CTE K12 CAREER PATHWAYS FOR CYBERSECURITY STUDY

Study Funded by the National Security Agency (NSA)

Abstract:

The goal of this study is to examine the current state of cybersecurity careerprograms of study and the career pathways systems that support these programs.

John Sands, Ph.D.
Sands@MoraineValley.edu

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

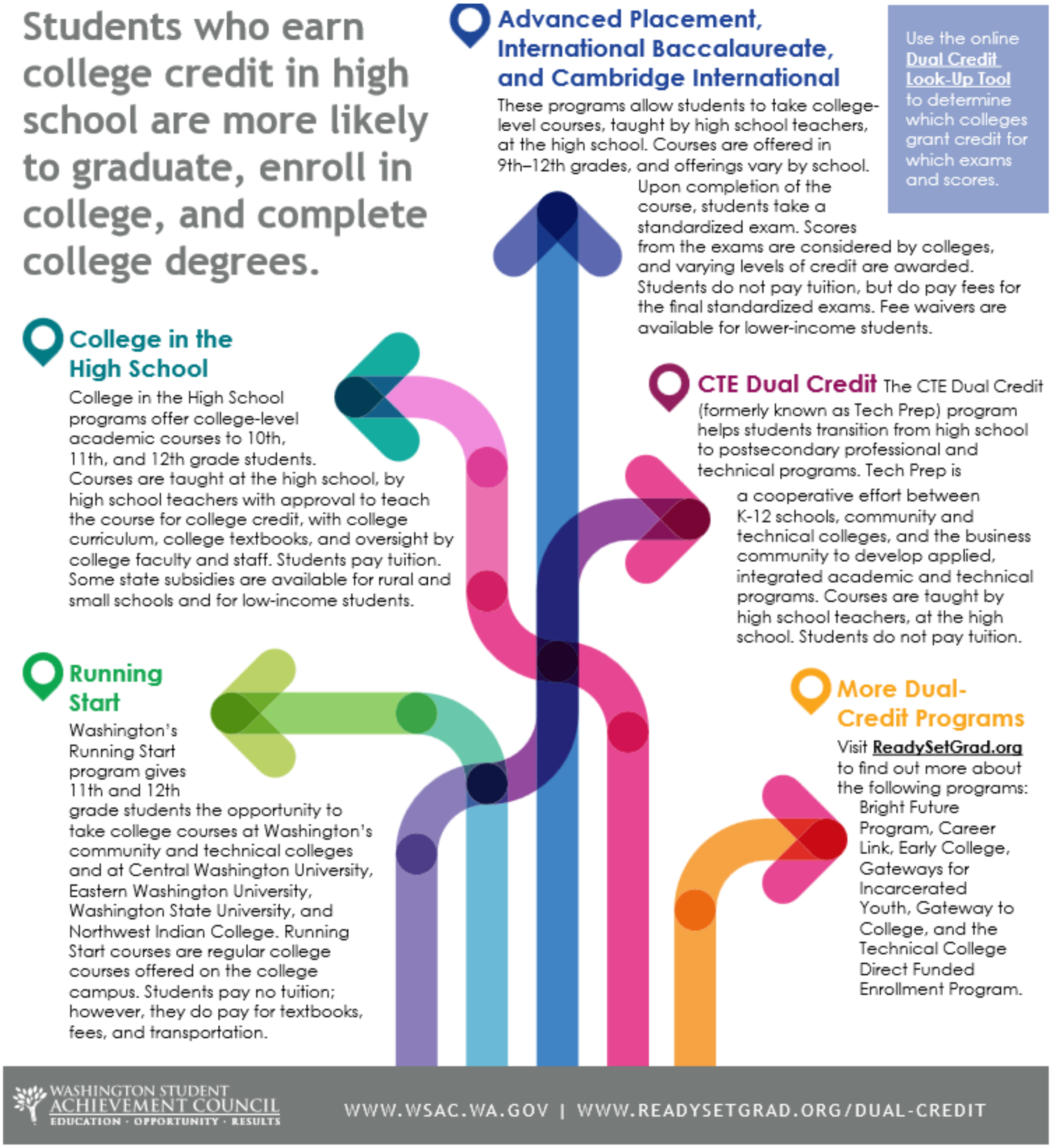
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This study is designed to measure the progress of building career pathways to support the occupation of cybersecurity professionals. A Career Pathway is a term used to describe an educational ecosystem. This ecosystem is made up of multiple elements of an effective pathway for students that identify and enroll in courses leading to a specific career field or occupation. These elements typically consist of classes or courses in middle school, high school, two-year colleges and possibly four-year schools and universities. Pathway elements also often include workforce learning programs like work-study programs, internships and apprenticeships. Key elements would include well-defined articulation programs between K-12 and institutions of higher education such as advanced placement, dual credit, dual enrollment, early college programs, TechPrep and locally established agreements that enable students to earn college credit while still in K-12 programs.



Students who earn college credit in high school are more likely to graduate, enroll in college, and complete college degrees.

Advanced Placement, International Baccalaureate, and Cambridge International

These programs allow students to take college-level courses, taught by high school teachers, at the high school. Courses are offered in 9th–12th grades, and offerings vary by school. Upon completion of the course, students take a standardized exam. Scores from the exams are considered by colleges, and varying levels of credit are awarded. Students do not pay tuition, but do pay fees for the final standardized exams. Fee waivers are available for lower-income students.

Use the online Dual Credit Look-Up Tool to determine which colleges grant credit for which exams and scores.

College in the High School

College in the High School programs offer college-level academic courses to 10th, 11th, and 12th grade students. Courses are taught at the high school, by high school teachers with approval to teach the course for college credit, with college curriculum, college textbooks, and oversight by college faculty and staff. Students pay tuition. Some state subsidies are available for rural and small schools and for low-income students.

CTE Dual Credit The CTE Dual Credit (formerly known as Tech Prep) program helps students transition from high school to postsecondary professional and technical programs. Tech Prep is a cooperative effort between K-12 schools, community and technical colleges, and the business community to develop applied, integrated academic and technical programs. Courses are taught by high school teachers, at the high school. Students do not pay tuition.

Running Start

Washington's Running Start program gives 11th and 12th grade students the opportunity to take college courses at Washington's community and technical colleges and at Central Washington University, Eastern Washington University, Washington State University, and Northwest Indian College. Running Start courses are regular college courses offered on the college campus. Students pay no tuition; however, they do pay for textbooks, fees, and transportation.

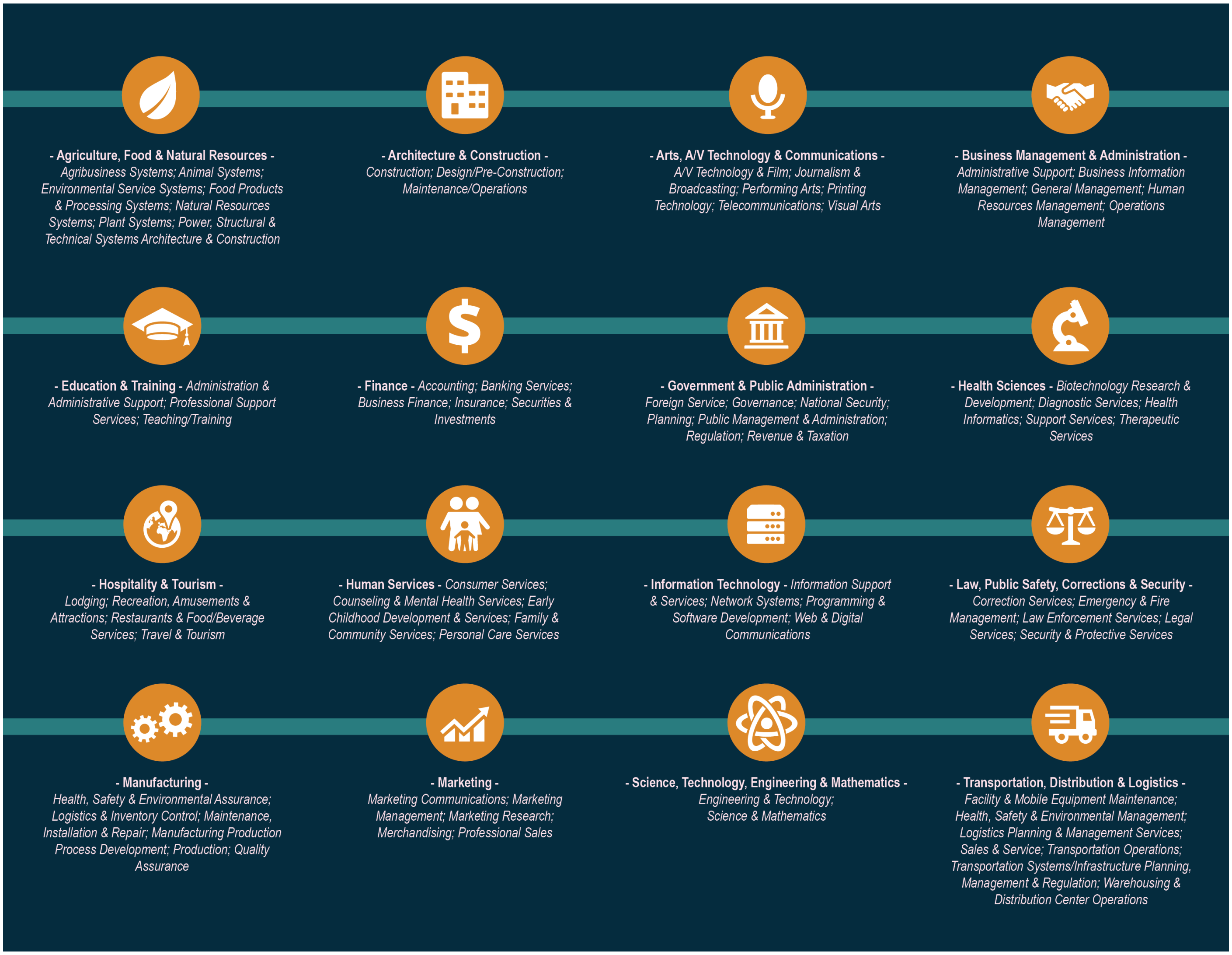
More Dual-Credit Programs

Visit ReadySetGrad.org to find out more about the following programs: Bright Future Program, Career Link, Early College, Gateways for Incarcerated Youth, Gateway to College, and the Technical College Direct Funded Enrollment Program.

WASHINGTON STUDENT ACHIEVEMENT COUNCIL
EDUCATION · OPPORTUNITY · RESULTS

WWW.WSAC.WA.GOV | WWW.READYSETGRAD.ORG/DUAL-CREDIT

Model programs typically contain supplementary programs and services like career counseling, academic advising, personal interest survey tools and career awareness programs. Well-designed Career Pathways enable students to gain an early start to a targeted career and may also shorten the time required to complete academic studies and enter the workforce. The United States Department of Education created a Career Pathways framework that grouped occupations within associated career clusters. Occupations within a pathway share common skills, knowledge, and interests. In total, there are 16 Career Clusters in the National Career Clusters Framework, representing more than 79 career pathways.



- Agriculture, Food & Natural Resources - *Agribusiness Systems; Animal Systems; Environmental Service Systems; Food Products & Processing Systems; Natural Resources Systems; Plant Systems; Power, Structural & Technical Systems Architecture & Construction*

- Architecture & Construction - *Construction; Design/Pre-Construction; Maintenance/Operations*

- Arts, A/V Technology & Communications - *A/V Technology & Film; Journalism & Broadcasting; Performing Arts; Printing Technology; Telecommunications; Visual Arts*

- Business Management & Administration - *Administrative Support; Business Information Management; General Management; Human Resources Management; Operations Management*

- Education & Training - *Administration & Administrative Support; Professional Support Services; Teaching/Training*

- Finance - *Accounting; Banking Services; Business Finance; Insurance; Securities & Investments*

- Government & Public Administration - *Foreign Service; Governance; National Security; Planning; Public Management & Administration; Regulation; Revenue & Taxation*

- Health Sciences - *Biotechnology Research & Development; Diagnostic Services; Health Informatics; Support Services; Therapeutic Services*

- Hospitality & Tourism - *Lodging; Recreation, Amusements & Attractions; Restaurants & Food/Beverage Services; Travel & Tourism*

- Human Services - *Consumer Services; Counseling & Mental Health Services; Early Childhood Development & Services; Family & Community Services; Personal Care Services*

- Information Technology - *Information Support & Services; Network Systems; Programming & Software Development; Web & Digital Communications*

- Law, Public Safety, Corrections & Security - *Correction Services; Emergency & Fire Management; Law Enforcement Services; Legal Services; Security & Protective Services*

- Manufacturing - *Health, Safety & Environmental Assurance; Logistics & Inventory Control; Maintenance, Installation & Repair; Manufacturing Production Process Development; Production; Quality Assurance*

- Marketing - *Marketing Communications; Marketing Management; Marketing Research; Merchandising; Professional Sales*

- Science, Technology, Engineering & Mathematics - *Engineering & Technology; Science & Mathematics*

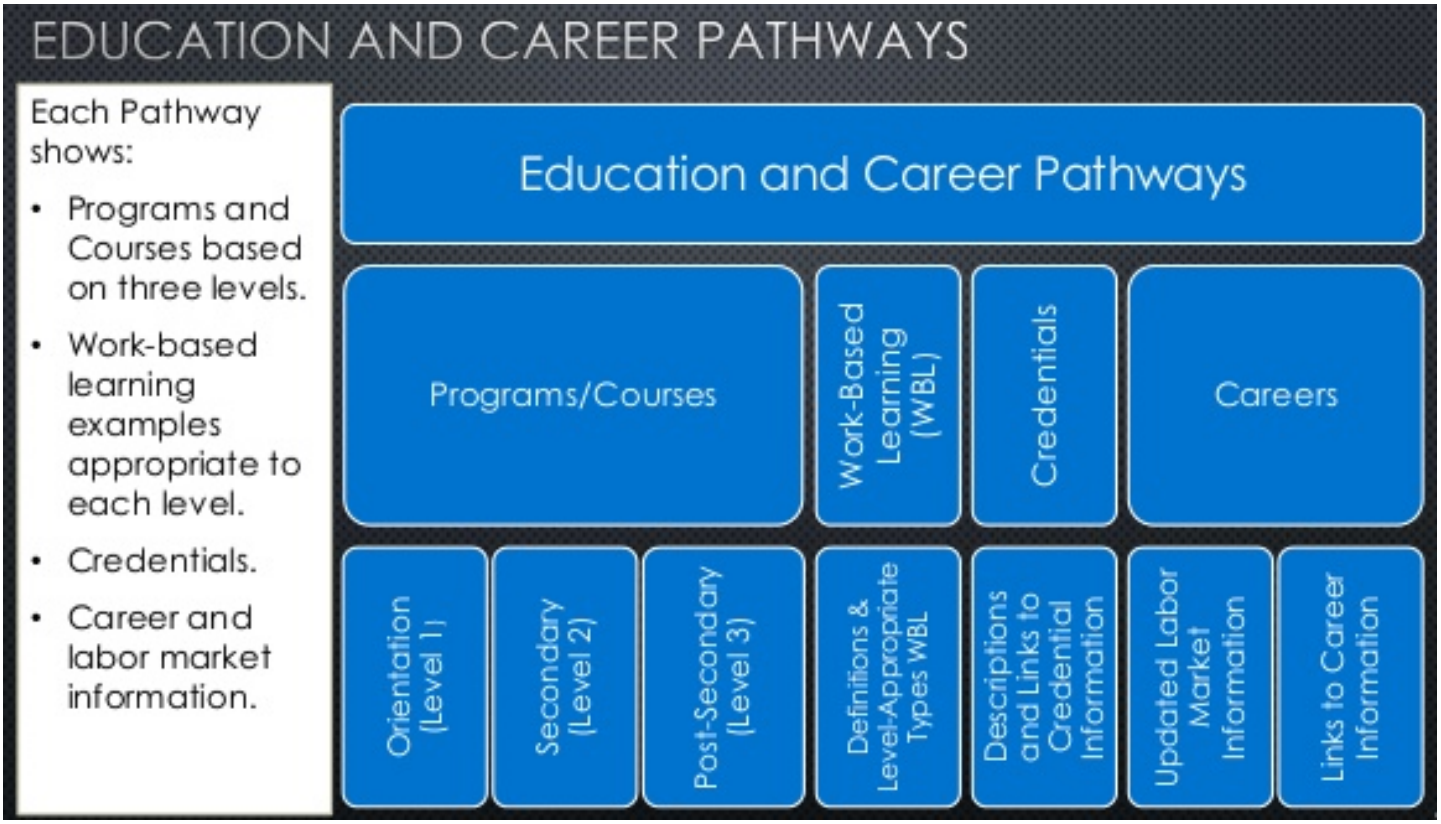
- Transportation, Distribution & Logistics - *Facility & Mobile Equipment Maintenance; Health, Safety & Environmental Management; Logistics Planning & Management Services; Sales & Service; Transportation Operations; Transportation Systems/Infrastructure Planning, Management & Regulation; Warehousing & Distribution Center Operations*

ORIGINS OF CAREER CLUSTERS FRAMEWORK

The Career Cluster initiative began in 1996 in the United States as the Building Linkages Initiative and was a collaborative effort between the U.S. Department of Education, the Office of Vocational and Adult Education (OVAE), the National School-to-Work Office (NSTWO) and the National Skill Standards Board (NSSB). The purpose of the Initiative was to establish linkages among State educational agencies, secondary and post-secondary educational institutions, employers, industry groups, other stakeholders and Federal agencies. The goal was to create curricular frameworks in broad career clusters, designed to prepare students to transition successfully from high school to post-secondary education and employment in a career area.

The creation of curricular models within the context of broad career clusters ensures the alignment of academic and technical instructional strategies with the requirements of post-secondary education and the expectations of employers in increasingly academic and technologically demanding careers. The vocational education field has historically responded to the needs of the national economy by preparing individuals for in-demand jobs.

(https://en.wikipedia.org/wiki/Career_Clusters#cite_note-2)



EDUCATION AND CAREER PATHWAYS

Each Pathway shows:

- Programs and Courses based on three levels.
- Work-based learning examples appropriate to each level.
- Credentials.
- Career and labor market information.

Education and Career Pathways
Programs/Courses
Work-Based Learning (WBL)
Credentials
Careers
Orientation (Level 1)
Secondary (Level 2)
Post-Secondary (Level 3)
Definitions & Level-Appropriate Types WBL
Descriptions and Links to Credential Information
Updated Labor Market Information
Links to Career Information

CURRENT FRAMEWORK CHALLENGES

The challenge faced by the cybersecurity academic community is the absence of a formal career cluster framework for the cybersecurity field. Unfortunately, when the Career Pathways framework was developed by the U.S. Department of Education in 1996, there was no placement within the framework for many of today's high-demand career fields like cybersecurity. This is due to the fact that careers like cybersecurity were not established or a recognized profession in 1996.

However, there are many opportunities for students to start and advance their careers within the cybersecurity career field. Several states and local Career and Technical Education (CTE) communities have taken the initiative to develop and implement homegrown or organic career pathway programs in cybersecurity. This study is designed to explore and record the details of such programs throughout the United States.

PROJECT SUMMARY

The National Security Agency awarded grants to a group of institutions that earned the Center of Academic Excellence in Cyber Defense (CAE-CD) designation and are active in the Career Technical Education (CTE) community.

- Coastline Community College (California)
- Dakota State University (North Dakota)
- Mohawk Valley Community College (New York)
- Moraine Valley Community College (Illinois)

The grants funded several different studies to research and document the current state of cybersecurity CTE K-12 career pathways programs across the nation. Each of the four grant recipients proposed a different approach to study the challenges of establishing and building effective career pathways in the cybersecurity field of study. The goal is to formally identify and document these programs, share best practices and identify how investments can improve and sustain a new era of cybersecurity career pathways. The team at Coastline Community College worked with CTE stakeholders at the state level in the state of California to identify programs at the state and regional level. The team at Dakota State University examined the challenges of establishing cybersecurity pathway programs in small rural communities. The team at Mohawk Community College worked with CTE leaders in establishing faculty development classes and established a statewide-recognized standard for K-12 instructors teaching cybersecurity concepts. The team at Moraine Valley Community College took a different approach in gathering and documenting data. This team organized a series of statewide focus groups to discuss and explore the unique cybersecurity pathway programs in their states.

RATIONAL FOR STUDY

RATIONALE

Career pathway systems are one of the most proven ways to increase program impact in addressing careers in high demand. The U.S. Department of Education established the career pathways and career cluster framework in the 1990's. At that time, the cybersecurity field of study was not a separate occupation. During this period, cybersecurity related tasks were typically the responsibility of information technology specialists. One of the first tasks of the research teams was to document existing statewide career cluster publications to identify where a cybersecurity program of study would reside. The results were surprising. Only two states, Maryland and Virginia, formally recognized cybersecurity programs of study in their career cluster publications.

PERTINENCE

In recent years, the National Institute for Standards and Technologies (NIST) published the NIST National Initiative for Cyber Education (NICE). The NICE project is led by NIST in the U.S. Department of Commerce. The project is a partnership between government, academia, and the private sector that seeks to energize and promote a robust network and ecosystem of cybersecurity education, training, and workforce development. The NICE project fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals responsible for keeping our nation secure and economically competitive.

COMPONENTS OF THE NICE FRAMEWORK

The NICE Framework organizes cybersecurity and related work. This section introduces and defines the core components of the NICE Framework in support of those areas. These areas include:

CATEGORIES

Categories provide the overarching organizational structure of the NICE Framework. There are seven categories, and all are composed of Specialty Areas and Work Roles. This organizational structure is based on extensive job analyses, which group together work and workers that share common major functions, regardless of job titles or other occupational terms.

SPECIALTY AREAS

Categories contain groupings of cybersecurity work, which are called ***Specialty Areas***. There were 31 Specialty Areas called out in National Cybersecurity Workforce Framework version 1.0 [2] and 32 in National Cybersecurity Workforce Framework version 2.0 [3]. Each Specialty Area represents an area of concentrated work, or function, within cybersecurity and related work. In previous versions of the NICE Framework, tasks and knowledge, skills, and abilities (KSAs) were associated with each specialty area. Tasks and KSAs are now associated with the Work Roles.

WORK ROLES

Work Roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role. Work being performed in a job or position is described by selecting one or more Work Roles from the NICE Framework relevant to that job or position, in support of mission or business processes. To aid in the organization and communication about cybersecurity responsibilities, Work Roles are grouped into specific classes of Categories and Specialty Areas.

