technical assistance in defining problems or opportunities; evaluating the effects of change; and providing recommendations for improvements.

2. Graduate students work on applied research projects involving actual community or organization case scenarios (e.g., retail trade studies, economic impact studies).

3. Each student is required to complete a data analytics capstone project. The capstone project involves completing a Quality-of-Place (QOP) study for a community.

4. Each student is required to complete an internship in an economic development organization.

5. Communities may have sponsored research projects and tap into the faculty expertise and university data sources (e.g., EMSI and REMI).

Examples of class projects involving research for Mississippi communities:

- Retail Analysis for Marion County
- Feasibility of a multi-sports complex in Grenada County
- Economic Impact of the Gulfport-Biloxi International Airport
- Ecotourism Development for the Mississippi Aquarium in Gulfport
- Strategic Plans for the City of Pearl and Simpson County Development Foundation
- Community Study for the Hattiesburg Mid-Town District
- Competitiveness studies for defense-dependent communities
- Multimodal transportation research for Mississippi Port Directors
- Workforce Analyses for the Mississippi Department of Education and Department of Human Services

The University of Southern Mississippi also offers economic development training for working professionals and graduate students through its annual True South Basic Economic Development Course - an International Economic Development Council accredited introductory course. This course fulfills one of the prerequisites for those who wish to take the Certified Economic Developer (CEcD) exam.