KNOWLEDGE, SKILLS, AND ABILITIES (KSAS)

Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform Work Roles and are generally demonstrated through relevant experience, education, or training.

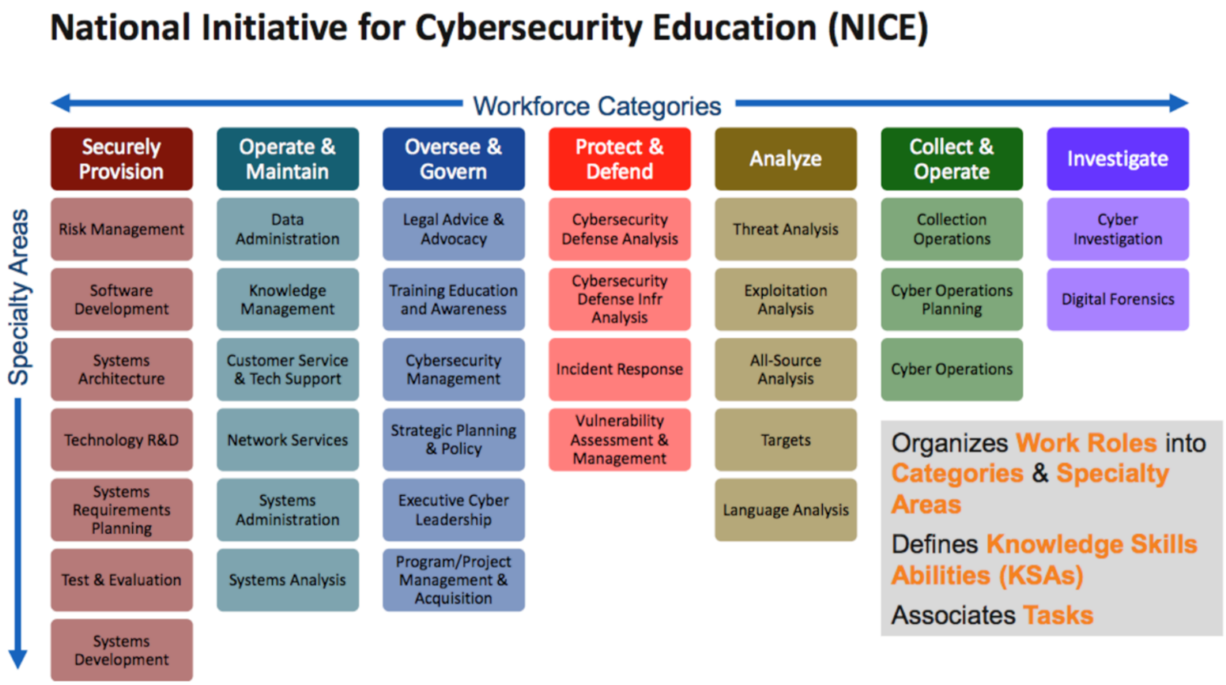
Knowledge is a body of information applied directly to the performance of a function. ***Skill*** is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual. ***Ability*** is competence to perform an observable behavior or a behavior that results in an observable product.

RESEARCH TASKS

A ***Research Task*** is a specific defined piece of work that, combined with other identified tasks, composes the work in a specific Specialty Area or Work Role.

NICE FRAMEWORK COMPONENT RELATIONSHIPS

The NICE Framework components describe cybersecurity work. Workforce Categories are composed of Specialty Areas, each of which is composed of one or more Work Roles. Each Work Role, in turn, includes KSAs and Tasks. Grouping components in this manner simplifies communication about cybersecurity workforce topics and helps with alignment to other frameworks. The associations of Work Roles to KSAs and Tasks are illustrated in the infographic below:



National Initiative for Cybersecurity Education (NICE)

Securely Provision	Operate & Maintain	Oversee & Govern	Protect & Defend	Analyze	Collect & Operate	Investigate
Risk Management	Data Administration	Legal Advice & Advocacy	Cybersecurity Defense Analysis	Threat Analysis	Collection Operations	Cyber Investigation
Software Development	Knowledge Management	Training Education and Awareness	Cybersecurity Defense Infr Analysis	Exploitation Analysis	Cyber Operations Planning	Digital Forensics
Systems Architecture	Customer Service & Tech Support	Cybersecurity Management	Incident Response	All-Source Analysis	Cyber Operations	
Technology R&D	Network Services	Strategic Planning & Policy	Vulnerability Assessment & Management	Targets		
Systems Requirements Planning	Systems Administration	Executive Cyber Leadership		Language Analysis		
Test & Evaluation	Systems Analysis	Program/Project Management & Acquisition				
Systems Development						

Organizes Work Roles into Categories & Specialty Areas

Defines Knowledge Skills Abilities (KSAs)

Associates Tasks

ESTABLISHMENT OF RESEARCH GOALS

This study will examine a handful of states to identify and record how each state's career clusters and pathways framework is designed, published, disseminated, managed, evaluated and updated. The study will explore how each state uses the framework to determine K-12 CTE teaching credentials and endorsements. Researchers will also examine how the framework is used to determine minimum qualifications to teach dual credit, dual enrollment and TechPrep classes. States were selected by their geographic proximity to the CSSIA center and the state's reputation for having high-quality K-12 and two-year college cybersecurity programs. The states that participated in this study include Florida, Illinois, Indiana, Michigan, New York, Ohio and Wisconsin. As previously stated, the Coastline Community College project will study career pathways in the state of California, Dakota State University will study pathway programs in the Dakotas and the Mohawk Valley Community College study will work with the CTE community in New York State.

SELECTION OF A GATEKEEPER

In the process of establishing statewide focus groups, the Moraine Valley Community College research team identified and contracted a lead representative from each state in the study. These individuals would serve as gatekeepers or primary point of contact in each state participating in the study. Research is now an integral part of the study and continuous improvement of educational programs. Research teams need to be responsive to meet the changing needs in light of evidence-based research findings.

Within this process, gatekeepers have a key role to ensure researchers gain access to potential participants and sites for research. The positive influences of the gatekeepers were invaluable to the research process. These individuals were selected based on their participation and leadership as an NSA Center of Academic Excellence designation. The gatekeepers are listed below:

LIST OF GATEKEEPERS

- **California** – Nancy Jones, Dean of Career and Technical Education, Coastline Community College
- **Dakotas** – Wayne Pauli, Professor of Information Systems, Dakota State University
- **Florida** – Ernie Friend, CAE Instructional Program Manager, Florida State College, Jacksonville
- **Indiana** – Pam Schmelz, Faculty and Jiri Jirik, Associate Professor, School of Information Technology, Ivy Tech Community College
- **Illinois** – Stan Kostka, CAE Regional Resource Center Manager, Moraine Valley Community College
- **Michigan** – Lonnie Decker, Computer Information Systems Department Chair, Davenport University
- **New York** – Jake Mihevc, Dean of the School of STEM, Mohawk Valley Community College
- **Ohio** – Kyle Jones, Department Chair, Computer Information Systems, Sinclair College
- **Wisconsin** – Michael Masino, Information Security Program Director, Madison Technical College

GRANT GOALS AND OBJECTIVES

The faculty and staff at Moraine Valley Community College received a grant award to conduct a nationwide study of Cybersecurity pathways of study. The goals of the grant are listed below.

GOAL #1:

Identifying existing cybersecurity pathways that span between K-12 programs and institutions of higher education.

OBJECTIVE #1:

Host a series of state-wide CTE summits that bring together key stakeholders from K-12, community colleges, career and academic advisors and employers in an effort to identify existing programs of study and best practices.

OBJECTIVE #2:

Share existing programs for school officials interested in building pathways of study for cybersecurity careers within their local school districts.

GOAL #2:

Examine new models including articulation agreements, dual credit programs, internships and apprenticeships that enable students to gain an early start in preparing for careers in cybersecurity.

OBJECTIVE #1:

Engage local employers to examine the establishment of internship and apprenticeship programs.

OBJECTIVE #2:

Work with local school districts to establish formal pathways of study that enables high school students to earn college credit.

OBJECTIVE #3:

High school faculty from these districts will attend faculty development workshops in preparing to launch the new programs.

GOAL #3:

Study potential efforts to increase the visibility of a cybersecurity pathway within the national and state career pathways and career clusters publications.

OBJECTIVE #1:

The new proposed programs were also shared with officials from NSA, NIST and the U.S. Department of Education for dissemination to other schools interested in modeling this program.

OBJECTIVE #2:

Collaborate with state officials from their respective state Departments of Education to formally adopt new marketing materials and state frameworks for establishing a cybersecurity career cluster and a full pathway of study model.

OBJECTIVE #3:

Serve as a framework for other states interested in updating their CTE pathways of study to incorporate cybersecurity programs.

EMPIRICAL RESEARCH QUESTIONS

RESEARCH QUESTIONS

The research questions explored in the study include:

1) Did states and academic institutions progressively design and implement career cluster and pathways within the existing U.S. Department of Education framework, or did key stakeholders work outside the framework to implement new cybersecurity pathways?
2) Do the states selected in the study have formal processes for examining, updating and distributing revisions to the states existing career cluster and pathways framework?
3) Who is responsible in each state for maintaining the framework, supplemental services and formal publications?
4) What are the model programs and best practices within each state's K-12 and two-year college cybersecurity articulation programs?
5) What are the obstacles and challenges in maintaining and updating the Career Clusters framework?

ASSOCIATED DATA RESOURCES

BENEFIT OF WELL-DESIGNED CAREER PATHWAYS SYSTEMS

According to focus group members, the benefits of a well-designed and implemented career pathway system provides students and a local workforce with the following opportunities:

1) Students develop awareness of career fields, the skills needed, credentials required and courses that need to be taken as part of a certificate or degree.
2) Reduction in duplicate efforts in repetitive course content.
3) Increase number of students interested in careers in high demand.
4) On-ramp and bridge programs for disadvantaged and diverse populations including underprepared students with limited basic skills, and youth and adults with barriers to employment.
5) Stackable credentials that allow students to begin employment earlier and traverse steps to advanced professions.
6) Work based learning opportunities including work-study programs, internships and apprenticeships.
7) Increased retention and graduation rates.
8) Accelerated program completion and time to employment.
9) Decreased cost for program completion.
10) Alignment to workforce needs.

ESSENTIAL RESOURCES FOR SUSTAINABLE K-12 CYBERSECURITY PROGRAMS

Faculty participants in the focus groups identified the following best practices. In particular, high school instructors identified these elements essential to building sustainable high school cybersecurity programs. These include the following:

- relevant technical content
- faculty development based on technical certificates
- standardized assessment instruments and methods
- hands-on experiential and contextualized learning
- accelerated skills building activities
- recognition of previous learned and earned credentials
- flexible class schedules
- cohort-based instruction
- combinations of online and face-to-face instruction
- safe virtual teaching and learning environments
- gamification of learning activities

STRATEGIC PARTNERSHIPS

Participants in the focus groups identified the following strategic partnerships:

- K-12 institutions with a focus on CTE programs
- technical and community colleges
- 4-year colleges and universities
- community-based organizations
- business and industry certification organizations
- employers
- key cybersecurity industry leaders

PROGRAM DESIGN BEST PRACTICES

Participants in the study identified the following program design best practices in establishing sustainable cybersecurity career pathways:

- multiple entry and exit points
- multiple postsecondary pathways
- marketable credentials at each step
- link between noncredit & credit training
- short term stackable credentials
- long term advanced credentials
- worksite training
- internships and apprenticeships
- placement services
- financial support services
- workforce skills
- pathways that support regional workforce needs

Many of these program design best practices reflect best practices of successful career pathway programs. Cybersecurity programs do require some specialized key elements in preparing students for the workforce. A large sector of the cybersecurity workforce involves federal, state and local agencies. These agencies face particular difficulty in finding qualified employees. These challenges are a result of employees having to qualify for security clearances. Many of these positions salary structures are not competitive with the private sector and the hiring cycles tend to be lengthier. For these reasons, academic institutions need to build stronger cross-agency partnerships. The cybersecurity field has matured and subdivided into a multitude of highly specialized Work Roles. The NIST framework currently identifies 52 different Work Roles. For this reason, academic institutions need to identify industry sectors and engage potential employers in order to build programs that prepare students for the applicable Work Roles in their community. Many of these Work Roles require substantially different knowledge, skills and abilities. This information provides a critical framework for the design of effective and relevant education and training programs. Cybersecurity programs are unique in that they require continuous updating of technology, products, threats, vulnerabilities and countermeasures. The constant need to update these programs results in additional cost and attention to faculty development and program improvement. These considerations need to be part of the funding and budgeting for these programs. Business partnerships and sponsorships can be used to reduce these costs.

One of the greatest challenges of developing cybersecurity programs in K-12 institutions is the alignment of institutional policies and programs. Most K-12 institutions security policies require instructional workstations and networks to be locked down. Students are monitored and restricted from visiting a large majority of websites that may be beneficial and provide resources in the classroom. As a result, K-12 instructors identify the need for safe, virtual teaching and learning environments as a critical element needed to build engaging and relevant instruction. Our study identifies this challenge as one of the most important challenges in developing sustainable cybersecurity programs.

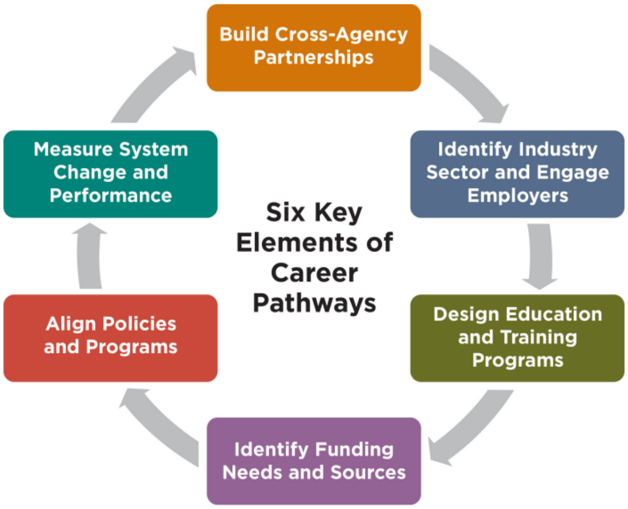

Build Cross-Agency Partnerships
Identify Industry Sector and Engage Employers
Design Education and Training Programs
Identify Funding Needs and Sources
Align Policies and Programs
Measure System Change and Performance
Six Key Elements of Career Pathways

Figure 1: Six Key Elements for Developing Career Pathways Systems

The final element in building effective cybersecurity programs is the continuous assessment of existing programs. Several participants identified external instruments for measuring program performance including industry certifications, student competitions and micro-badging programs. The use of external assessments provides a more meaningful measure of program success.

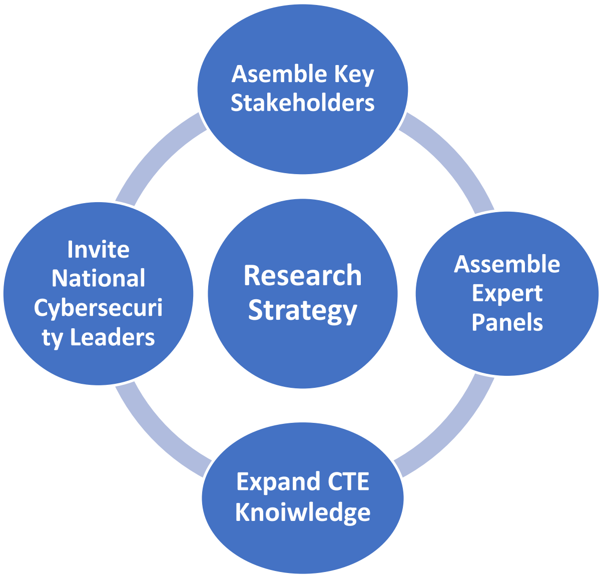
RESEARCH STRATEGY

This study will primarily depend on qualitative data collection. Quantitative research is focused on testing and answering research questions or hypotheses. Based on the hypotheses and subject examined the research team planned and organized a series of statewide meetings with key stakeholders of career path programs in each state. The meetings served three purposes:

1) Each meeting served as an opportunity to bring cybersecurity career pathways stakeholders in each state including state leaders of CTE programs, CTE teachers, professors, counselors, advisors, students and employers.
2) Each meeting included the assembly of expert panels to explore and answer research questions.
3) Each meeting sought to improve communications and understanding of cybersecurity career pathway programs in each state participating in the study.
4) Each meeting provided an opportunity for local state stakeholders to connect with national leaders from federal agencies to provide information concerning resources and services available to stakeholders of cybersecurity career pathways programs.

STATE	MEETING DATE
Indiana	September 27, 2018
Ohio	November 2, 2018
Michigan	December 14, 2018
Florida	March 1, 2019
Illinois	March 21, 2019
New York	March 22, 2019
Wisconsin	June 21, 2019

The research team also interviewed stakeholders individually to gain insight and better understanding of the processes and programs in each state. The team also researched the website for each State's Department of Education to better understand the organization of CTE education programs in the state.



DESCRIPTION OF PARTICIPANTS

STATE CAREER AND TECHNICAL EDUCATION (CTE) LEADERSHIP

Each state typically has an office for CTE programs within their state Department of Education. In some states, there are multiple people within the CTE program. We found that the majority of states employ a director of Career and Technical Education programs. In other states, the key state CTE leadership actually come from the community college system, university system or officeholders in their state Association for Career and Technical Education (ACTE). The smaller, rural states tended not to have a director of CTE at the state level.

REGIONAL CAREER AND TECHNICAL EDUCATION (CTE) DIRECTORS

Many of the states that participated in the study have regional or district Career and Technical Education Directors. These individuals are typically employees of the local school districts. In some cases, there is a separate organization that serves multiple districts in a larger region within the states. We found some states divided their CTE region by county. Florida was an example of this type of system.

DISTRICT AND INSTITUTION DIRECTORS

Several states in the study had both district and institutional Career and Technical Education Directors. These institutions were employees of the school districts or individual high schools. A few states in the study have high schools dedicated to career and technical education. Wisconsin was an example. Illinois also has what are called area career centers.

HIGH SCHOOL CAREER AND TECHNICAL EDUCATION (CTE) FACULTY

The study involved high school CTE faculty. In most states, the CTE faculty represented the information technology career cluster. Faculty invited to our events were directly involved in career pathway programs including dual credit, dual enrollment or TechPrep programs. A few states also include cybersecurity concepts that are taught in the business programs. In most cases, the cybersecurity occupation emerged from the information technology career field; however, it no longer accurately represents the makeup of the current cybersecurity workforce.

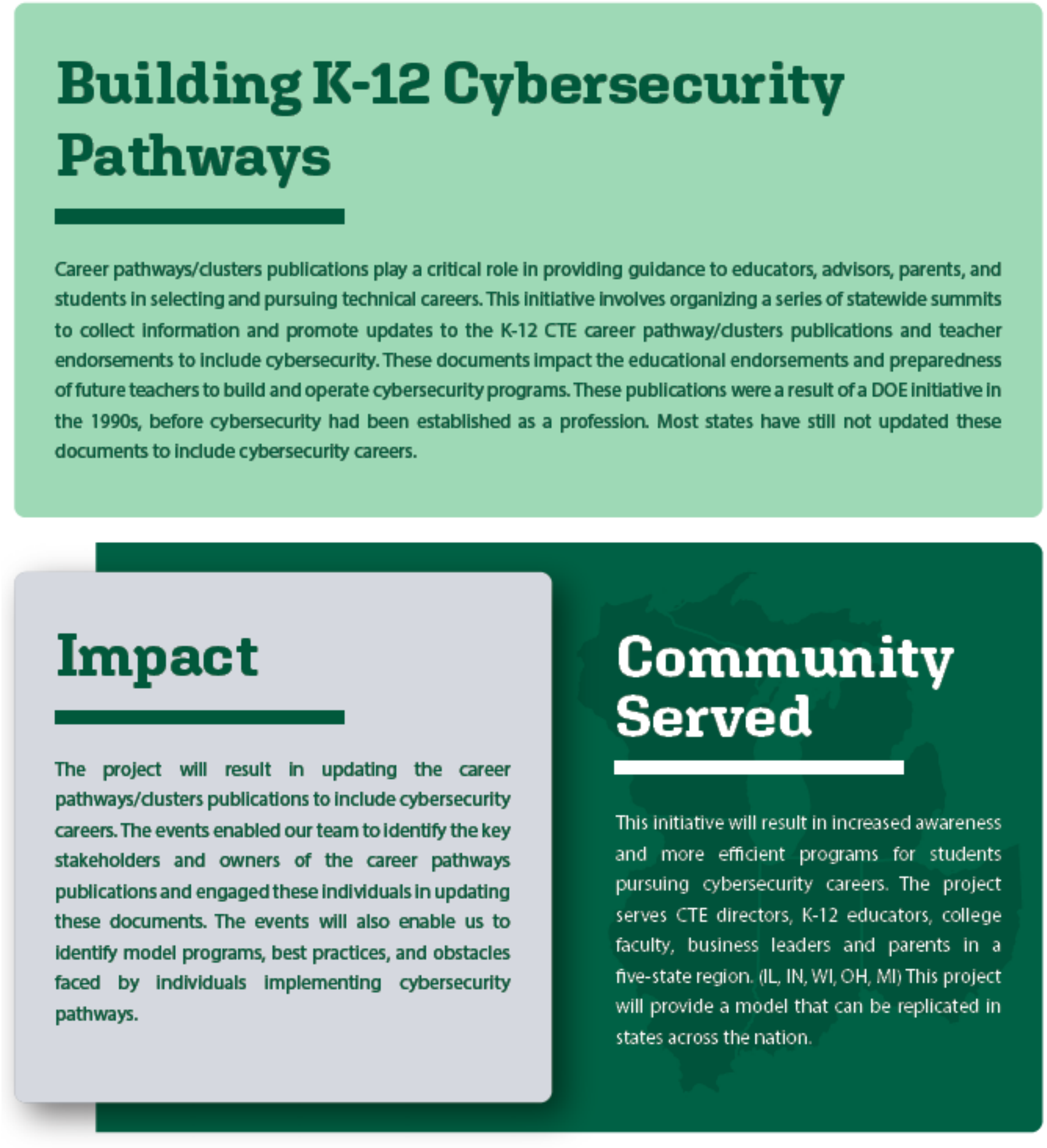
COMMUNITY COLLEGE FACULTY

The research team also invited community college faculty to the statewide focus groups. Most faculty attending the events were directly involved in dual credit, dual enrollment and TechPrep programs. The faculty represented the following programs:

- Cybersecurity
- Business
- Computer Technologies
- Information Systems
- Information Technology
- Computer Science
- Criminal Justice

4-YEAR COLLEGE AND UNIVERSITY FACULTY

The research team invited representatives from 4-year colleges and universities based on their involvement in transfer and articulation agreements with 2-year colleges. A few of the states have very strong feeder programs from K-12 and community colleges to local universities. The state of Ohio was probably the best example of these partnerships. It is worth noting that several institutions are establishing Baccalaureate Applied Sciences in cybersecurity. These programs will provide expanded opportunities for students from career pathway programs in cybersecurity.



Building K-12 Cybersecurity Pathways

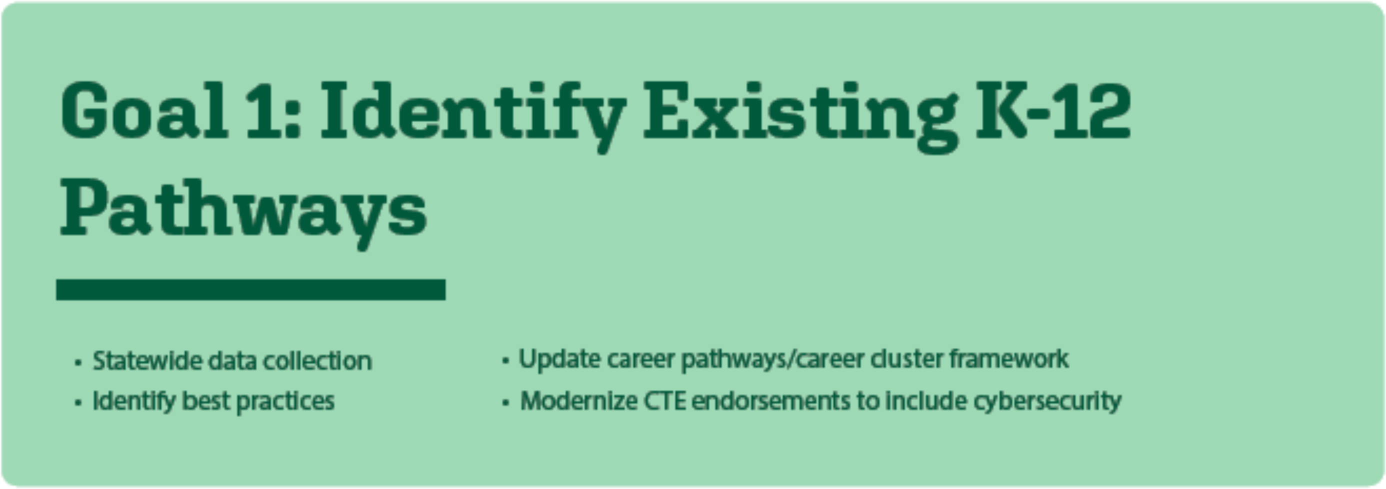
Career pathways/clusters publications play a critical role in providing guidance to educators, advisors, parents, and students in selecting and pursuing technical careers. This initiative involves organizing a series of statewide summits to collect information and promote updates to the K-12 CTE career pathway/clusters publications and teacher endorsements to include cybersecurity. These documents impact the educational endorsements and preparedness of future teachers to build and operate cybersecurity programs. These publications were a result of a DOE initiative in the 1990s, before cybersecurity had been established as a profession. Most states have still not updated these documents to include cybersecurity careers.

Impact

The project will result in updating the career pathways/clusters publications to include cybersecurity careers. The events enabled our team to identify the key stakeholders and owners of the career pathways publications and engaged these individuals in updating these documents. The events will also enable us to identify model programs, best practices, and obstacles faced by individuals implementing cybersecurity pathways.

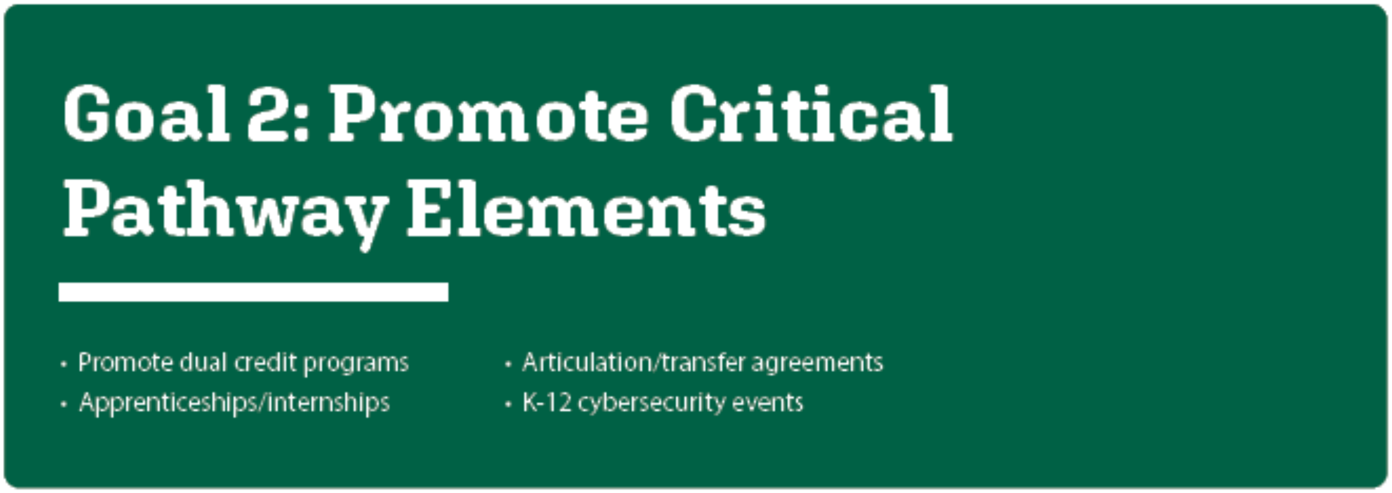
Community Served

This initiative will result in increased awareness and more efficient programs for students pursuing cybersecurity careers. The project serves CTE directors, K-12 educators, college faculty, business leaders and parents in a five-state region. (IL, IN, WI, OH, MI) This project will provide a model that can be replicated in states across the nation.



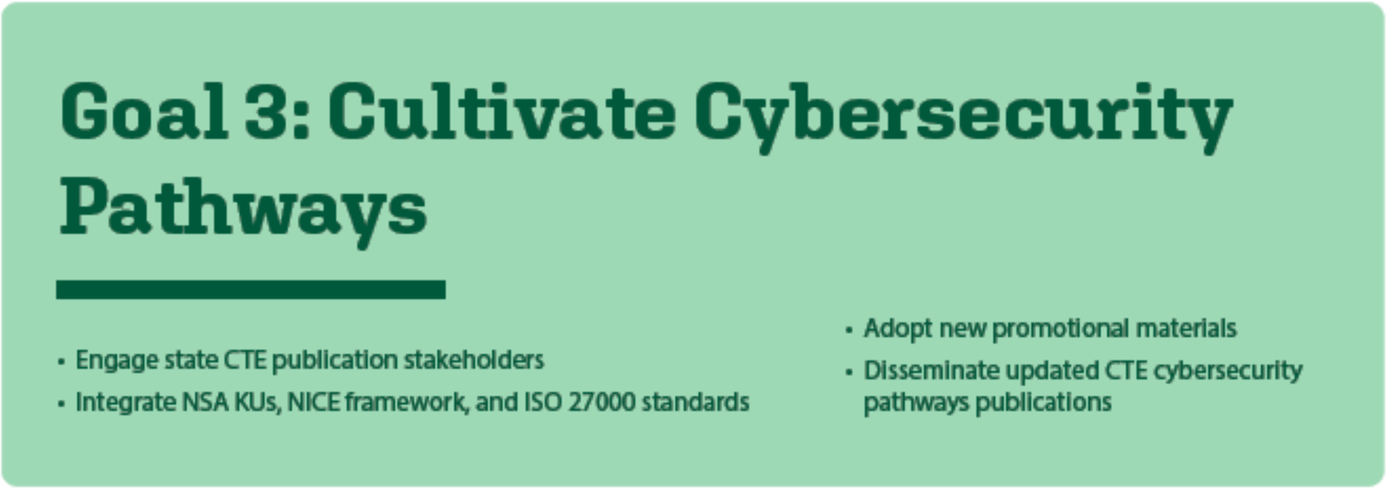
Goal 1: Identify Existing K-12 Pathways

- Statewide data collection
- Identify best practices
- Update career pathways/career cluster framework
- Modernize CTE endorsements to include cybersecurity



Goal 2: Promote Critical Pathway Elements

- Promote dual credit programs
- Apprenticeships/internships
- Articulation/transfer agreements
- K-12 cybersecurity events



Goal 3: Cultivate Cybersecurity Pathways

- Engage state CTE publication stakeholders
- Integrate NSA KUs, NICE framework, and ISO 27000 standards
- Adopt new promotional materials
- Disseminate updated CTE cybersecurity pathways publications

FLORIDA

FLORIDA CTE AND CAREER PATHWAYS SYSTEM

The state of Florida has:

State of Florida CTE and Career Pathways Systems	
746	Public High Schools
53	Public High Schools Offering Solely/Primarily CTE Courses
793,367	Public High School Enrollment
341,648	High School CTE Enrollment
133,648	High School CTE Concentrators
60	Public Community Colleges
59,358	Public Community Colleges Enrollment (full & part-time)
105,937	Postsecondary CTE Enrollment
81,067	Postsecondary CTE Concentrators

FLORIDA CTE STRUCTURE

The state of Florida has a very well organized and state led CTE program including cybersecurity career pathways programs. The Florida Department of Education organizes CTE programs across each of its three delivery systems into 17 Career Clusters based on state workforce requirements and based on The National Career Clusters Framework. The career programs in Florida are offered by the following types of educational institutions:

- Comprehensive high schools
- Charter schools
- Career academies
- Early college high schools
- Area technical centers
- Community colleges

FLORIDA CTE CAREER CLUSTERS

1. Agriculture, Food & Natural Resources Career Cluster	10. Architecture & Construction Career Cluster
2. Arts, A/V Technology & Communication Career Cluster	11. Business Management & Administration Career Cluster
3. Education & Training Career Cluster	12. Energy Career Cluster
4. Engineering & Technology Education Career Cluster	13. Finance Career Cluster
5. Government & Public Administration Career Cluster	14. Health Science Career Cluster
6. Hospitality & Tourism Career Cluster	15. Human Services Career Cluster
7. Information Technology Career Cluster	16. Law, Public Safety & Security Career Cluster
8. Manufacturing Career Cluster	17. Marketing, Sales & Service Career Cluster
9. Transportation, Distribution & Logistics Career Cluster	

FLORIDA PROGRAMS OF STUDY/CAREER PATHWAYS

Florida approves programs of study developed in each of the state's 17 Career Clusters. Each local program of study must include the following:

- A written articulation agreement must be in place for each Program of Study that establishes and validates the career pathway. All articulation agreements must be signed and approved by the agency head of each participating secondary and postsecondary local education agency (LEA).
- A locally endorsed sequence of core academic and CTE courses from Grade 9 through the postsecondary component of the Program of Study.
- A pathway leading to a postsecondary credential. This may include a certificate, diploma, associate or baccalaureate degree, an industry certification or licensure. In general, career pathways should offer students opportunities for continued education as well as access to the skilled workforce.
- Each Program of Study is expected to be guided by the workforce and economic development needs of business / industry, the community and employment opportunities for students.

FLORIDA CTE/CAREER PATHWAYS MEETING LOGISTICS

The Moraine Valley Community College (MVCC) team coordinated the event with Ernie Friend of Florida State College at Jacksonville on March 1, 2019. The event was held at their Advanced Technology Center in Room T112. This event included representatives from the State of Florida Department of Education, CTE representatives from four local counties, high school teachers, community college faculty, counselors, academic advisors and business and industry representatives. The State of Florida has made cybersecurity programs one of the state’s highest priorities in CTE programs. Florida has modeled programs including middle college programs hosted at their community college institutions, dual credit and dual enrollment.

Florida Department of Education: www.fldoe.org

Advance CTE: State Leaders Connecting Learning to Work: www.careertech.org/florida

FLORIDA CTE/CAREER PATHWAYS MEETING LOCATION & AGENDA

LOCATION

March 1, 2019
Florida State College at Jacksonville
Advanced Technology Center – Room T112
401 West State Street, Jacksonville, FL 32202

AGENDA

10:00am-10:30am	**Registration**
10:30am-10:45am	**Welcome** **Ernie Friend** **Dr. Sheri Litt**, Associate Provost for Baccalaureate and Career Education
10:45am–11:00am	**Cybersecurity Pathways** **John Sands, Computer-Integrated Technology Department Chair, Moraine Valley Community College**
11:00am-11:30pm	**Where is Cyber: Current CTE Clusters and Consequent Pathways** *CTE Panel:* **Eric Owens** - Senior Educational Program Director Division of Career and Adult Education FLDOE **Brent Lemond** - Director of Career and Adult Education Nassau County School District **Wendy Dunlap** - Director, School Counseling & Acceleration Programs Duval County Public Schools
11:30am–12:00pm	Government's role in supporting Educators preparing students for cybersecurity careers. *Speaker:* **Chris Valencia** - Chief, Active Cybersecurity (Y254) Information Assurance Security Center NSA
12:00pm-12:30pm	**Lunch and Networking**
12:30pm-1:00pm	**Who are our Students: Pathways to Cyber** *College Panel:* **Clair Hart** - FSCJ **Ernie Friend** – Instruction Program Manager **Regis Frederick**- Advisor Counselor FSCJ **Julie Stein**- Program Manager FSCJ
1:00pm-1:30pm	**HS & Middle College** – Best Practices in Building Cybersecurity Pathways *Panelists:* **Mary Hall** - Clay County **Cassie Solliday** – Duval County **Kalvin Thompson** - Nassau County **Kathy Sinardi** – St Johns County
1:30pm-2:00pm	**NICE K-12 - Career Opportunities in Today's Cyber Workplace** *Speaker:* **Davina Pruitt-Mentle**
2:00pm - 2:30pm	**Employers panel** – High Paid, High Demand Jobs of Tomorrow *Panelists:* **Ana Fraxedas** - Marketing Coordinator TSYS **Kathleen Schofield** - Executive Director, STEM2 Hub **Roben Faircloth** - CareerSource Northeast Florida **Taryn Swietek** - Vulnerability Assessments – Team Manager Global Consumer Information Security CITI
2:30pm–3:00pm	Closing Remarks – **Dr. John Sands**

KEY STATE LEVEL CTE STAKEHOLDERS

- **Eric Owens** - Senior Educational Program Director, Division of Career and Adult Education, FLDOE
- **Brent Lemond** - Director of Career and Adult Education, Nassau County School District
- **Wendy Dunlap** - Director, School Counseling & Acceleration Programs, Duval County Public Schools
- **High School CTE Faculty**
- **Community College Faculty**
- **Councilors and Advisors**
- **Business and Industry Leaders**

PROGRAMS OF STUDY/CAREER PATHWAYS

The state of Florida has several unique programs in cybersecurity from dual credit to middle college programs. The cybersecurity pathways in Florida are associated with the Information Technology career cluster. The state incorporates the following supplemental services as part of the cybersecurity pathways:

HIGH SCHOOL CLASSES

Like most states, the cybersecurity programs are located in the Information Technology Career cluster. The state formally identifies the following cybersecurity career pathway programs. These pathways include dual credit classes in the following programs:

- Applied Cybersecurity Career Preparatory (Program Number: 9001300)
- Applied Cybersecurity Career Preparatory (Program Number: Y100300)
- Cybersecurity Associate in Science Degree (CIP Number: 1511100308)

HIGH SCHOOL STUDENT CYBERSECURITY COMPETITIONS

The state of Florida's cybersecurity students have a multitude of options when it comes to participating in cybersecurity skills competitions. The list below represents several of the programs regularly attended by Florida students.

- National Cyber League
- CyberPatriot
- National Collegiate Cyber Defense Competition (CCDC)
- Department of Energy CyberForce
- Cybersecurity Awareness Week Competition (CSAW)
- National Cyber Analyst Challenge and Conference (NCAC)

GENCYBER CAMPS

The state of Florida has been awarded several GenCyber grants. The following is a list of recent GenCyber camps operated with this funding:

- University of Florida
- University of West Florida Pathways to Cyber Program
- University of Central Florida, Center for Initiatives in STEM
- University of South Florida, Florida Center for Cybersecurity

CAE CENTERS

The state of Florida, at the time of this study has 16 Centers of Academic Excellence. The list below represents current programs:

1) Daytona State College
2) Embry-Riddle Aeronautical University - Daytona Beach Campus
3) Florida A & M University
4) Florida Atlantic University
5) Florida Institute of Technology
6) Florida International University
7) Florida State College at Jacksonville
8) Florida State University
9) Indian River State College
10) Nova Southeastern University
11) Saint Leo University
12) University of Central Florida
13) University of Florida
14) University of South Florida
15) University of West Florida
16) Valencia College

STATE APPROVED CYBERSECURITY CAREER PATHWAYS PROGRAM

MIDDLE SCHOOL COURSES

- Coding Fundamentals (Course Number: 9009200)
- Digital Discoveries in Society (Course Number: 9009600)
- Exploring Information Technology Careers (Course Number: 9009350)
- Exploring Information Technology Careers & Career Planning (Course Number: 9009360)
- Fundamentals of Networking and Information Support (Course Number: 9009400)
- Information and Communications Technology (ICT) Essentials (Course Number: 9009100)
- Information and Communications Technology (ICT) Essentials Careers & Career Planning (Course Number: 9009370)

SECONDARY COURSES/PROGRAMS

- Applied Cybersecurity (Course Number: 9001300)
- Cloud Computing & Virtualization (Course Number: 9001500)
- Computer Science Principles (Course Number: 9007600)
- Integrated Information Technology (Course Number: 9003500)
- Java Development & Programming (Course Number: 9007200)

CAREER CERTIFICATE PROGRAMS

- Applied Cybersecurity (Program Number: Y100300)
- Applied Information Technology (Program Number: Y300400)
- Enterprise Desktop and Mobile Support Technology (Program Number: Y300600)
- Java Development & Programming (Program Number: Y700200)
- Network Support Services (Program Number: B078000)

DEGREE & CERTIFICATE PROGRAMS

- Business Intelligence Specialist Associate in Science Degree (Program Number: 1552130101)
- Computer Information Technology Associate in Science Degree (Program Number: 1511010307)
- Information Technology Analysis College Credit Certificate (Program Number: 0511010312)
- Information Technology Support Specialist College Credit Certificate (Program Number: 0511010311)
- Mobile Device Technology College Credit Certificate (Program Number: 0511010309)
- Computer Programming and Analysis Associate in Science Degree (Program Number: 1511020101)
- Internet of Things Applications College Credit Certificate (Program Number: 0511020110)
- Cybersecurity Associate in Science Degree (Program Number: 1511100308)
- Internet Services Technology Associate in Science Degree (Program Number: 1511080103)
- IT Security Associate in Science Degree (Program Number: 1511100307)
- Digital Forensics College Credit Certificate (Program Number: 0511100119)
- Network Security College Credit Certificate (Program Number: 0511100118)

COOP AND INTERNSHIPS

- Information Technology Cooperative Education - OJT (Program Number: 9000420)
- Information Technology Directed Study (Program Number: 9000100)

APPROVED COLLEGE DEGREE AND CERTIFICATE PROGRAMS

SCHOOL NAME	PROGRAMS	NSA
Daytona State College	• Advanced Technical Certificate – Cybersecurity and Cyberforensics	NSA CAE
Embry-Riddle Aeronautical University	• Master of Science in Cybersecurity Engineering	
Florida Agricultural and Mechanical University	• Master of Science in Cybersecurity Management and Policy	NSA CAE
Florida Atlantic University	• Cyber Defense Certificate	NSA CAE
Florida Institute of Technology	• Information Assurance Certificate	NSA CAE
Florida International University	• Bachelor of Management Information Systems (MIS) – specialization in Information Security and Business Analytics	
Florida Polytechnic University	• Master of Science in Applied Mathematics and Statistics – cryptology track	
Florida State College at Jacksonville	• MBA in Cybersecurity	NSA CAE
Florida State University	• MS – Information Assurance & Cybersecurity	NSA CAE

Indian River State College	• Master of Science in Computer Engineering with a concentration in Network Security	
Keiser University	• Bachelor of Science in Computer Science: Information Assurance & Cyber Security	
Nova Southeastern University	• Associate in Science in IT Security	NSA CAE
Palm Beach State College	• Technical Certificate in Digital Forensics	
Pasco-Hernando State College	• Master of Science in Computer Science – Cybersecurity Major	
Saint Leo University	• Associate of Arts in I.T. Management & Cyber Security	NSA CAE
St Petersburg College	• Cyber Forensics/Information Security, BS	
The University of West Florida	• Master of Science in Cybersecurity Management	
University of Central Florida	• Master of Science in Information Assurance & Cybersecurity	NSA CAE
University of Florida	• Associate in Science – Networking Administrator	NSA CAE
University of South Florida-Main Campus	• Bachelor of Applied Science in Information Management – Security and Network Assurance	NSA CAE
Valencia College	• Certificate in Network Security	NSA CAE

CAREER PATHWAYS INITIATIVE

On January 30, 2019, Governor Ron DeSantis issued Executive Order 19-31 that charts a course for Florida to become number one in the nation for workforce education by 2030 as well as ensuring that Florida students are prepared to fill the high-demand, high-wage jobs of today and the future.

Executive Order 19-31 directs Education Commissioner Richard Corcoran to audit career and technical education (CTE) offerings in the state and develop a methodology to audit and review offerings annually. The audit should include:

- An analysis of alignment with certificate or degree programs offered at the K-12 and postsecondary levels
- An analysis of alignment with professional level industry certifications
- An analysis of alignment with high-growth, high-demand and high wage employment opportunities
- A review of student outcomes such as academic achievement, college readiness, postsecondary enrollment, credential attainment and attainment of industry certifications

To accomplish the goals and vision of the Governor’s executive order, Florida Department of Education (FLDOE) will work with and utilize the expertise of CareerSource Florida, the Department of Economic Opportunity, the Board of Governors, the State College System, school districts and business and industry leaders to ensure CTE offerings are aligned with market demands.

Annually FLDOE will make recommendations to the Governor to eliminate CTE offerings that are not aligned to market demands, create new offerings aligned to market demands and strengthen existing CTE offerings as needed.

STUDENT CYBERSECURITY COMPETITIONS

The state promotes student competitions and has one of the large numbers of school participating in the CyberPatriot program.

School	No. of Teams	Division	Location
Ascension Catholic School	3 teams	Middle School	Melbourne
Belleview High School	1 team	All Service	Belleview
Civil Air Patrol, Clearwater	1 team	All Service	Largo
Creekside High School	13 teams	Open	Saint Johns
Cypress Bay High School	1 team	Open	Weston
Escambia County School District	1 team	Open	Pensacola
Evans High School	1 team	All Service	Orlando
Ferry Pass Middle	4 teams	Middle School	Pensacola
Galaxy Middle	2 teams	Middle School	Deltona
Lehigh Senior High School	1 team	All Service	Lehigh Acres
Melbourne Central Catholic High School	3 teams	Open	Melbourne
Pine Forest High School	5 teams	Open	Pensacola
Riverview High School NJROTC	2 teams	All Service	Riverview
South Fort Myers High School	1 team	All Service	Fort Myers
Wendell Krinn Technical High School- KTECH	1 team	Open	New Port Richey

STATEWIDE UNIVERSITY PROGRAM STANDARDS

The state of Florida has one of the best cybersecurity pathway systems in the nation. The state established the Cyber Florida program which works with each State University System of Florida (SUS). This program ensures cybersecurity academic programs align with industry needs, such as including a hands-on component, so students graduate ready to be hired. The list of Florida colleges and Universities represent the cybersecurity-specific degree and certificate programs offered by SUS institutions.

- Florida A&M University
- Florida Atlantic University
- Florida Gulf Coast University
- Florida International University
- Florida Polytechnic University
- Florida State University
- New College of Florida
- University of Central Florida
- University of Florida
- University of North Florida
- University of South Florida
- University of West Florida

OVERALL SUMMARY OF FLORIDA CYBERSECURITY PATHWAYS

The state of Florida has embraced the opportunities currently associated with the cybersecurity workforce. The state has encouraged, funded, implemented and recognized the importance of strong career pathways for the student interested in cybersecurity related occupation. The funding models and state level recognition of middle, high school and college level programs could be replicated. The Cyber Florida program also provides an example of how states can standardize and improve cybersecurity program across the state. The interviews also revealed strong support from the business and industry partners. This would include co-op and internship programs.

STATEWIDE CHALLENGES TO MAINTAINING CYBERSECURITY CAREER PATHWAY PROGRAMS

Like many other systems across the nation the real obstacles and challenges faced by the state cybersecurity career pathways initiatives are listed below:

FACULTY

- Recruiting new faculty
- Salary discrepancy with business and industry
- Faculty and staff training and development
- Retention and retirements

OUTREACH

- More women
- More minorities
- Better outreach to middle and high schools

FACILITIES

- Cost
- Need for new technologies and products
- Security concerns
- Virtual and cloud based instructional content
- Keeping up with the moving target

BUSINESS AND INDUSTRY

- More internships
- Sponsorships
- Advisory members
- Adjunct faculty

STATEWIDE FINDINGS AND RECOMMENDATIONS

- The state of Florida has a very centralized Department of Education system. Each program offered from middle school through universities are well-documented and are building strong pathways for their cybersecurity programs.
- The state has well-defined processes for periodically examining and updating the career clusters framework.
- Cybersecurity pathway programs in Florida are primarily found in the information technology-related programs and computer science. Florida also has cybersecurity certificates and majors available in their business and engineering schools. A unique approach to cybersecurity pathways would be the inclusion of charter schools, career academies, and technical centers, and home-schooled students.
- Florida has a statewide articulation system mandated by the state and all 2-year; 4-year universities participate.
- The state of Florida promotes dual-credit, dual-enrollment, tech prep, and early college programs. Cybersecurity is taught as part of each of these statewide programs.

- Six of the major state universities offer cybersecurity programs. Cybersecurity programs range from high school courses through PhD programs. Florida would be a leading state when comparing number of graduates, number of programs, and number of institutions focusing on cybersecurity.
- The state also has a unique program for promoting and funding high school students pursuing industry certification. The state provided funding to the institutions based on the students successfully passing certification exams. The funding is used to reimburse students for the cost of the exams and help fund programs promoting industry certification.
- The state has executive-level support for cybersecurity education. As illustrated by the Governor Ron DeSantis' Executive Order 19-31 for Workforce Education Goals by 2030.

ILLINOIS

ILLINOIS CTE AND CAREER PATHWAYS SYSTEM

The state of Illinois has:

State of Illinois CTE and Career Pathways Systems	
742	Public High Schools
600,080	Public High School Enrollment
277,458	High School CTE Enrollment
29,950	High School CTE Concentrators
49	Public Community Colleges
620,056	Public Community Colleges Enrollment (full & part-time)
139,854	Postsecondary CTE Enrollment
24,700	Postsecondary CTE Concentrators

ILLINOIS CTE STRUCTURE

The Career programs in Illinois are offered by the following types of educational institutions:

- Comprehensive high schools
- Charter schools
- Area career centers
- Community colleges

ILLINOIS CTE CAREER CLUSTERS

Illinois maintains five college and career ready CTE program areas, under which the 16 Career Clusters fit:

1. Agricultural Education
2. Business, Marketing and Computer Education
3. Family and Consumer Sciences
4. Health Science Technology
5. Technology and Engineering Education (Industrial)

ILLINOIS PROGRAMS OF STUDY/CAREER PATHWAYS

Illinois has programs of study within each of the 16 Career Clusters but, does not maintain statewide CTE standards for any of the Career Clusters.

1. Agriculture, Food & Natural Resources Career Cluster	9. Architecture & Construction Career Cluster
2. Arts, A/V Technology & Communications Career Cluster	10. Business, Management & Administration Career Cluster
3. Education & Training Career Cluster	11. Finance Career Cluster
4. Government & Public Administration Career Cluster	12. Health Science Career Cluster
5. Hospitality & Tourism Career Cluster	13. Human Services Career Cluster
6. Information Technology Career Cluster	14. Law, Public Safety, Corrections & Security Career Cluster
7. Manufacturing Career Cluster	15. Marketing Career Cluster
8. Science, Technology, Engineering & Mathematics Career Cluster	16. Transportation, Distribution & Logistics Career Cluster

PERKINS ELIGIBLE AGENCY

The organization within the state of Illinois that received and distributes Perkins funding is the Illinois State Board of Education.

ILLINOIS CAREER PATHWAYS OPERATIONS

The state of Illinois was the first state the team examined in the K-12 CTE Cybersecurity Pathways study. The state operates an "Illinois Pathways" web portal. The portal serves as a hub for publications and information related to the establishment of Career Pathways systems in the state.

Illinois Pathways: www.illinoisworknet.com/ilpathways/Pages/default.aspx

The state of Illinois has a decentralized system for CTE programs. The state has several organizations that contribute to the state Career Cluster and Career Pathways Framework. The Office of Community College Research and Leadership (OCCRL) was established in 1989 at the University of Illinois at Urbana-Champaign. OCCRL is affiliated with the Department of Education Policy, Organization and Leadership in the College of Education. The OCCRL mission is to use research and evaluation methods to improve policies, programs, and practices to enhance community college education and transition to and through college for diverse learners.

The Illinois Community College Board (ICCB) and the Illinois State Board of Education (ISBE), along with other state, federal, and private foundation and not-for-profit organizations that support statewide CTE programs. Illinois Pathways are an innovative public-private education partnership that is organized to support local implementation of P-20 STEM Programs of Study by coordinating and reducing the transaction cost among statewide networks of education partners, businesses, industry associations, labor organizations, and other organizations. The state recognized nine Career Pathways:

- Agriculture, Food & Natural Resources
- Architecture & Construction
- Energy
- Finance
- Health Science
- Information Technology
- Manufacturing
- Research & Development
- Transportation, Distribution & Logistics

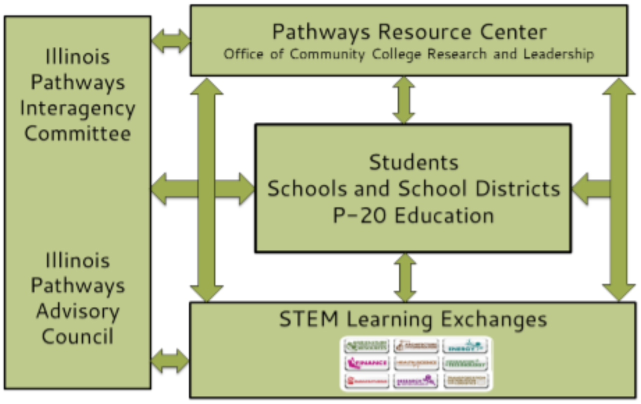
The partnership focuses on the following:

- secondary and postsecondary alignment
- seamless transition
- reduced remediation
- non-duplicated courses
- integrated academic and career-technical education (CTE) curricula
- dual credit opportunities
- standards-based curricula aligned with industry credentials and/or certification
- career development
- professional development
- articulation agreements
- data-sharing agreements
- partnerships and collaboration
- accountability
- continuous improvement

ILLINOIS CAREER CLUSTERS FRAMEWORK REVIEW AND MAINTENANCE PROCESS

The state of Illinois has established the Pathways Resource Center to review and maintain the formal publications and framework. The Pathways Resource Center (PRC) is a supportive and coordinating structure within Illinois' implementation of the 2012 Race to the Top III grant. In this capacity, the PRC serves as a centralized resource for local districts, their postsecondary and employer partners, and the Illinois STEM Learning Exchanges as they seek to:

- Create effective partnerships.
- Select and implement student programs of study within the Race to the Top career cluster areas.
- Implement curriculum reforms necessary to support their chosen programs of study and career cluster areas.
- Create and maintain sustainable and effective pathways for their student populations from P-12 schools to postsecondary education to careers. As part of the Illinois Pathways Initiative, the PRC has a number of associated partners, all working together to support schools and school districts as they work to ensure college and career success for their students.



Illinois Pathways Interagency Committee
Illinois Pathways Advisory Council
Pathways Resource Center
Office of Community College Research and Leadership
Students
Schools and School Districts
P-20 Education
STEM Learning Exchanges

ILLINOIS CTE/CAREER PATHWAYS MEETING LOGISTICS

The research team coordinated the event with Dr. Lazaro Lopez of District 214 at Forest View Educational Center in Arlington Heights, IL. The event was held on March 21, 2018 and was entitled "Developing Pathways for Cyber Careers in Illinois".

Illinois Cybersecurity Careers: www.il-cybersecurity.org

ILLINOIS CTE/CAREER PATHWAYS MEETING LOCATION & AGENDA

LOCATION

March 21, 2019
Forest View Educational Center
2121 S Goebbert Rd, Arlington Heights, IL 60005

AGENDA

11:00am-11:30am	**Registration and Lunch**
11:30am-12:00pm	**Leading the Way** Today's high school students are blazing the trails of cybersecurity. With pathway courses that help them creatively explore their interests, we are encouraging students to find their passion. We're going to hear from a couple of students who've done just that – had their interest sparked while in high school and have taken that interest to the next level. **Jack Cable:** White-Hat Hacker **Jimmy McDermott:** App Development
12:00pm-12:45pm	**Addressing the Cybersecurity Skills Gap with a "New Collar" Approach** With technology evolving so rapidly, it becomes harder for organizations to find candidates with the right skills to fill thousands of open IT jobs. Much of today's IT work requires specific skills and knowledge but may not require a university degree. Here is where IBM's New-Collar Initiatives fit in: New Collar focuses on skills (not degrees earned) around emerging technologies, including cybersecurity, design, data science, mobile development, cloud, support and project management **Heather Ricciuto:** Global Leader, IBM Security's Academic Outreach Programs, IBM
12:45pm-1:30pm	***Career Opportunities in Today's Cyber Workplace*** According to the Department of Homeland Security, promoting and expanding cybersecurity education is essential to protecting the Nation's critical infrastructure. In order for the United States to best protect our interests in the 21st century, educators must understand a new set of essential knowledge and skills that can prepare students to secure today's ever-evolving technologies. *Panelists:* ***Don Bora:*** *Co-Founder and Principal of Technology, Eight Bit Studios;* ***Kirk Havens:*** *Director Information Security Strategy, Discover,* ***Chris Hill:*** *Chief Information Security Officer, State of Illinois* ***Michael Lenz:*** *Senior Vice President, IT Security, MB Financial Bank* ***Nick Percoco:*** *Chief Security Officer, Uptake* ***Heather Ricciuto:*** *Global Leader, IBM Security's Academic Outreach Programs, IBM*

1:30pm-2:00pm	**Is Illinois Ready to Compete in a Global Marketplace?** IBM has partnered with 48 states and nations around the world to engage in strategic planning around a cybersecurity professional workforce. Where does Illinois stand in a globally competitive marketplace? *Speaker:* **Valinda Scarbro Kennedy:** IBM Midwest University Relations Program Manager, IBM
2:00pm-2:30pm	**Proposed Cyber Pathway Youth Apprenticeship Model** Illinois has celebrated its 10th anniversary implementing a career pathway model statewide. Many schools have successfully implemented Information Technology Programs of Study along two pathways: software development or hardware and networking. Cybersecurity professionals transcend both paths and, as such, a new youth apprenticeship model may provide the best opportunity for our students to enter the field. *Panelists:* **Julio Rodriguez:** Deputy Director, Office of Employment and Training, Illinois Department of Commerce and Economic Opportunity **John Sands:** Department Chair, Computer Integrated Technologies, Moraine Valley Community College **Dan Weidner:** Director of Academic Programs and Pathways, High School District 214
2:30pm-3:15pm	**Pathways to Higher Ed** Illinois has been focused on developing P20 models for Career Pathways that overlap institutional systems and lead students to persistence and completion. How do we design a program of study in cybersecurity that remains current in an ever-changing environment? How do we introduce a diverse student population as early as elementary school to the field? What experiences will best prepare students while in high school to transition seamlessly in higher education programs? *Facilitator:* **Brian Durham:** Deputy Director for Academic Affairs, Illinois Community College Board *Panelists:* **John Bambenek:** University of Illinois; Illinois Community College Board **Jack Cable:** White-Hat Hacker **Tony Chen:** Cyber Information Security Program Director, College of DuPage **Jimmy McDermott:** App Development **John Sands:** Department Chair, Computer Integrated Technologies, Moraine Valley Community College
3:15pm-4:00pm	**Scaling an Illinois Cyber Pathway** *Speakers:* **Jonathon Furr:** Education Systems Center, Northern Illinois University **Davina Pruitt-Mentle:** Lead for Academic Engagement, National Initiative for Cybersecurity Education (NICE) Participants will be briefed on key elements of the Postsecondary and Workforce Readiness Act impacting pathway design. They will then work in teams to identify local assets and partnerships that can be leveraged to begin, or expand, a cybersecurity pathway from awareness in elementary grades, certification opportunities in high school, and earning postsecondary credentials, as well as employment as a cybersecurity professional.

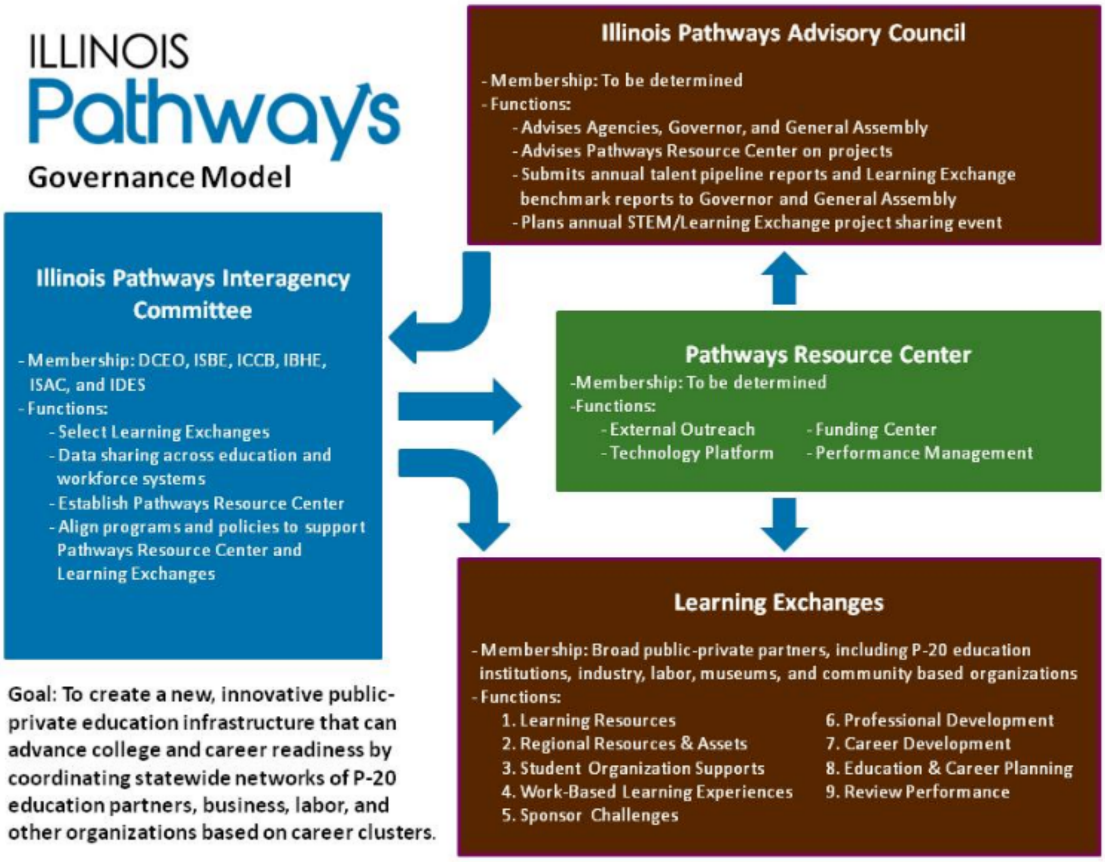
KEY STATE LEVEL CTE STAKEHOLDERS

- **Dr. Lazalo Lopez** - Associate Superintendent for Teaching & Learning
- **Dan Weidner** - Director, Academic Programs and Pathways
- **Scott McDermott** - Assistant Principal for Instruction, Prospect High School
- **Jeff Bott** - Career & Technical Education Division Head, Buffalo Grove High School
- **Bob Brown** - CTE Teacher, John Hersey High School
- **Paul Hennig** - CTE Teacher, Prospect High School
- **Tom Mroz** - CTE Teacher, Buffalo Grove High School

STATE DIRECTOR

Marci Johnson, Director of Teaching and Learning

Illinois State Board of Education
100 North First Street
Springfield, IL 62777
marjohns@isbe.net



ILLINOIS Pathways Governance Model

Illinois Pathways Advisory Council

- Membership: To be determined
- Functions:
  - Advises Agencies, Governor, and General Assembly
  - Advises Pathways Resource Center on projects
  - Submits annual talent pipeline reports and Learning Exchange benchmark reports to Governor and General Assembly
  - Plans annual STEM/Learning Exchange project sharing event

Illinois Pathways Interagency Committee

- Membership: DCEO, ISBE, ICCB, IBHE, ISAC, and IDES
- Functions:
  - Select Learning Exchanges
  - Data sharing across education and workforce systems
  - Establish Pathways Resource Center
  - Align programs and policies to support Pathways Resource Center and Learning Exchanges

Pathways Resource Center

- Membership: To be determined
- Functions:
  - External Outreach
  - Technology Platform
  - Funding Center
  - Performance Management

Learning Exchanges

- Membership: Broad public-private partners, including P-20 education institutions, industry, labor, museums, and community based organizations
- Functions:
  1. Learning Resources
  2. Regional Resources & Assets
  3. Student Organization Supports
  4. Work-Based Learning Experiences
  5. Sponsor Challenges
  6. Professional Development
  7. Career Development
  8. Education & Career Planning
  9. Review Performance

Goal: To create a new, innovative public-private education infrastructure that can advance college and career readiness by coordinating statewide networks of P-20 education partners, business, labor, and other organizations based on career clusters.

PROGRAMS OF STUDY/CAREER PATHWAYS

The state of Illinois has several unique programs in cybersecurity from dual credit to early college programs. The cybersecurity pathways in Illinois are associated with the Information Technology career cluster. The state incorporates the following supplemental services as part of the cybersecurity pathways:

HIGH SCHOOL STUDENT CYBERSECURITY COMPETITIONS

The students in the state of Illinois regularly participate in the following cybersecurity skills competitions:

- National Cyber League
- CyberPatriot
- National Collegiate Cyber Defense Competition (CCDC)
- U.S. Department of Energy Cyber Defense Competition
- Cyber Aces State Championship

GENCYBER CAMPS

The state of Illinois has received GenCyber awards to operate the following GenCyber camps:

- University of Chicago
- College of DuPage
- Moraine Valley Community College

CAE CENTERS

At the time of this study, the state of Illinois had 11 institutions that participate in the NSA CAE program and host the Midwest National Collegiate Cyber Defense Competition.

1) DePaul University
2) College of DuPage
3) Illinois Institute of Technology
4) Illinois State University
5) John A Logan College
6) Lewis University
7) Lincoln Land Community College
8) Moraine Valley Community College
9) Roosevelt University
10) University of Illinois at Springfield
11) University of Illinois, Urbana-Champaign

MIDDLE SCHOOL COURSES

- Coding Fundamentals (Course Number: 9009200)
- Digital Discoveries in Society (Course Number: 9009600)
- Exploring Information Technology Careers (Course Number: 9009350)
- Exploring Information Technology Careers & Career Planning (Course Number: 9009360)
- Fundamentals of Networking and Information Support (Course Number: 9009400)
- Information and Communications Technology (ICT) Essentials (Course Number: 9009100)
- Information and Communications Technology (ICT) Essentials Careers & Career Planning (Course Number: 9009370)

APPROVED COLLEGE DEGREE & CERTIFICATE PROGRAMS

SCHOOL NAME	PROGRAMS	NSA
College of DuPage	Associate in Applied Science in Cybersecurity and Defense	NSA CAE
DePaul University	Certificate in Information Assurance and Cyber Defense	NSA CAE
Eastern Illinois University	Master of Science in Cybersecurity	
Elmhurst College	Technology Security graduate certificate program	
Illinois Institute of Technology	Certificate in Cyber Security	NSA CAE
Illinois State University	Certificate in Information Security and Assurance	NSA CAE
John A Logan College	Master Certificate in Cyber Security Management	NSA CAE
Joliet Junior College	Master Certificate in Cyber Security Technologies	
Lewis University	Master of Cyber Forensics and Security Program	NSA CAE
Lincoln Land Community College	Information Assurance and Security Graduate Certificate	NSA CAE
McHenry County College	Master of Science in Information Systems-Network and Security Management	
Moraine Valley Community College	Associate in Applied Science in Computer Forensics	NSA CAE
Northeastern Illinois University	Associate in Applied Science in Cyber Security/Information Assurance	
Northwestern University	Computer Information Systems Computer and Network Security Specialist, Certificate of Achievement	
Purdue University Global	BS in Information Security and Risk Management	
Rock Valley College	Master of Science in Information Security (MSIS)	
Roosevelt University	Online Master of Science in Computer Science – Cyber Security Concentration	NSA CAE

Shawnee Community College	Associate in Applied Science in Computer Systems – Networking Track	
Southern Illinois University Carbondale	Certificate of Achievement in Computer Administration – Networking Track	NSA CAE
University of Illinois at Springfield	Cyber Security Certificate	NSA CAE
University of Illinois at Urbana-Champaign	Network Security AAS	NSA CAE

COOP AND INTERNSHIPS

- IDES' Apprenticeship Information Center Program (AIC)

CYBERSECURITY JOBS IN ILLINOIS

Greater Chicago has the fourth-most information security specialists in the country, with over 2,600. (www.cyberdegrees.org/listings/illinois/) However, there is a need for more, with 9,623 job postings in 2014, according to Burning Glass Technologies (Burning Glass Report). Its 164 percent growth rate in postings from 2010 to 2014 places it fifth on that list, meaning its already strong market for cybersecurity professionals is nowhere near saturation. Competitors DC, New York and Silicon Valley cannot argue the same.

Illinois does not have the same volume of cybersecurity firms as other states, but there are a few to keep an eye on. In particular, five firms made Cybersecurity Ventures' list of the hottest 500 companies in the field: Cimcor (#75), NowSecure (#124), Trustwave (#157), Flexera Software (#174) and Kenna (#338). They may not be big name companies but should be looked into for employment. For instance, Trustwave sponsors the Illinois Technology Association's annual Tech Challenge, partly so it can woo the top competitors away for internships.

Other big names include Boeing, United, and Discover. All Fortune 500 companies based in Illinois with information that needs to be protected from hackers. Two of the biggest insurance companies in the U.S., State Farm and Allstate, are also on the list as insurance is Illinois' biggest industry. With companies being hacked left and right, insurance companies are now offering cyber policies worth billions in premiums. To insure against security breaches, though, they have to understand the risks they pose, and TechCrunch anticipates the insurance industry to be a major growth area for cybersecurity professionals in the coming years.

CYBERSECURITY SALARIES IN ILLINOIS

At $87,690 per year, the median average salary for information security analysts is a slightly behind the national average of $90,120, according to the U.S. Bureau of Labor Statistics. However, the cost of living in Illinois is slightly below the national average.

Perhaps that is too general — most cybersecurity specialists will work in the Chicago Metropolitan Area, which is a little more costly to live in than the state at large. Even so, Indeed.com found that after adjusting for cost of living, Chicago placed sixth for average salary among the site's 15 most popular search destinations for tech jobs. That is better than rivals New York, DC and Los Angeles.

STUDENT CYBERSECURITY COMPETITIONS

The state promotes student competitions and has one of the largest numbers of school participating in the CyberPatriot program.

School	Number of Teams	Division
Elmhurst Cyber Club	4 teams	Open
ITW David Speer Academy	5 teams	All Service
John Hersey High School	2 teams	Open
Lake County-Palwaukee Composite Squadrons	1 team	All Service
Midwest Cyber Center -JB	1 team	Open
Shorty Powers Composite Squadron	1 team	All Service

OVERALL SUMMARY OF ILLINOIS CYBERSECURITY PATHWAYS

The state of Illinois has embraced the opportunities currently associated with the cybersecurity workforce. The state has encouraged, funded, implemented and recognized the importance of strong career pathways for the students interested in cybersecurity-related occupations. As a decentralized system, the cybersecurity programs in the state of Illinois are independent and do not have to meet or fall into categories established by the U.S. Department of Education. Dual credit programs exist within and outside of district and county boundaries. Institutions within the state of Illinois host virtual teaching and learning environments that can be used at no cost by high school educators incorporating cybersecurity content in their programs. The state of Illinois has officially placed cybersecurity programs under the Information Technology career cluster. K-12 teachers teaching cybersecurity are required to meet endorsements within this career cluster. The state of Illinois has provided both K-12 and community college faculty with multiple opportunities for faculty development in cybersecurity. Events like Working Connections hosted by Illinois Community College Board (ICCB) and the CSSIA National Faculty Development Center, located at Moraine Valley Community College, have provided these opportunities over the last decade. A common element in each of the state cybersecurity pathways include a 16-hour Orientation to Careers in Cybersecurity and a 32-hour course entitled Cybersecurity Essentials.

STATEWIDE CHALLENGES TO MAINTAINING CYBERSECURITY CAREER PATHWAY PROGRAMS

Like many other systems across the nation the real obstacles and challenges faced by the state cybersecurity career pathways initiatives are listed below:

STATE BUDGET CHALLENGES

- A decrease in funding for CTE programs
- A decrease in the number of students participating in CTE programs

FACULTY

- Recruiting cybersecurity faculty
- Retention
- Retirement
- Salary discrepancy with business & industry

BUSINESS AND INDUSTRY

- More internships
- Adjunct faculty

FACILITIES

- Budgets to update new technologies
- Security concerns
- Virtual & cloud-based instructional content
- Keeping up with the new threats & technologies

OUTREACH

- More women & minorities students & faculty
- Greater middle & high schools' awareness

STATEWIDE FINDINGS AND RECOMMENDATIONS

- The state of Illinois has a decentralized department of education system in which schools have increased latitude and authority to develop business-friendly programs that meet local workforce needs.
- The state lacks a formal process for periodic examination and updating of the career clusters framework, including cybersecurity programs.
- Cybersecurity pathway programs in Illinois are primarily found in the information technology-related programs and computer science. Illinois also has cybersecurity certificates and majors available in their business and engineering schools. Cyber forensics are also taught in some of the state criminal justice programs.
- Illinois has a statewide articulation program, but it is limited to general education programs. Career programs are required to establish institution-to-institution agreements for articulation of these classes.
- The state of Illinois promotes dual-credit, dual-enrollment, and tech prep. Cybersecurity is taught as part of each of these statewide programs.
- Three of the major state universities offer cybersecurity programs. Illinois has strong cybersecurity programs in several of the private and religious-affiliated institutions. Cybersecurity programs range from high school courses through PhD programs.
- Several community colleges in Illinois provide leadership and statewide resources including faculty development, instructional content, cybersecurity competitions, and mentoring for new and improvement of cybersecurity programs.
- Illinois has instituted several innovative dual-enrollment programs in which high school students can take college courses while still enrolled in high school.

INDIANA

INDIANA CTE AND CAREER PATHWAYS SYSTEM

The state of Indiana has:

State of Indiana CTE And Career Pathways Systems	
402	Public High Schools
28	Public High Schools Offering Solely/Primarily CTE Courses
317,482	Public High School Enrollment
167,611	High School CTE Enrollment
18,741	High School CTE Concentrators
16	Public Community Colleges
173,371	Public Community Colleges Enrollment (full & part-time)
27,972	Postsecondary CTE Enrollment
8,013	Postsecondary CTE Concentrators

INDIANA CTE STRUCTURE

The state of Indiana CTE programs is offered through the following institutions:

- Comprehensive high schools
- Charter schools
- Area Career centers
- Community colleges
- Four-year universities

INDIANA CTE CAREER CLUSTERS

Indiana has organized its secondary CTE programs into eleven College and Career Clusters, based in part on The National Career Clusters® Framework. The College and Career Clusters are as follows:

1. Agricultural	2. Architecture & Construction
3. Arts, AV Technology & Communication	4. Business & Marketing
5. Education & Training	6. Health Science
7. Hospitality & Human Services	8. Information Technology
9. Manufacturing	10. Public Safety
11. Transportation	

INDIANA PROGRAMS OF STUDY/CAREER PATHWAYS

Indiana offers programs of study derived from the following Career Clusters:

1. Agriculture, Food & Natural Resources Career Cluster	9. Architecture & Construction Career Cluster
2. Arts, A/V Technology & Communications Career Cluster	10. Business Management & Administration Career Cluster
3. Education & Training Career Cluster	11. Finance Career Cluster
4. Health Science Career Cluster	12. Hospitality & Tourism Career Cluster
5. Human Services Career Cluster	13. Information Technology Career Cluster
6. Law, Public Safety, Corrections & Security Career Cluster	14. Manufacturing Career Cluster
7. Marketing Career Cluster	15. Science, Technology, Engineering & Mathematics Career Cluster
8. Transportation, Distribution & Logistics Career Cluster	

INDIANA CTE/CAREER PATHWAYS MEETING LOGISTICS

The research team coordinated the event with Jiri Jirik, Information Technology Professor at Ivy Tech. The event was held at Ivy Tech's North Meridian Campus in Indianapolis, IN on September 27, 2018.

Cybersecurity Career Pathway: www.cyberseek.org/pathway.html

Indiana Department of Education: www.doe.in.gov/cte

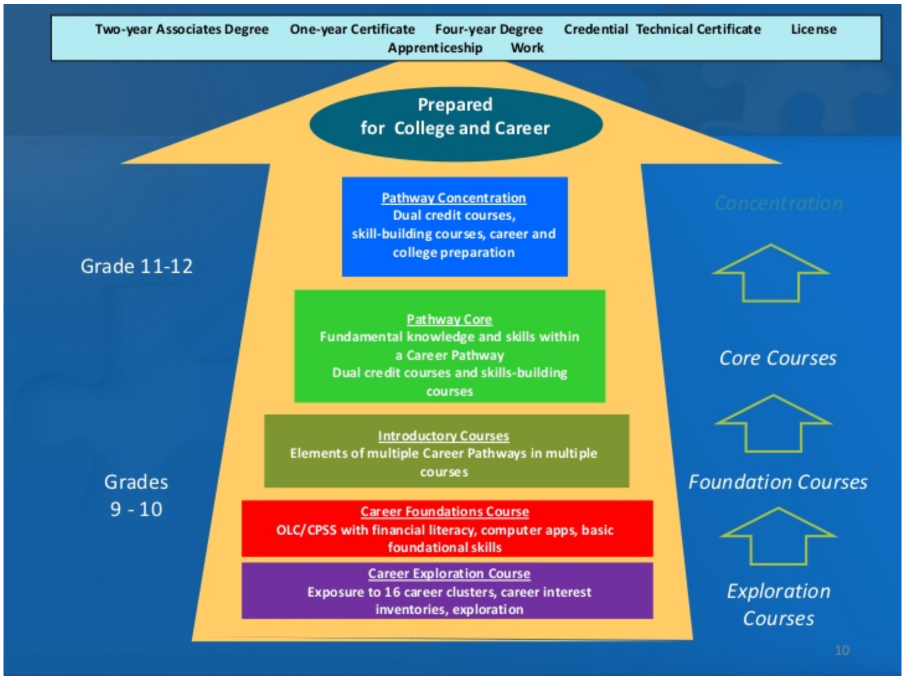
INDIANA CTE/CAREER PATHWAYS MEETING AGENDA

The administration, staff, and faculty at Ivy Tech would like to invite you to participate in a discussion regarding a future career pathway or cluster for cybersecurity in the state of Indiana. We will discuss ways to strengthen the opportunities for students to engage in this work by designing scalable pathways and learning the skills needed to access these "new collar" jobs.

LOCATION

September 27, 2018
Ivy Tech Community College
North Meridian Campus - Room 438
50 W Fall Creek Parkway North Drive, Indianapolis, IN 46208

10:00 am - 10:30 am	**Registration**
10:30 am - 10:45 am	**Welcome** **Dr. Monroe**, Provost and VP of Academic Affairs
11:00 am - 11:30 am	**CTE Panel** – Where is Cyber: Current CTE Clusters and Consequent Pathways *Panelists:* **Mike Ripperger** – CTE Director, Marion Regional Career Center **Michele Roberts** – Director of Computing Outreach and K-12 Edu., IU **Chris Lamb** – Director, New Castle Career Center
11:30 am – 12:00 pm	**NSA** - Addressing the Cybersecurity Skills Gap with a "New Collar"
11:30 am - 12:00 pm	**Community College Panel** – Who are our Students: Pathways to Cyber *Panelists:* **Danette Coughlan** - Lead Chair; School of IT **Pam Schmelz** - State-wide Chair; Cybersecurity/Information Assurance **Valerie Golay** - Department Chair; Network Infrastructure
12:00 pm - 12:30 pm	Lunch and Networking
12:30 pm - 1:00 pm	**DOE** – Topic and Personnel TBA
1:00 pm - 1:30 pm	**HS Panel** – Best Practices in Scaling an Indiana Cyber Pathway (Established Prog) *Panelists*: **Dr. Travis Huesto -** Computer Science teacher, Marion Regional Career Center **Vickie Houlihan** - Information Tech. Pathway Teacher, Heartland Career Center **Amy Doyle** - NetworkingTteacher, New Albany-Floyd County Con. School Corp.
1:30 pm - 2:00 pm	**NIST** - Career Opportunities in Today's Cyber Workplace (Dr. Pruitt-Mentle)
2:00 pm - 2:30 pm	**Employers Panel** – High Paid, High Demand Jobs of Tomorrow *Panelists*: **Bill Russell** - CISO, Cummins Inc. **Walter Grudzinski** - Director, Information Security and Bus Continuity, Vectren **Owen LaChat** - VP of Technology Infrastructure and Security, Mutual Bank



Two-year Associates Degree One-year Certificate Four-year Degree Credential Technical Certificate License Apprenticeship Work

Prepared for College and Career

Grade 11-12

Pathway Concentration
Dual credit courses, skill-building courses, career and college preparation

Pathway Core
Fundamental knowledge and skills within a Career Pathway
Dual credit courses and skills-building courses

Grades 9 - 10

Introductory Courses
Elements of multiple Career Pathways in multiple courses

Career Foundations Course
OLC/CPSS with financial literacy, computer apps, basic foundational skills

Career Exploration Course
Exposure to 16 career clusters, career interest inventories, exploration

Concentration

Core Courses

Foundation Courses

Exploration Courses

10

KEY STATE LEVEL CTE STAKEHOLDERS

- **Mike Ripperger** - CTE Program Director, Marion Regional Career Center
- **Amanda Wilkerson** - CTE Program Director, Central Nine Career Center
- **Pam Schmelz** - Ivy Tech Community College, Statewide Chair Cybersecurity/Information Assurance
- **Tony Brooks** - CTE Program Director, South Bend CSC
- **Amanda McCammon** – Indiana Department of Education
- **James Little** - CTE Program Director, Century Career Center
- **Gene Hack** - CTE Program Director, C4 Columbus Area Career Center
- **Michele Roberts** - Director of Computing Outreach Education, School of Informatics, Computing & Engineering, Indiana University Bloomington
- **Margaret Semmer** - Vice Chancellor for Academic Affairs, Ivy Tech Community College, Lake County Campus

STATE DIRECTOR

Stefany Deckard, State Director of Career and Technical Education

Indiana Department of Education
151 West Ohio Street
Indianapolis, IN 46204
stdeckard1@doe.in.gov

CYBERSECURITY DEGREES IN INDIANA

ASSOCIATE DEGREES IN CYBERSECURITY

- Ivy Tech Community College, a National Center of Academic Excellence in Cyber Security (CAE)

BACHELOR'S DEGREES IN CYBERSECURITY

- Purdue University-Northwest and Indiana University Bloomington, both CAEs

MASTER'S DEGREES IN CYBERSECURITY

Four universities in Indiana, all of which are CAEs.

- Indiana University Bloomington
- Indiana University – Purdue University Indianapolis
- Indiana University Northwest
- Indiana University South Bend

Certificates and Doctoral Degrees in cyber security are offered by two institutions in the state, both CAEs. Indiana University Bloomington confers Ph.D.'s in Computer Science with a Minor in Security Informatics as well as Informatics with a Security Informatics Track. Purdue University has a Ph.D. program in Computer Science with an Info-Security Focus.

CYBERSECURITY INVESTMENTS IN K-12

The state of Indiana has a very centralized system for career cluster and pathways. One of the major CTE cybersecurity state initiatives is a partnership with the Indiana Office of Technology and the Indiana Information Sharing and Analysis Center, the Indiana Department of Education (IDOE). The new initiative involves providing cybersecurity investments in K-12 schools across the state. "Cybersecurity is a mission critical component in today's technology-centered work and learning environments. It has become an industry with many demands and career opportunities. The Indiana Department of Education, along with our partners, recognize the importance of cyber education and is taking bold steps to prepare Hoosiers," said Dr. Jennifer McCormick, State Superintendent of Public Instruction.

New cybersecurity investments will involve a slate of programming aimed at improving cybersecurity in Indiana schools. Programming includes: a state provided platform for training and awareness on cybersecurity topics for all K-12 school personnel; funding for schools interested in offering a cybersecurity high school course starting in the 2018-2019 and 2019-2020 school years; the creation of a Cybersecurity Task Force coordinated through the Indiana Chief Technology Officer Council; and matching grants of up to $25,000 for schools to improve their cybersecurity posture. The cybersecurity initiative is funded through the U.S. Department of Homeland Security.

"Cybersecurity continues to be a key area of concern for organizations, as well as a growing field for technology professionals," said Dewand Neely, Chief Technology Officer for the Indiana Office of Technology. "The programs and resources dedicated by the Indiana Department of Education show both an investment in the State's youth and the ability to generate a new pipeline of talent for a growing job sector." (https://www.doe.in.gov/news/indiana-department-education-announces-new-initiative-provide-cybersecurity-investments-k-12)

NEW DUAL CREDIT CYBERSECURITY COURSES

Indiana University's dual credit program, ACP, announced the addition of a two IU dual credit computer science courses:

Course Code	Course Title (Credit Hours)	IDOE Course Crosswalk
Computer Science C102	Great Ideas in Computing (3)	4801
Informatics I230	Analytical Foundations of Security (3)	5253

Great Ideas in Computing is a very popular IU course designed for students new to Computer Science. The course covers the "Big Ideas" of computer science and the role of computing in the modern world and includes both lecture and lab work. Labs are deliberately constructed to engage students in key concepts, as well as provide exposure to the breadth of job opportunities in Computer Science. Analytical Foundations of Security (I230) is IU's foundational course in Cybersecurity. The course is modular, covering content and hands-on labs developed to introduce students to the increasingly important field of cyber science. Topics include threat analysis and assurance, cryptography, operating system security, attacks and malware, network and web security, and much more.

PROJECT LEAD THE WAY CYBERSECURITY PROGRAM

The Indiana Department of Education (IDOE) announced, in January 2019, the 50 recipients of the Project Lead the Way (PLTW) Cybersecurity Course Grant. The award will be used towards implementation of the PLTW Cybersecurity course in schools and to continue statewide cybersecurity efforts. As part of IDOE's STEM initiatives, the PLTW Cybersecurity Course Grant awarded 50 schools up to $8,000 per school to assist in offsetting costs associated with implementation of the PLTW Cybersecurity course during the 2019-2020 and 2020-2021 school years. Awards may be used to cover PLTW Computer

Science program participation fees, PLTW Cybersecurity professional development expenses, Cybersecurity Network Security Lab fees, and required course equipment and supplies. In addition to offering this grant opportunity, the IDOE has successfully partnered with over 43,000 school personnel on a district-level cybersecurity training platform. IDOE has also mandated the completion of cybersecurity awareness training for all employees. Proudly, IDOE is active on several statewide computer science related panels and the Governor's Cybersecurity Taskforce.

PROGRAMS OF STUDY/CAREER PATHWAYS

The state of Indiana has also approved a new course that provides students with a capstone course in cybersecurity, Networking II: Cybersecurity Capstone. This course is part of the Indiana Career and Technical Education Pathways. Careers in this cluster focus on design, development, support and management of hardware, software, multimedia, and systems integration services. The course framework for all courses in this content area include a course description, course specifications, and the state standards for that course. All course frameworks are indexed by subject/content area on the Indiana Academic Standards web page.

- Cluster: Info Technology
- Pathway: Networking
- Max Course Credits: 6
- CTE Course Funding Level: $
- Dual Credit Available: No
- 2018-2019 List of Industry Recognized Certifications

STATE RECOGNIZED INDUSTRY CERTIFICATIONS

The state of Indiana has also standardized industry certification associated with CTE concentrations, which are defined as course sequences in which a student must earn a C average in at least two non-duplicative advanced courses within a particular program or program of study. Though current high school students are grandfathered under the previous CTE Concentrator definition – earning at least six high school credits in a career sequence – schools may opt to use this new definition of two courses for their current students.

HIGH SCHOOL STUDENT CYBERSECURITY COMPETITIONS

- National Cyber League
- CyberPatriot
- Collegiate Cyber Defense Competition (CCDC) State of Indiana and Midwest Region
- US Cyber Defense Challenge (CyberQuest)
- Cyber ACES Camp Midwest
- Mitre Cyber Academy

CYBERSECURITY SPRING TRAINING CAMP

Regional Opportunity Initiatives, Inc. (ROI) is to support economic and community prosperity in the 11 counties of Southwest Central Indiana (now called the Indiana Uplands). This year ROI kicked-off their first Cybersecurity Spring Training Camp, ROI's 11 county region has an enormous cross-sector need for cybersecurity and cyberinfrastructure professionals. ROI has partnered with Indiana University's School of Informatics, Computing, and Engineering (SICE) and Carnegie Mellon University to help train educators and their student teams and to introduce them to the challenges seen in the PICO Capture the Flag (picoCTF) competition.

GENCYBER CAMPS

The state of Indiana has hosted several GenCyber Camps over the last few years. The list below represents the host of these camps.

- Purdue University
- Purdue Northwest University
- Ivy Tech (4 Campuses)

CAE CENTERS

The state of Indiana has four formally recognized CAEs at the time of this study.

- Indiana University
- Ivy Tech Community College
- Purdue University
- Purdue University Northwest

STUDENT CYBERSECURITY COMPETITIONS

The state promotes student competitions and has one of the large numbers of school participating in the CyberPatriot program.

School	No. of Teams	Division	Location
Anderson Composite Squadron	2 Teams	All Service, Middle School	Anderson
University High School of Indiana	1 Team	Open	Carmel
Garrett High School	2 Teams	Open	Garrett
Garrett Middle School	1 Team	Middle School	Garrett
CAP GLR-IN-802 Titan Cadet Squadron	3 Teams	All Service	Indianapolis
South Newton High School	1 Team	Open	Kentland
MICHIGAN CITY HIGH SCHOOL	1 Team	All Service	Michigan City
Twin Lakes High School	3 Teams	Open	Monticello
Twin Lakes High School	1 Team	Open	Monticello
Twin Lakes High School	1 Team	Open	Monticello
Terre Haute North Vigo High School/AFJROTC	4 Teams	All Service	Terre Haute

STATE APPROVED CYBERSECURITY CAREER PATHWAYS PROGRAM

APPROVED COLLEGE DEGREE AND CERTIFICATION PROGRAMS

SCHOOL NAME	PROGRAMS	NSA
Indiana University Bloomington	Bachelor of Science in Computer Science – Security Specialization	NSA CAE
Indiana University-Purdue University-Indianapolis	Bachelor of Science in Informatics – Security Informatics Specialization	
Indiana Wesleyan University	Graduate Certificate in Cybersecurity	
Ivy Tech Community College	M.S. in Secure Computing	NSA CAE
Purdue University-Northwest	Master of Science in Cybersecurity Risk Management	NSA CAE
Purdue University	Master of Science in Information Systems – Enterprise Risk Management	NSA CAE
Taylor University	Minor in Security Informatics	
Valparaiso University	Ph.D. in Computer Science – Minor in Security Informatics	

OVERALL SUMMARY OF INDIANA CYBERSECURITY PATHWAYS

STATEWIDE CHALLENGES TO MAINTAINING CYBERSECURITY CAREER PATHWAY PROGRAMS

Like many other systems across the nation, the real obstacles and challenges faced by the state cybersecurity career pathways initiatives are listed below:

FACULTY

- Recruiting new faculty
- Salary discrepancy with business and industry
- Faculty and staff training and development
- Retention and retirements

FACILITIES

- Security concerns in the classroom
- Cost of software and equipment
- Virtual and cloud based instructional content
- Required updating of curriculum and faculty development

OUTREACH

- More women and minorities
- Better outreach to middle and high schools
- Outreach in rural areas

BUSINESS AND INDUSTRY

- Greater participation in internships
- Adjunct faculty

STATEWIDE FINDINGS AND RECOMMENDATIONS

- The state of Indiana, having a single community college system, has a very centralized department of education system in which institutions share common curriculum on a statewide basis.
- The state has a very formalized process for periodic examination and updating of the career clusters framework, including cybersecurity programs.
- Cybersecurity pathway programs in Indiana are primarily found in the information technology-related programs and computer science. Indiana also has cybersecurity certificates and majors available in their business and engineering schools.
- The state of Indiana has the TransferIN program which is a statewide transfer and articulation program. The program is primarily focused on AS and AA degrees. The agreement does account for limited transfer of AAS courses. A state committee is responsible for reviewing these agreements on an annual basis.
- The state of Indiana promotes dual enrollment. Cybersecurity is taught as part of each of these statewide programs.
- Several of the major state universities, including Indiana University, Purdue, Indiana Institute of Technology, and Indiana Tech, offer cybersecurity programs. Indiana has strong cybersecurity programs in several of the private and religious-affiliated institutions. Cybersecurity programs range from high school courses through PhD programs.
- Purdue University Online recently applied for CAE status. This institution will be providing cybersecurity training online in a world-wide platform.
- The state of Indiana has a new statewide initiative providing cybersecurity investment in K-12 schools across the state. This involves matching grants of up to $25,000 per school to improve their cybersecurity posture.

MICHIGAN

MICHIGAN CTE AND CAREER PATHWAYS SYSTEM

The state of Michigan has:

State of Michigan CTE And Career Pathways Systems	
764	Public High Schools
4	Public High Schools Offering Solely/Primarily CTE Courses
425,738	Public High School Enrollment
109,005	High School CTE Enrollment
77,381	High School CTE Concentrators
31	Public Community Colleges
271,086	Public Community Colleges Enrollment (full & part-time)
107,012	Postsecondary CTE Enrollment
76,284	Postsecondary CTE Concentrators

MICHIGAN CTE STRUCTURE

In the state of Michigan, CTE and career pathways are offered through the following institutions:

- Comprehensive high schools
- Area CTE centers
- Charter schools
- Community colleges
- Four-year universities
- Tribal colleges

MICHIGAN PROGRAMS OF STUDY/CAREER CLUSTERS

Michigan uses programs of study to link secondary and postsecondary CTE programs. In particular, secondary and postsecondary agencies review standards that are submitted as part of the Rigorous Programs of Study (RPOS) approval process. At the secondary level, this requires addressing the state's secondary CTE standards; at the postsecondary level, this requires addressing locally selected postsecondary CTE standards.

Michigan has implemented programs of study in all 16 of the Career Cluster areas. Michigan maintains Rigorous Programs of Study in the following Career Clusters:

1. Business Management & Administration Career Clusters	2. Education & Training Career Clusters
3. Health Science Career Clusters	4. Human Services Career Clusters
5. Law, Public Safety, Corrections & Security Career Clusters	6. Manufacturing Career Clusters

CTE DUAL CREDIT PROGRAMS IN MICHIGAN

Michigan has three dual credit programs:

- ***Postsecondary Enrollment Options*** allows students to enroll in postsecondary courses for high school and/or postsecondary credit.
- ***Career and Technical Preparation Act (2000)*** a student may enroll in a CTE course at an eligible postsecondary institution. Concurrent enrollment courses are taught at the high school, either by a high school instructor approved by the partnering postsecondary institution, or by a postsecondary faculty member.
- ***Fifth-year High School*** pupils in attendance at a school district, intermediate school district or public school academy may enroll in postsecondary or CTE preparation dual enrollment courses if the pupil has not met all high school diploma requirements, and is enrolled in not more than two postsecondary dual enrollment courses taken at any given time and not more than four postsecondary enrollment courses taken during the school year. The pupil must have a plan on file at the district to complete district graduation requirements within the academic year, including postsecondary dual enrollment options.

DUAL ENROLLMENT PROGRAMS IN MICHIGAN

- ***Postsecondary Enrollment Options Act or Career and Technical Preparation Act:*** At the time a public-school student enrolls in a postsecondary course, he/she must designate whether the course is for high school or postsecondary credit, or both. A non-public school student may enroll only for postsecondary credit and may not receive high school credit for the course. Exceptions provided for a course that would be determined "a nonessential elective course" under specified circumstances.
- ***All Programs:*** For a district to be eligible for supplemental payments under the Postsecondary Enrollment Options Act or Career and Technical Preparation Act, the district must award high school credit for the postsecondary course if the student successfully completes the course. For a district to be eligible for payments for students enrolled in a concurrent enrollment program, a district must ensure the student is awarded both high school and college credit at any community college or state public institution in the state upon successful completion of the course.

MICHIGAN CTE/CAREER PATHWAYS MEETING LOGISTICS

The MVCC team coordinated the event with Lonnie Decker, Networking Department Chair at Davenport University in Grand Rapids, Michigan, on December 14, 2018.

Advance CTE – Michigan: www.careertech.org/michigan

Cybersecurity Career Pathway: www.cyberseek.org/pathway.html

Michigan Initiative for Cybersecurity Education: www.miceK-12.com

Meeting audio recording (morning): bit.ly/2wCTdD9

(afternoon): bit.ly/2K6mNtJ

MICHIGAN CTE/CAREER PATHWAYS MEETING LOCATION & AGENDA

The Administration, staff and faculty at Davenport University, would like to invite you to be participate in a discussion in regarding the career pathway for cybersecurity in the state of Michigan. We will discuss ways to strengthen the opportunities for students to engage in this work by designing scalable pathways, and learning the skills needed to access these "new collar" jobs.

LOCATION

December 14, 2018
Davenport University
6191 Kraft Ave SE, Grand Rapids, MI 49512

AGENDA

10:00 am - 10:30 am	**Registration**
10:30 am - 10:40 am	**Welcome** - **Dr. Pamela Imperato**, Dean, Davenport University
10:40 am - 10:50 am	**CSSIA** - Leading the Way - **Dr. John Sands,** Moraine Valley Communiity College
10:50 am – 11:00 am	**Cybersecurity Pathways** - **Clydene Stangvik,** Cisco
11:00 am - 11:30 pm	**CTE Panel** - Where is Cyber: Current CTE Clusters and Consequent Pathways *Panelists*: **Patrick Schulz** - BAISD, MICE **Paul Fedele** - Calhoun Area Career Center **Thomas Knight** - Michigan Department of Education, OCTE **Amanda Stoel** - Michigan Department of Education
11:30 am – 12:00 pm	**NSA** – Government's role in supporting cybersecurity K-12 - **Kevin Nolten,** NICERC
11:30 pm - 12:00 pm	**College Panel** – Who are our Students: Pathways to Cyber *Panelist:* **Lonnie Decker** - Davenport University **Andrew Rozema** - Grand Rapids CC **Cyndi Millns** - Washtenaw CC, Pinckney Cyber Training Institute
12:00 pm - 12:30 pm	Lunch and Networking
12:30 pm - 1:00 pm	**DOE** – Topic and Personnel TBA
1:00 pm - 1:30 pm	**HS & Middle College Panel** – Best Practices in Building Cybersecurity Pathways *Panelist*: **Marcee Theisen** - Eaton RESA **Tamara Shoemaker** - UDM, Midwest CISSE **Michelle Ribant** - Michigan Department of Education **Cyndi Millns** - Washtenaw CC, Pinckney Cyber Training Institute
1:30 pm - 2:00 pm	**NIST** - Career Opportunities in Today's Cyber Workplace - **Davina Pruitt-Mentle,** NIST
2:00 pm - 2:30 pm	**Employers Panel** – High Paid, High Demand Jobs of Tomorrow *Panelist*: **Aphrodite Jones** - Spectrum Health, MiHCC **John Weller** - MetroHealth, MiHCC **Nicole Scheffler** - Cisco **Ed Koledo** - Talent & Economic Development, Department of Michigan

KEY STATE LEVEL CTE STAKEHOLDERS

- **Paul Fedele** - Calhoun Area Career Center
- **Thomas Knight** - Michigan Department of Education, Office of CTE
- **Cyndi Millns** - Washtenaw Community College, Pinkney Cyber Training Institute
- **Michelle Ribant** - Michigan Department of Education
- **Patrick Schulz** - Bay-Arenac Integrated School District (BAISD), MICE
- **Amanda Stoel** - Michigan Department of Education
- **Marcee Theisen** - Eaton Regional Education Service Agency (RESA)

STATE DIRECTOR

Brian Pyles, State CTE Director

Office of Career and Technical Education
Michigan Department of Education
608 West Allegan Street
Lansing, MI 48909
pylesb@michigan.gov

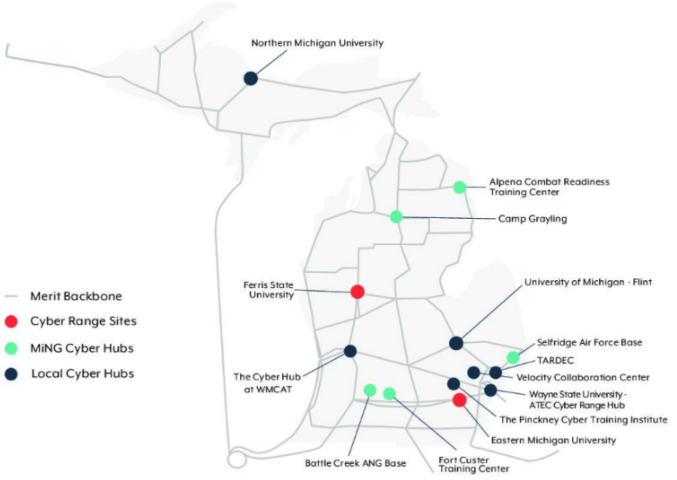
STATE CYBERSECURITY ACCOMPLISHMENTS

MICHIGAN NSA CAE DESIGNATED INSTITUTIONS

- Davenport University
- Eastern Michigan University
- Ferris State University
- Grand Rapids Community College
- Henry Ford College
- Oakland University
- University of Detroit Mercy
- Walsh College

MICHIGAN CYBER RANGE

Michigan Cyber Range was established by Merit Network in the summer of 2012 to teach cybersecurity certification courses and to provide cybersecurity related services. Merit Network staffs and operates the Michigan Cyber Range in Ann Arbor, Michigan. The Michigan Cyber Range aims to strengthen Michigan's cyber defenses by mitigating the growing number of cyber threats and providing a more secure environment that promotes economic development. This can be accomplished by nurturing a cybersecurity industry that leverages Michigan's unique advantages, which include educational institutions, a large IT workforce, the manufacturing base and federal cooperation with the security industry.


Northern Michigan University
Alpena Combat Readiness Training Center
Camp Grayling
Ferris State University
University of Michigan - Flint
Merit Backbone
Cyber Range Sites
MiNG Cyber Hubs
Local Cyber Hubs
Selfridge Air Force Base
TARDEC
Velocity Collaboration Center
The Cyber Hub at WMCAT
Wayne State University - ATEC Cyber Range Hub
The Pinckney Cyber Training Institute
Eastern Michigan University
Battle Creek ANG Base
Fort Custer Training Center

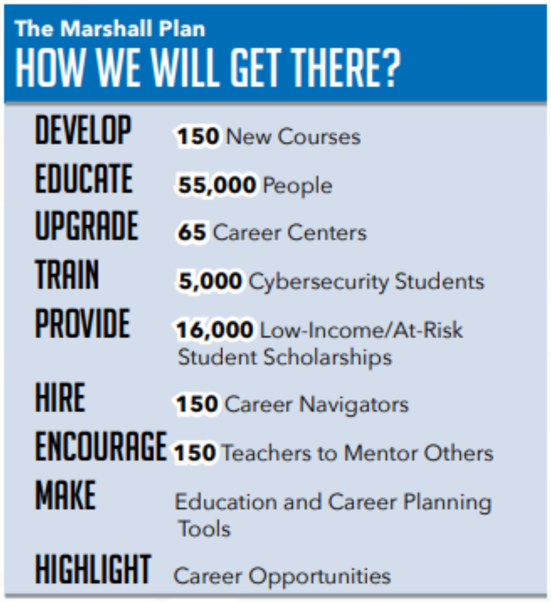
TEACH: Provide access to lab-based experiential learning and certification for all compliance requirements and frameworks, including the NIST 800 Standards, NICE Framework, NSA, DoD 8570, HiTrust, FFIEC, PCI, CJIS and CSA.

TEST: Engage, support and attract surrounding industries and entrepreneurs to provide cost effective and scalable access to software, systems and penetration testing.

TRAIN: Host live security attack and defense exercises to benchmark skills across the spectrum, from K-20 to public, private, defense and military sectors. Custom training programs can be tailored to each customer's needs.

STRATEGIC PARTNERSHIPS MICHIGAN'S MARSHALL PLAN

The Michigan Career Pathways Alliance was launched, proposing actions and recommendations to assure every student has the opportunity to explore multiple pathways to find a career matching their interests and goals. This year, this initiative, along with several other efforts to promote and support a talented workforce in Michigan, expanded into the Marshall Plan for Talent, continuing the cross-agency collaboration with the Michigan Department of Talent and Economic Development (TED) and the governor's office. In June 2018, Governor Rick Snyder signed into law a multi-bill package that supports these efforts and allocates $100 million to revolutionize Michigan's talent and education system and prepare students for the 21st century economy.



The Marshall Plan

HOW WE WILL GET THERE?

DEVELOP	**150** New Courses
EDUCATE	**55,000** People
UPGRADE	**65** Career Centers
TRAIN	**5,000** Cybersecurity Students
PROVIDE	**16,000** Low-Income/At-Risk Student Scholarships
HIRE	**150** Career Navigators
ENCOURAGE	**150** Teachers to Mentor Others
MAKE	Education and Career Planning Tools
HIGHLIGHT	Career Opportunities

MICHIGAN INITIATIVE FOR CYBERSECURITY EDUCATION (MICE)

MICE was founded in 2017, but the dream of building the initiative has been in the works for over five years as a collaboration of educators with over 75 years of combined experience. Over the past two years, MICE has trained over 75 teachers through quarterly train-the-trainer sessions. MICE has presented at multiple education conferences, the Michigan State Board of Education, and to the Michigan Governor. We have been actively involved in the development of Cybersecurity and Computer Science standards adoption in Michigan and partner with Cisco, Microsoft, and Amazon to support multiple nationwide education initiatives. Starting with a vision to build something awesomely effective targeting the current lack of training in Cybersecurity and Computer Science and technology talent gap, MICE was designed by a collaboration of K-12 and post-secondary educators to build a true K-12 pipeline that connects to both post-secondary institutions and business industry simultaneously.

Combined with multiple years of classroom teaching experience, MICE is highly involved in curriculum development at the state and national level, teacher training, and work-based learning opportunities both virtually and on-site.

(https://www.micek12.com/about/)

GOVERNOR'S SCHOOL CURRICULUM FOCUS

Governor Rick Snyder joined industry leaders at the 2018 SAE CyberAuto Challenge™ to announce a new high school curriculum focused on automotive cybersecurity training and filling the existing skills gap in the career field of automotive cybersecurity. Masters of Mobility: Cyber Security on the Road will provide in-depth training for Michigan high school teachers as well as resources and materials that will teach students to program, hack and learn to defend against cyberattacks. “Offering our high school students hands-on experience in dynamic fields like automotive cybersecurity will be critical to filling the growing demand for talent in key professional trades,” Gov. Snyder said. “This is the type of innovative approach to career training that is at the core of the Marshall Plan for Talent.”

The program coursework was developed by the Square One Education Network and includes ethical considerations, fundamental training in Unix/Linux (the language used to program small computers on cars), CANBUS protocols (how small computers communicate amongst themselves), engine fundamentals, cryptology and more. It also builds on SAE’s 6-8 grade A World in Motion (AWIM) programming. Combined, the programs will help move students through an integrated STEM experience focused on developing Michigan’s automotive cyber-workforce.

The pilot Masters of Mobility program will launch in two schools over the course of 12 weeks in the fall of 2018, with a roll-out to eight additional schools planned for 2019. Schools being considered to launch the program are Oak Park High School, Clinton High School, Wilson Talent Center (Mason) and Hale Area Schools.

PINCKNEY COMMUNITY SCHOOLS

Pinckney Community Schools in Pinckney, MI are the first district in the nation to create a cyber defense education program. (https://www.livingstondaily.com/story/news/education/pinckney/2016/12/12/pinckney-schools-first-nation-offer-cyber-security-education-program/95194194/)

The Pinckney Cyber Training Institute and Sentinel Center will provide educational and certification opportunities for high school and college students, as well as tech professionals. “The development of the Pinckney Cyber Training Institute is just one way we’re dedicating resources to educating people in cyber defense and subsequently protecting our citizens, infrastructure and economy,” said Steve Arwood, CEO of the MEDC. “From smart phones to connected and automated vehicles, our world is relying more and more on advanced technologies and these initiatives are developing the talent and skills needed to prevent cyber-attacks.”

The institute will serve as a hub for the Michigan Cyber Range, which has centers across the state. Created and managed by the nonprofit, member-owned Merit Network, the Michigan Cyber Range hones security software and the cyber defense skills of professionals through classes and exercises. It also enables product development and testing for clients and has working relationships with multiple entities, including the MEDC and the Michigan National Guard.

Students and professionals who enroll in the institute will be able to take cybersecurity courses, earn state-approved certifications and engage in cybersecurity training exercises. While each Michigan Cyber Range hub offers 22 professional certifications, the institute is the first hub to be located at a high school, allow students to earn college credits and provide access to early internship opportunities.

CYBERSECURITY EDUCATION PROGRAMS

HIGH SCHOOL STUDENTS EDUCATION

- Pinckney Cyber Training Institute
- Utica Community Schools Cybersecurity Course

ASSOCIATE DEGREES AND CERTIFICATIONS

- Macomb Community College - IT - Network Security Professional (Cybersecurity)
- Grand Rapids Community College - Information Security
- Henry Ford College - Computer Information Systems - Cybersecurity
- Jackson College - Cybersecurity
- Monroe County Community College - CIS: Cybersecurity and Information Assurance
- Oakland Community College - Cybersecurity Certificate
- Wayne County Community College District – Cybersecurity

STATE APPROVED CYBERSECURITY CAREER PATHWAYS PROGRAMS

APPROVED COLLEGE DEGREE AND CERTIFICATE PROGRAMS

SCHOOL NAME	PROGRAMS	NSA
Baker College	Bachelor of Science in Information Technology and Security – Concentration in Information Assurance	
Central Michigan University	Bachelor of Science in Information Technology and Security – Concentration in Information Assurance and Cyber Security	
Davenport University	Bachelor of Science in Information Technology and Security – Concentration in Network Professional	NSA CAE
Eastern Michigan University	Bachelor of Science in Information Technology and Security – Concentration in Server Administration	NSA CAE
Ferris State University	Graduate Certificate in Cybersecurity	NSA CAE
Grand Rapids Community College	Undergraduate Certificate in Cybersecurity	NSA CAE
Henry Ford Community College	BS in Cyber Defense	NSA CAE
Jackson Community College	Digital Forensics, BS	
Macomb Community College	Master of Science in Information Assurance and Cyber Security	
Michigan Technological University	Network Security, BS	
Monroe County Community College	Bachelor of Science in Information Assurance & Cyber Defense	
Northern Michigan University	Associate in Applied Science in Information Security and Intelligence	
Oakland Community College	Bachelor of Science in Information Security and Intelligence	
Oakland University	Certificate in Cybersecurity	
Saginaw Valley State University	Certificate in Cybersecurity: Ethical Hacking	
University of Detroit Mercy	Information Security and Intelligence – 5 Year BS and MS	NSA CAE
University of Michigan-Dearborn	Master of Science in Information Security and Intelligence	
Walsh College	Minor in Digital Forensic/Cybersecurity	NSA CAE
Wayne County Community College District	Minor in Information Security and Intelligence	

MICHIGAN DEPARTMENT OF EDUCATION - CYBERSECURITY COMPETITION EVENT GRANTS

The fiscal year (FY) 2017 State School Aid Act, Section 99k appropriated $500,000 for the 2017-18 school year for competitive grants to districts that provide pupils in grades 6 to 12 with expanded opportunities to improve computer science skills by participating in cybersecurity competitive events hosted by Merit Network. The following schools received awards:

- Airport Community Schools
- Cadillac Area Public Schools
- Gull Lake Community Schools
- Hillsdale Integrated School District
- Ingham Integrated School District
- Les Cheneaux Community Schools
- Southgate Community School District
- Westwood Community School District

OVERALL SUMMARY OF MICHIGAN CYBERSECURITY PATHWAYS

STATEWIDE CHALLENGES TO MAINTAINING CYBERSECURITY CAREER PATHWAY PROGRAMS

STATE BUDGET

- A decrease in funding for CTE programs
- A decrease in the number of students participating in CTE programs

FACULTY

- Recruiting cybersecurity faculty
- Retention
- Retirement
- Salary discrepancy with business and industry

FACILITIES

- Budgets to update new technologies
- Virtual and cloud-based instructional content
- Keeping up with the new threats and technologies
- Ability to teach tools and products in the classroom

OUTREACH

- More women and minorities students and faculty
- Greater middle and high schools' awareness

BUSINESS AND INDUSTRY

- More internships
- Apprenticeships

STATEWIDE FINDINGS AND RECOMMENDATIONS

- The state of Michigan has a decentralized department of education system in which schools have increased latitude and authority to develop business-friendly programs that meet local workforce needs.
- The state has a very formalized process for periodic examination and updating of the career clusters framework, including cybersecurity programs. The post-secondary agencies review programs that are submitted using a rigorous program of study approval process in which local programs meet state secondary CTE standards and local workforce needs.
- Cybersecurity pathway programs in Michigan are primarily found in the information technology-related programs and computer science. Michigan also has cybersecurity certificates and majors available in their business and engineering schools.
- The state of Michigan has a statewide articulation and transfer agreement referred to as Michigan Department of Education Office of Career and Technical Education (MDE-OCTE). This program provides students the opportunity to test out of courses. The agreement also enables institutions to grant articulated credit hours for students completing one year of a CTE program.
- The state of Michigan promotes dual-enrollment. Cybersecurity is taught as part of each of these statewide programs.
- Several of the major state universities offer cybersecurity programs. Michigan has strong cybersecurity programs in several of the private and religious-affiliated institutions. Cybersecurity programs range from high school courses through Master's programs.
- Michigan has been operating a statewide cyber range under the MERIT Program, the nation's longest-running research and education network, the Michigan Cyber Range is the nation's largest unclassified, network accessible cybersecurity training platform.

NEW YORK

NEW YORK CTE AND CAREER PATHWAYS SYSTEM

The state of New York has:

State of New York CTE and Career Pathways Systems	
1,190	Public High Schools
21	Public High Schools Offering Solely/Primarily CTE Courses
762,914	Public High School Enrollment
190,988	High School CTE Enrollment
102,873	High School CTE Concentrators
43	Public Community Colleges
462,720	Public Community Colleges Enrollment (full & part-time)
182,472	Postsecondary CTE Enrollment
153,324	Postsecondary CTE Concentrators

NEW YORK CTE STRUCTURE

The state of New York CTE and career pathways are offered through the following institutions:

- Comprehensive high schools
- Technical high schools
- Career Academies
- Community colleges
- Four-year universities

NEW YORK CAREER CLUSTERS

New York's Learning Standards for CTE are identified in the Career Development and Occupational Studies document. The Career Development and Occupation Studies standards include both cross-cutting standards for all CTE students, as well as standards organized into six career majors based on state workforce requirements. New York's CTE career majors are the following:

1. Arts/Humanities
2. Business/Information Systems
3. Engineering/Technologies
4. Health Services
5. Human and Public Services
6. Natural and Agricultural Sciences

NEW YORK PROGRAMS OF STUDY

New York maintains programs of study in each of the 16 Career Cluster areas.

1. Agriculture, Food & Natural Resources Career Cluster	9. Architecture & Construction Career Cluster
2. Arts, A/V Technology & Communications Career Cluster	10. Business, Management & Administration Career Cluster
3. Education & Training Career Cluster	11. Finance Career Cluster
4. Government & Public Administration Career Cluster	12. Health Science Career Cluster
5. Hospitality & Tourism Career Cluster	13. Human Services Career Cluster
6. Information Technology Career Cluster	14. Law, Public Safety, Corrections & Security Career Cluster
7. Manufacturing Career Cluster	15. Marketing Career Cluster
8. Science, Technology, Engineering & Mathematics Career Cluster	16. Transportation, Distribution & Logistics Career Cluster

PERKINS ELIGIBLE AGENCY

New York State Education Department

NEW YORK CTE/CAREER PATHWAYS MEETING LOGISTICS

The MVCC team coordinated this event with Jake Mihevc of Mohawk Valley Community College at their Rome, NY campus 1101 Floyd Avenue.

Meeting audio recording: bit.ly/2QOFnHb

New York Career and Technical Education: www.p12.nysed.gov/cte

New York State Pathways to Certification: www.highered.nysed.gov/tcert/certificate/pathways.html

NEW YORK CTE/CAREER PATHWAYS MEETING LOCATION & AGENDA

LOCATION

March 22, 2019
Mohawk Valley Community College
Rome Campus – Room 150
1101 Floyd Ave, Rome, NY 13440

AGENDA

9:30am - 10:00am	**Registration** & Light Breakfast
10:00am - 10:10am	**Welcome** Jake Mihevc, Mohawk Valley Community College, Associate Dean, CNY Hackathon Co-Founder
10:10am - 10:20am	**CSSIA** - Leading the Way - Dr. John Sands, Director and PI
10:20am - 10:50am	**DOE** - Albert Palacios, Education Policy Analyst, US Department of Education
10:50am - 11:20am	**NIST** - Cybersecurity Career Pathways Resources - Dr. Davina Pruitt-Mentle, NIST
11:20am - 11:30am	Break
11:30am - 12:00pm	**Panel:** Cybersecurity CTE Pathways in New York State *Panelists:* **Robert Leslie** - CTE Director, Syracuse City School District **Tim Ott** - CEO, SPN, and Director, CTE TAC of New York
12:20pm - 1:00pm	Working Lunch: CNY Hackathon, Reinforcing Cybersecurity Pathways
1:00pm - 1:45pm	• Central New York Cybersecurity Employment Landscape • Griffiss Institute • Assured Information Security
1:45pm - 2:30pm	**Panel -** Educators- CTE Pathways and Academics • Regional Cybersecurity CTE Instructors • Cybersecurity Faculty-Higher Education
2:30 pm	Wrap Up

KEY STATE LEVEL CTE STAKEHOLDERS

- **Timothy S. Kroecker**, PhD, Senior Operations Research Analyst/Enterprise Learning Officer, Information Directorate, Air Force Research Laboratory, RI
- **Tim Ott**, CEO, Successful Practices Network and Director, CTE Technical Assistance Center of NY
- **Robert Leslie**, CTE Director, Syracuse City School District

STATE DIRECTOR

Deborah Reiter, State Director

New York State Education Department
860 Education Building Annex
89 Washington Avenue, Room 315 EB
Albany, NY 12234
deborah.reiter@nysed.gov

NYS TECHNOLOGY EDUCATION FRAMEWORK INITIATIVE

MISSION AND GOAL

To evolve to a technologically literate society, educational entities in NYS require a framework for developing a continuum of instruction in technology education for the future.

BACKGROUND

Technology education in New York state enjoyed a renaissance in the mid 1980's and 90's that produced a number of innovative courses and programs. These programs were viewed as models of contemporary technology education. But various events over the last 10-15 years have combined to create an environment not friendly to technology education in schools. Since adoption of the NYS Learning Standards in 1996, no State-developed technology-related curriculum development has taken place introducing new technologies or techniques to the classroom. Turnover by school district administrations has created administrators unaware of the potential and value of technology education programs. Recent changes to Commissioner's Regulations and revised graduation requirements have turned the system into a patchwork.

Accountability systems layered on schools have placed increased emphasis and pressure on academic areas with testing requirements. This increased pressure has created an atmosphere putting greater importance on certain Learning Standard areas over others.

Through the foresight of many, the standard for technology and technology education programs was linked to mathematics and science. Illustrating the interconnectedness of these three subjects the Mathematics, Science, Technology (MST) Learning Standards has created a dynamic force for demonstrating student knowledge. While mathematics and science have had a long history in education, technology education is a relatively new subject with less stature and acceptance. Added to this the testing pressures placed on mathematics and science education; technology education has been overlooked as a tool for improving student achievement.

Recent efforts to create awareness about, and value for, technology education have been less then successful partly due to the general population not having a clear understanding of what technology is. With these issues to be addressed by stakeholders in the field, it is imperative that a clear structure exists to build a case for full acceptance of technology education as a vital curriculum component.

RATIONALE FOR DEVELOPING A FRAMEWORK

The notion of a framework is consistent with the structure of the Learning Standards. While the 28 Learning Standards identify what students should know and be able to do at various levels, they do not elaborate on contextualized content for specialized subjects such as technology. Subjects like science use broad terms to organize its dynamic content; Biology, Chemistry, and Physics. The current environment for technology education has evolved into an array of courses with titles that may or may not appear appropriate to school district curriculum decision makers. To be consistent with other subject areas, technology education needs to identify its dynamic content.

Through this effort a better understanding and sense of purpose and place in the overall school curriculum will help to build capacity and consistency across the State. Administrators and teachers will be better positioned to identify their roles and responsibilities in a large or small educational system that allows all parties to have a common vision.

The added benefit of a defined framework for multiple grade-levels improves chances of transferable skill and knowledge retention and continued interest for students wishing to pursue technology-related postsecondary education or career opportunities.

CONTENT, CONTEXT, AND STANDARDS

A tremendous hurdle for school districts and teachers in all subjects and especially teachers responsible for technology education is moving to a standards-based educational system. Technology education has traditionally and logically been content-focused. While content remains the primary factor in what influences technology teachers, other factors in a dynamic system require serious consideration. School and student accountability systems are centered on assessment of their respective Learning Standards as a measure of student performance. A system of accountability will continue for the foreseeable future no matter what political influences may be imposed through educational reform. The reality is that school districts are driven by these accountability measures and are consequently judged by governments, communities and the general public. Untested subject areas must carve a place for themselves within this system to remain viable and relevant in the overall educational system. Not addressing the concerns of the school district and governmental agencies will lead to the demise and eventual extinction of these subjects that support the positive developmental aspects of every student. This change in our thinking must lead us to addressing standards through what is taught.

For many this effort seems impossible. If what we do is content-driven how can we change the focus? Developing a standards-based system does not mean we need to discard everything we are currently doing. But we do need to change the way we think about content. If our goal is achievement of the standards, content needs to be reviewed for its effectiveness at meeting those standards. Old content needs to be viewed with a critical eye as to its ability to address standards in a coherent manner. Achievement of standards through relevant content must take precedent over content that has been aligned with standards after the fact. Deciding on content that addresses specific aspects of a standard requires attention to its place in an overall plan or goal of the program. A framework that identifies broad areas of content within a specific context helps curriculum developers address standards in a uniform way yet provides flexibility for expanding a dynamic subject area like technology.

To redirect the effort towards this goal a model is suggested that incorporates existing content-focused programs but provides a path for future program changes that better addresses the standards-based school curriculum. The use of Technology Content Organizers (TCO) evolved from national efforts to identify the most critical areas of technology essential to the Unites States' economic future in a secure environment.

INFORMATION COMMUNICATION CLUSTER

Broadly defined as: Producing, storing, manipulating and moving information.

Perhaps more than any other technical area, information and communication technologies are what make our society "modern." The ability to rapidly access and share vast amounts of information has been the driving force in economic growth and improved quality of life in the latter part of the twentieth century. Accordingly, information and communication technologies are essential to meeting national goals in economic growth and national security, and in helping other technical areas to realize their full potential. The technologies identified as critical include those contributing to the leading edge of components, communications, computer systems, information management, intelligent complex adaptive systems, sensors and software and toolkits. Of these areas, components, computer systems, communications, information management, and software and toolkits have the highest potential to contribute to economic growth. Computer systems (particularly high-performance systems), intelligent complex adaptive systems and sensors have significant potential to contribute to national security.

With the exception of high-definition displays and high-resolution scanning, the U.S. is ahead, or at least at parity, in almost all the fields comprising the Information and Communication technology category. The U.S. invented and widely deployed such technologies as UNIX, the Ethernet, the Internet, LANs, and most of the field of artificial intelligence; U.S.-developed operating systems for personal computers are the world standard; our digital HDTV plans lead the world. The National Display Initiative will help to fill in the gap in high-definition displays, and in most areas where we have some weakness, U.S. firms are forming alliances with other firms in Japan and Europe, leading to multinational initiatives. (NCT Report 1995)

- Technology Areas
- Components
- Communications
- Computer Systems
- Information Management
- Intelligent Complex Adaptive Systems
- Sensors
- Software and Toolkits

APPROVED NY STATE CTE CYBERSECURITY PROGRAMS

The state of New York has several different K-12 CTE programs recognized by the New York State Department of Education. The following is the current list of recognized programs.

High School	Program Title	CIP CODE
Hamilton-Fulton-Montgomery BOCES	Cybersecurity & Computer Technology	15.1202
Rockland BOCES	Cyber Technology	11.1003
Syracuse City School District	Cybersecurity	11.1003
Tompkins-Seneca-Tioga BOCES	Computer Technology/Cybersecurity	15.1202
Oneida-Herkimer-Madison BOCES	Emerging Technologies and Cyber Security	11.1003
Erie 1 BOCES	Cybersecurity and Networking	11.1003

** BOCES stands for Board of Cooperative Educational Services. BOCES are public organizations that were created by the New York State Legislature in 1948 to provide shared educational programs and services to school districts.*

CTE PROFESSIONAL CYBERSECURITY CERTIFICATE

The state of New York has defined a professional Career and Technical Education Certificate.

Pathway: Certificate Progression

This pathway is for individuals who hold a valid New York State entry-level certificate (such as an Initial or Provisional certificate). They may progress to the advanced-level credential (such as a Professional or Permanent certificate) by meeting the requirements for that certificate.

Requirements:

- Hold/Held an Initial Certificate - Cyber Security 7-12
- Additional Pedagogy - 9 S.H.
    - College Coursework - Instruction and/or Assessment
    - College Coursework - Teaching Literacy Skills Methods - 3 S.H.
    - College Coursework - Classroom Management
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years

- Mentored Experience - Cyber Security 7-12
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: CTE Certificate progression - Initial/Trans A issued prior to May 9, 2017

This pathway is to be used for candidates that had their Initial CTE certificate issued prior to May 9, 2017.

Requirements:

- Hold/Held an Initial Certificate - Cyber Security 7-12
- Additional College Coursework - 30 S.H.
  - College Coursework - Liberal Arts & Sciences
  - College Coursework - Career and Technical Education
  - College Coursework - Teaching Literacy Skills Methods - 3 S.H.
  - College Coursework - Foundations of Education
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Yrs.
- Mentored Experience - Cyber Security 7-12
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: CTE Program Cert progression - Initial/Trans A issued prior to May 9, 2017

This pathway is to be used for candidates that completed an approved Career and Technical teacher preparation program at a New York State College and had their Initial CTE certificate issued prior to May 9, 2017.

Requirements:

- Hold/Held an Initial Certificate - Cyber Security 7-12
- Completion of a NYS Registered Program - Cyber Security 7-12
- Institutional Recommendation - Cyber Security 7-12
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Yrs.
- Mentored Experience
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: Option A - Individual Evaluation

This pathway is for candidates who are seeking a certificate in a career or technical subject and who hold an associate degree from a program that has not been preapproved by the State Education Department for certification. Candidates must submit original credentials for an evaluation to determine eligibility for the certificate sought. Non-coursework requirements, such as the New York State Teacher Certification Examinations and fingerprint clearance, must also be satisfied.

Requirements:

- Associates Degree or Higher - Cyber Security 7-12
- Minimum 2.50 Undergraduate GPA
- Pedagogical Core - 18 S.H.
    - College Coursework - Human Development and Learning
    - College Coursework - Teaching Students with Disabilities & Special Health-Care Needs
    - College Coursework - Curriculum and Instruction
    - College Coursework - Teaching Literacy Skills Methods - 3 S.H.
    - College Coursework - Instruction and/or Assessment
    - College Coursework - Classroom Management
- Student Teaching - Cyber Security 7-12 - 40 Days
- Occupational Work Experience - Cyber Security 7-12 - 2 Yrs.
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Yrs.
- Mentored Experience - Cyber Security 7-12
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

<u>Pathway: Option B - Individual Evaluation</u>

This pathway is for candidates who are seeking a certificate in a career or technical subject but whose undergraduate program has not been preapproved by the State Education Department for certification. "Option B" candidates must hold a high school diploma or its equivalent. Candidates must submit original credentials for an evaluation to determine eligibility for the certificate sought. Non-coursework requirements, such as the New York State Teacher Certification Examinations and fingerprint clearance, must also be satisfied.

Requirements:

- Education - High School Diploma, GED or HSE
- Pedagogical Core - 18 S.H.
    - College Coursework - Human Development and Learning
    - College Coursework - Teaching Students with Disabilities & Special Health-Care Needs
    - College Coursework - Curriculum and Instruction
    - College Coursework - Instruction and/or Assessment
    - College Coursework - Teaching Literacy Skills Methods - 3 S.H.
    - College Coursework - Classroom Management
- Student Teaching - Cyber Security 7-12 - 40 Days
- Occupational Work Experience - Cyber Security 7-12 - 4 Years.
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years.
- Mentored Experience - Cyber Security 7-12
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: Option C - Individual Evaluation

This pathway is for candidates who possess an associate degree or its equivalent in the career and technical field in which a certificate is sought and at least two years of satisfactory teaching experience, excluding experience as a teaching assistant, at the post-secondary level in the certificate area to be taught or in a closely related subject area acceptable to the department

Requirements:

- Associates Degree or Higher - Cyber Security 7-12
- Minimum 2.50 Undergraduate GPA
- Paid, Post-Secondary Teaching Experience - Cyber Security 7-12 - 2 Years.
- Pedagogical Core - 18 S.H.
    - College Coursework - Human Development and Learning
    - College Coursework - Teaching Students with Disabilities & Special Health-Care Needs
    - College Coursework - Curriculum and Instruction
    - College Coursework - Teaching Literacy Skills Methods - 3 S.H.
    - College Coursework - Instruction and/or Assessment
    - College Coursework - Classroom Management
- Student Teaching - Cyber Security 7-12 - 40 Days
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years.
- Mentored Experience - Cyber Security 7-12
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: Option D - Individual Evaluation

The candidate possesses a full license as a teacher issued by the Department pursuant to section 126.6(f) in the career and technical field in which the application is submitted for.

Requirements:

- Valid NYS Full Private Career School Teacher License - Cyber Security
- Paid, Full-Time Teaching Experience Under the Full License - Cyber Security - 2 Years.
- Pedagogical Core - 18 S.H.
    - College Coursework - Human Development and Learning
    - College Coursework - Teaching Students with Disabilities & Special Health-Care Needs
    - College Coursework - Curriculum and Instruction
    - College Coursework - Teaching Literacy Skills Methods - 3 Years.
    - College Coursework - Instruction and/or Assessment
    - College Coursework - Classroom Management
- Student Teaching - Cyber Security 7-12 - 40 Days
- New York State Teacher Certification Exam - Educating All Students Test (EAS)

- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years.
- Mentored Experience - Cyber Security 7-12
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: Option G - Individual Evaluation

If you hold an Industry credential and have two years of work experience in the certificate area, you may be eligible for this option

Requirements:

- Holds an Industry Related Credential or Passed an Industry Accepted CTE Exam - Cyber Security
- Occupational Work Experience - Cyber Security - 2 Years.
- Pedagogical Core - 18 S.H.
    - College Coursework - Human Development and Learning
    - College Coursework - Teaching Students with Disabilities & Special Health-Care Needs
    - College Coursework - Curriculum and Instruction
    - College Coursework - Teaching Literacy Skills Methods - 3 S.H.
    - College Coursework - Instruction and/or Assessment
    - College Coursework - Classroom Management
- Student Teaching - Cyber Security 7-12 - 40 Days
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years.
- Mentored Experience - Cyber Security 7-12
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: Option H - Approved Program

If you are. Enrolled in a New York State Teacher education program for the certificate title for which you are applying and have at least one year of occupational experience, you may be eligible to use this pathway.

Requirements:

- Completion of a NYS Registered Program - Cyber Security 7-12
- Institutional Recommendation - Cyber Security 7-12
- One Year of Work Experience or Passing Score on an Industry Accepted CTE Exam - Cyber Security 7-12
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years.
- Mentored Experience
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: Option I - Holds A Valid 7-12 Classroom Teaching Certificate

If you hold a valid New York State teaching certificate in a Career and Technical field and either have two years of work experience or hold an industry credential in the certificate title you are applying for, you may be eligible for this pathway.

Requirements:

- Holds a Valid NYS Grade 7-12 Classroom Teaching Certificate (not CTE)
- Holds an Industry Related Credential or 2 Years of Satisfactory Work Experience - Cyber Security
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years.
- Mentored Experience
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

Pathway: Option J - Individual Evaluation

If you have a bachelor’s degree in the CTE Field and have one year of occupational work experience in the certificate area, you may be eligible for this option.

Requirements:

- Bachelor's Degree or Higher - Cyber Security
- Minimum 2.50 Undergraduate GPA
- One Year of Occupational experience or Hold an Industry Related Credential - Cyber Security
- Pedagogical Core - 18 S.H.
    - College Coursework - Human Development and Learning
    - College Coursework - Teaching Students with Disabilities & Special Health-Care Needs
    - College Coursework - Curriculum and Instruction
    - College Coursework - Teaching Literacy Skills Methods - 3 S.H.
    - College Coursework - Instruction and/or Assessment
    - College Coursework - Classroom Management
- Student Teaching - Cyber Security 7-12 - 40 Days
- New York State Teacher Certification Exam - Educating All Students Test (EAS)
- Paid, full-time Classroom Teaching experience - Cyber Security 7-12 - 3 Years.
- Mentored Experience - Cyber Security 7-12
- Workshop - Child Abuse Identification
- Workshop - School Violence Intervention and Prevention
- Workshop - Dignity for All Students Act
- Fingerprint Clearance
- Citizenship Status - INS Permanent Residence or U.S. Citizenship

PROGRAMS OF STUDY/CAREER PATHWAYS

HIGH SCHOOL STUDENT CYBERSECURITY COMPETITIONS

- National Cyber League (NCL)
- CyberPatriot
- CCDC
- NYU Cybersecurity Awareness Week (CSAW)
- Central New York Hackathon

GENCYBER CAMPS

The state of New York has hosted multiple GenCyber camps. The following is a list of the institutions hosting these camps.

- Mohawk Valley Community College
- Excelsior College
- Capital Region BOCES
- Questar III BOCES
- University at Buffalo
- Pace University

CAE CENTERS

1) Excelsior College
2) Fordham University
3) Mercy College
4) Mohawk Valley Community College
5) New York Institute of Technology
6) New York University
7) Pace University
8) Rochester Institute of Technology
9) Rockland Community College
10) Syracuse University
11) University at Albany
12) University at Buffalo
13) Utica College

STATE APPROVED CYBERSECURITY CAREER PATHWAYS PROGRAMS

APPROVED COLLEGE DEGREE AND CERTIFICATE PROGRAMS

SCHOOL NAME	PROGRAMS	NSA
ASA College	Associate of Occupational Studies in Network Administration and Security	
Columbia University in the City of New York	Master of Science in Technology Management – Cybersecurity Focus	
CUNY John Jay College of Criminal Justice	Online Master of Science in Computer Science – Computer Security Track	
DeVry University	Master of Science in Digital Forensics and Cybersecurity	
Excelsior College	Bachelor's in Computer Information Systems – Computer Forensics	NSA CAE
Fordham University	Bachelor's in Justice Administration – Digital Forensics	
Iona College	Bachelor of Computer Information Systems – Cyber Security Programming	
Keller Graduate School of Management	Bachelor of Science in Cybersecurity	
Long Island University-Riverhead Campus	Bachelor of Science in Information Technology (Cybersecurity)	
Mercy College	Bachelor of Science in Information Technology with dual degree option for MS (Cybersecurity)	NSA CAE
Mohawk Valley Community College	Bachelor of Science in Nuclear Engineering Technology with dual degree option for MBA (Cybersecurity)	
New York Institute of Technology	Master of Science in Cybersecurity	
New York University	Master of Science in Cybersecurity	NSA CAE
Onondaga Community College	Bachelor of Science in Computer Science with Concentration in Cyber Security	
Pace University-New York	Graduate Certificate in Information Security	NSA CAE
Rochester Institute of Technology	Advanced Certificate in Cyber Security Policy	NSA CAE
Rockland Community College	Bachelor of Science in Cybersecurity	NSA CAE
St. John's University	Master of Science in Cybersecurity	
SUNY at Albany	Computer Science: Cybersecurity AS	NSA CAE
SUNY Polytechnic Institute	Cybersecurity Certificate	
SUNY Westchester Community College	Master of Science in Information, Network, and Computer Security	
The Sage Colleges	Master of Science in Cybersecurity	
United States Military Academy	Master of Science in Cybersecurity Risk and Strategy	NSA CAE
University at Buffalo	Computer Forensics A.S.	NSA CAE
Yeshiva University	Advanced Certificate in Secure Software and Information Engineering	

OVERALL SUMMARY OF NEW YORK CYBERSECURITY PATHWAYS

New York State has a very centralized K-12 CTE system but it does allow for new and innovative programs. The state provides a good example for establishing K-12 CTE teacher qualifications and endorsements. The state has also done an admirable job supporting cybersecurity as a program of study within their information technology career cluster.

STATEWIDE CHALLENGES TO MAINTAINING CYBERSECURITY CAREER PATHWAY PROGRAMS

Like many other systems across the nation the real obstacles and challenges faced by the state cybersecurity career pathways initiatives are listed below:

FACULTY

- Recruiting new faculty
- Salary discrepancy with business and industry
- Faculty and staff training and development
- Retention and retirements

FACILITIES

- Cost
- Need for new technologies and products
- Security concerns
- Virtual and cloud based instructional content
- Keeping up with the moving target

OUTREACH

- More women
- More Minorities
- Better outreach to middle and high schools

BUSINESS AND INDUSTRY

- More internships
- Sponsorships
- Advisory members
- Adjunct faculty

STATEWIDE FINDINGS AND RECOMMENDATIONS

- The career pathways program in the state of New York is centrally managed by the Department of Education. The state of New York has established extensive CTE teacher endorsements to teach cybersecurity in K-12 programs. The state has a very detailed program approval process. The state also publishes an Implementation Guide, which can be found at www.p12.nysed.gov/cte/ctepolicy/guide.html.
- The state has also officially recognized several CTE programs at the K-12 level. The state also has a very strong CAE program and is involved in multiple cybersecurity competitions.
- Cybersecurity pathway programs in New York are primarily found in the information technology-related programs and computer science. Ohio also has cybersecurity certificates and majors available in their business schools.

OHIO

OHIO CTE AND CAREER PATHWAYS SYSTEM

The state of Ohio has:

State of Ohio CTE and Career Pathways Systems	
874	Public High Schools
70	Public High Schools Offering Solely/Primarily CTE Courses
513,740	Public High School Enrollment
125,375	High School CTE Enrollment
33,593	High School CTE Concentrators
52	Public Community Colleges
264,623	Public Community Colleges Enrollment (full & part-time)
94,291	Postsecondary CTE Enrollment
65,086	Postsecondary CTE Concentrators

OHIO CTE STRUCTURE

The state of Ohio CTE is offered, and career pathways are offered through the following institutions:

- Comprehensive high schools
- Charter Schools
- Joint vocational school districts
- Community colleges

OHIO CTE CAREER CLUSTERS

Ohio structures its CTE programs around 16 Career Field Technical Content Standards that are based on the National Career Clusters Framework and state workforce requirements. The Ohio Career Field Technical Content Standards are as follows:

1. Agricultural and Environmental Systems	2. Arts and Communications
3. Business and Administrative Services	4. Construction Technologies
5. Education and Training	6. Engineering and Science Technologies
7. Finance	8. Government and Public Administration
9. Health Science	10. Hospitality and Tourism
11. Human Services	12. Information Technology
13. Law and Public Safety	14. Manufacturing Technologies
15. Marketing	16. Transportation Systems

Ohio has also adopted state administrative rules that support Career Clusters and integrated them into the state plan. Several strategies are currently supporting these policies. All technical content standards reflect a Career Cluster framework, which includes both breadth and depth. Each Career Cluster technical content standards document includes embedded academic content standards and an emphasis on core business processes/systems as well as technical competencies appropriate to Career Cluster pathways and occupational specializations.

OHIO PROGRAMS OF STUDY

Ohio offers programs of study within all 16 of the Career Clusters.

1. Agriculture, Food & Natural Resources Career Cluster	9. Architecture & Construction Career Cluster
2. Arts, A/V Technology & Communications Career Cluster	10. Business, Management & Administration Career Cluster
3. Education & Training Career Cluster	11. Finance Career Cluster
4. Government & Public Administration Career Cluster	12. Health Science Career Cluster
5. Hospitality & Tourism Career Cluster	13. Human Services Career Cluster
6. Information Technology Career Cluster	14. Law, Public Safety, Corrections & Security Career Cluster
7. Manufacturing Career Cluster	15. Marketing Career Cluster
8. Science, Technology, Engineering & Mathematics Career Cluster	16. Transportation, Distribution & Logistics Career Cluster

OHIO CTE/CAREER PATHWAYS MEETING LOGISTICS

The MVCC team in coordination with Kyle Jones of Sinclair College at Building 12 Charity Hall in Dayton, OH on November 2, 2018.

Ohio Department of Education: www.education.ohio.gov

Advance CTE – Ohio: www.careertech.org/ohio

https://www.career-tech.education.ohio.gov

Applied Educational Systems – Ohio CTE Career Pathways: www.aeseducation.com/states/ohio/career-pathways

OHIO CTE/CAREER PATHWAYS MEETING LOCATION & AGENDA

Excerpt from the invitation:

"The Administration, staff and faculty at Sinclair College, would like to invite you to be participate in a discussion in regarding a future career pathway or cluster for cybersecurity in the state of Ohio. We will discuss ways to strengthen the opportunities for students to engage in this work by designing scalable pathways, and learning the skills needed to access these "new collar" jobs."

LOCATION

November 2, 2018
Sinclair College – Building 12
444 W Third St, Dayton, OH 45402

AGENDA

11:00am – 11:30am	**Registration** and Lunch
11:30am – 11:45am	**Welcome** – Dr. Dave Collins
11:45am – 11:50am	**SFS CyberCorps Partnership Community College Pilot Program** - Kyle Jones
11:50am – 11:55am	**Ohio Cyber Range -** Rebekah Michael, University of Cincinnati
11:55am – 12:00pm	**High School Cyber Education** - Dan Heighton, Clark State
12:00pm – 12:05pm	**META** - Elaine Horn, Cisco
12:05pm -12:15pm	**Leading the Way** - Dr. John Sands, MVCC and CSSIA
12:15pm – 12:45pm	**Cyber CTE pipeline for the Workforce and CAE Institutions** - Lynne Clark, NSA
12:45pm – 1:15pm	**Cybersecurity in the K-12 Space Perspective** - Davina Pruitt-Mentle, NIST
1:15pm – 1:30pm	Break
1:30pm – 2:00pm	**Panel** - CTE Career Pathways/Clusters in Ohio *Panelist:* **John Underwood** - Miami Valley CTC **Don Corbet** - Warren County Career Center **John Wiseman** - Ohio Department of Education **Taylor Adami** - Sidney High School
2:00pm – 2:15pm	Break
2:15pm – 2:45pm	**Panel** - Establishing a Career Pathways in Ohio *Panelists:* **Danis Heighton** - Clark State **Larry McWherter** - Columbus State **Kyle Jones** - Sinclair College **Rebekah Michael** - University of Cincinnati
2:45pm – 3:00pm	Break
3:00pm – 3:30pm	**Panel** - Business Partnerships and Opportunities *Panelist:* **Marc Pruett** - Honda **Jon Leichty** - Springfield-Clark CTC **Len Orlando** - Air Force Research Lab
3:30pm – 3:45pm	**Wrap Up** - John Sands, CSSIA

KEY STATE LEVEL CTE STAKEHOLDERS

- John Underwood-Miami Valley CTC
- Don Corbet-Warren County Career Center
- John Wiseman-Ohio Department of Education
- Taylor Adami-Sidney High School

CYBERSECURITY WORKGROUP FEBRUARY – MARCH 2018

Deborah Smedley
Vice President, Cyber Security and Technology Controls
JPMorgan Chase & Co.
Columbus, OH

Joe Blazeley
Assistant Vice, President, Security Compliance and Risk Management
Miami University
Oxford, OH

John Hoag
Associate Professor, School of Information and Telecommunications Systems
Ohio University and Case Western
Cleveland, OH

Jeff Sweet
Manager, Cyber Security Testing and Assessments
American Electric Power
Columbus, OH

STATE DIRECTOR

Emily Passias, Director

Office of Career-Technical Education
Ohio Department of Education
25 South Front Street
Columbus, OH 43215
emily.passias@education.ohio.gov

PROGRAMS OF STUDY/CAREER PATHWAYS

INFORMATION TECHNOLOGY

Technical and professional level careers in the design, development, support and management of hardware, software, multimedia and systems integration services.

NETWORK SYSTEMS

Network Systems program areas will prepare students for careers dealing with network systems analysis, planning and implementation. Students will gain the necessary technical and academic skills to design, install, maintain and manage network systems.

Careers for which this pathway prepares students include:

- Network Technician
- Operations Technician
- Systems Integration Advisor
- Cybersecurity Specialist

Postsecondary majors for which this pathway prepares students include:

- Computer Engineering Integrated
- Media and Technology
- Project Management Telecommunications

CYBERSECURITY

The Cybersecurity program area will prepare students for careers using technical and academic skills to design, develop, implement, and test secure information technology systems.

Careers for which this pathway prepares students include:

- Cybersecurity Specialist
- Security Administrator
- Network Technician
- Network Administrator
- Security Consultant/Specialist
- Computer Technician

Postsecondary majors for which this pathway prepares students include:

- Cybersecurity
- Computer Science
- Information Systems
- Software Engineering
- Digital/Computer
- Forensics

STATE APPROVED CYBERSECURITY CAREER PATHWAYS PROGRAM

MIDDLE SCHOOL

- Middle School Information Technology Course Titles and Descriptions

HIGH SCHOOL

- High School Information Technology Career Field Course Titles and Descriptions
- High School Information Technology Career Field Course Outlines

TECHNICAL CONTENT STANDARDS

- Information Technology Career Field Technical Content Standards

ASSESSMENT

- Program and Assessment Matrix
- WebXam

LICENSURE

- CTE Teacher Preparation and License Information
- Teacher Certificate and License Search

CAREER TECHNICAL STUDENT ORGANIZATION (CTSO)

- Business Professionals of America, Ohio Association
- SkillsUSA

APPROVED COLLEGE DEGREE AND CERTIFICATE PROGRAMS

SCHOOL NAME	PROGRAMS	NSA
Air Force Institute of Technology-Graduate School of Engineering & Management	Master of Science degree with a major in Cyber Operations	NSA CAE
Clark State Community College	Associate of Applied Science in Cybersecurity / Information Assurance	NSA CAE
Franklin University	Bachelor's in Cyber Security	
James A Rhodes State College	Associate of Applied Science in Network Security	
Kent State University at Kent	Computer Forensics and Information Security (Post-Secondary) Certificate	
Ohio State University-Main Campus	Bachelor of Science in Computer Science and Engineering (BS CSE) – Information and Computation Assurance	NSA CAE
Sinclair Community College	Bachelor of Science with a major in Computer and Information Science (BS CIS) – Information and Computation Assurance	NSA CAE
Terra State Community College	Information Systems Security – Short Term Certificate	NSA CAE
University of Cincinnati	Linux Security and Networking – Short Term Certificate	
Wright State University	Secure System Administration – Associate of Applied Science	

CYBERSECURITY PROGRAM ASSESSMENT

The state of Ohio and the Department of Education has done an incredible job defining cybersecurity program-assessed knowledge and skills. This work provides a great model for other states. The model not only includes many of the NSA CAE Knowledge Units (KU's), but also aligns to several NICE framework job role responsibilities.

CTE Program Name & Code	Subject Name	Subject Code	Curriculum Code/Min-Max Course Hours for VT, VM; Min Course Hours for V3, Vp	Student Grade Level for VT; V3; VP
(N4) Cybersecurity	Information Technology	145005	VT/60-280; V3/60; VM/30-60	7-12
(N4) Cybersecurity	Cybersecurity Pathway Course	146005	VT/120-280; V3/60; VM/30-60	7-12
(N4) Cybersecurity	Computer Hardware	145025	VT/120-280; VP/280; V3/60; VM/30-60	7-12
(N4) Cybersecurity	Computer Software	145030	VT/120-280; VP/280; V3/60	7-12
(N4) Cybersecurity	Networking	145035	VT/120-280; VP/280; V3/60; VM/30-60	7-12
(N4) Cybersecurity	Network Operating Systems	145040	VT/120-280; VP/280; V3/60	7-12
(N4) Cybersecurity	Network Management	145045	VT/120-280; VP/280; V3/60	7-12
(N4) Cybersecurity	Network Security	145050	VT/120-280; VP/280; V3/60	7-12
(N4) Cybersecurity	Routing and Switching	145055	VT/120-280; VP/280; V3/60	7-12
(N4) Cybersecurity	Programming	145060	VT/120-280; VP/280; V3/60; VM/30-60	7-12
(N4) Cybersecurity	Cybersecurity Defense and Reinforcement	146010	VT/120-280; VP/280; V3/60	7-12
(N4) Cybersecurity	Cybersecurity Testing and Response	146015	VT/120-280; VP/280; V3/60	7-12
(N4) Cybersecurity	Information Technology Capstone	145015	VT/120-280; VP/280; V3/60	7-12

INFORMATION TECHNOLOGY STRAND/OUTCOME PATHWAYCHART

An “X” indicates that the pathway applies to the outcome.

Strand/Outcome	Career Pathway				
	Information Support and Services	Interactive Media	Network Systems	Programming and Software Development	Cybersecurity
Strand 1: Business Operations/21st Century Skills					
Outcome 1.1: Employability Skills	X	X	X	X	X
Outcome 1.2: Leadership and Communications	X	X	X	X	X
Outcome 1.3: Business Ethics and Law	X	X	X	X	X
Outcome 1.4: Knowledge Management and Information Technology	X	X	X	X	X
Outcome 1.5: Global Environment	X	X	X	X	
Outcome 1.6: Business Literacy	X	X	X	X	
Outcome 1.7: Entrepreneurship/Entrepreneurs	X	X	X	X	
Outcome 1.8: Operations Management	X	X	X	X	
Outcome 1.9: Financial Management	X	X	X	X	
Outcome 1.10: Sales and Marketing	X	X	X	X	
Outcome 1.11: Principles of Business Economics	X	X	X	X	
Outcome 1.12: Cyber Hygiene					X
Strand 2: IT Fundamentals					
Outcome 2.1: Security, Risks, and Safeguards	X	X	X	X	X
Outcome 2.2: Networking Fundamentals	X	X	X	X	X
Outcome 2.3: Data Encoding	X	X	X	X	X
Outcome 2.4: Emerging Technologies	X	X	X	X	X
Outcome 2.5: Operating Systems	X	X	X	X	X
Outcome 2.6: Installation and Configuration	X	X	X	X	X
Outcome 2.7: Web Architecture	X	X	X	X	X
Outcome 2.8: Databases	X	X	X	X	X
Outcome 2.9: Project Concept Proposal	X	X	X	X	X
Outcome 2.10: Equipment	X	X	X	X	X
Outcome 2.11: Troubleshooting	X	X	X	X	X
Outcome 2.12: Performance Tests and Acceptance Plans	X	X	X	X	X
Outcome 2.13: Rollout and Handoff	X	X	X	X	X

Strand/Outcome	Pathway				
	Information Support and Services	Interactive Media	Network Systems	Programming and Software Development	Cybersecurity
Strand 3: Information Security					
Outcome 3.1: Components of Information Security	X	X	X	X	X
Outcome 3.2: General Security Compliance	X	X	X	X	X
Outcome 3.3: Network Security	X		X		X
Outcome 3.4: Multilayer Defense Structure	X		X		X
Outcome 3.5: Wireless Security	X		X		X
Strand 4: Infrastructure Systems					
Outcome 4.1: Network Infrastructure	X		X		X
Outcome 4.2: Open Systems Interconnection	X		X		X
Outcome 4.3: Network Media	X		X		X
Outcome 4.4: Wireless Communications	X		X		X
Outcome 4.5: Wireless Network Solutions	X		X		X
Outcome 4.6: Network Protocols	X		X		X
Outcome 4.7: Transmission Control Protocol/Internet Protocol (TCP/IP)			X		X
Outcome 4.8: Network Architecture			X		X
Outcome 4.9: Network Operating Systems			X		X
Outcome 4.10: Network Administration			X		X
Outcome 4.11: Cloud Computing			X		X
Outcome 4.12: Wide Area Network			X		X
Outcome 4.13: Disaster Recovery	X		X		X
Strand 5: Programming and Software Systems					
Outcome 5.1: Programming Concepts	X	X	X	X	
Outcome 5.2: Computational and String Operations	X			X	
Outcome 5.3: Logical Operations and Control Structures				X	
Outcome 5.4: Integrated Development Environment				X	
Outcome 5.5: Programming Conventions				X	
Outcome 5.6: Software Development Lifecycle				X	
Outcome 5.7: Configuration Management				X	
Strand 6: Web Development					
Outcome 6.1: Web pages	X	X	X	X	

Strand/Outcome	Pathway				
	Information Support and Services	Interactive Media	Network Systems	Programming and Software Development	Cybersecurity
Outcome 6.2: Links and Multimedia	X	X		X	
Outcome 6.3: Scripting		X		X	
Outcome 6.4: Web Forms		X		X	
Outcome 6.5: Websites		X		X	
Strand 7: Digital Media					
Outcome 7.1: Interactive Media	X	X	X	X	
Outcome 7.2: Multimedia Tools		X		X	
Outcome 7.3: Production		X		X	
Outcome 7.4: Graphics		X			
Outcome 7.5: Typography		X			
Outcome 7.6: Animation		X		X	
Outcome 7.7: Video		X			
Outcome 7.8: Audio		X			
Outcome 7.9: Photographs		X			
Strand 8: Databases					
Outcome 8.1: Data Modeling				X	
Outcome 8.2: Design and Creation				X	
Outcome 8.3: Data Entry and Access				X	
Outcome 8.4: Database Management				X	
Strand 9: Cybersecurity					
Outcome 9.1: Cybersecurity					X
Outcome 9.2: Access Control and Asset Security					X
Outcome 9.3: Application Development Security					X
Outcome 9.4: Network Security					X
Outcome 9.5: Threat Management					X
Outcome 9.6: Cyber Law					X
Outcome 9.7: Digital Forensics					X
Outcome 9.8: Countermeasures					X
Outcome 9.9: Disaster Recovery and Business Continuity					X
Outcome 9.10: Risk Management					X
Total Outcomes	41	41	45	46	46

STRAND 1. BUSINESS OPERATIONS/21ST CENTURY SKILLS

Learners apply principles of economics, business management, marketing, and employability in an entrepreneur, manager, and employee role to the leadership, planning, developing, and analyzing of business enterprises related to the career field.

OUTCOME 1.1. EMPLOYABILITY SKILLS

Develop career awareness and employability skills (e.g., face-to-face, online) needed for gaining and maintaining employment in diverse business settings.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X	X	X	X	X

Competencies

1.1.1. Identify the knowledge, skills, and abilities necessary to succeed in careers.

1.1.2. Identify the scope of career opportunities and the requirements for education, training, certification, licensure, and experience.

1.1.3. Develop a career plan that reflects career interests, pathways, and secondary and postsecondary options.

1.1.4. Describe the role and function of professional organizations, industry associations, and organized labor and use networking techniques to develop and maintain professional relationships.

1.1.5. Develop strategies for self-promotion in the hiring process (e.g., filling out job applications, resumé writing, interviewing skills, portfolio development).

1.1.6. Explain the importance of work ethic, accountability, and responsibility and demonstrate associated behaviors in fulfilling personal, community, and workplace roles.

1.1.7. Apply problem-solving and critical-thinking skills to work-related issues when making decisions and formulating solutions.

1.1.8. Identify the correlation between emotions, behavior, and appearance and manage those to establish and maintain professionalism.

1.1.9. Give and receive constructive feedback to improve work habits.

1.1.10. Adapt personal coping skills to adjust to taxing workplace demands.

1.1.11. Recognize different cultural beliefs and practices in the workplace and demonstrate respect for them.

1.1.12. Identify healthy lifestyles that reduce the risk of chronic disease, unsafe habits, and abusive behavior.

OUTCOME 1.2. LEADERSHIP AND COMMUNICATIONS

Process, maintain, evaluate, and disseminate information in a business. Develop leadership and team building to promote collaboration.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X	X	X	X	X

Competencies

1.2.1. Extract relevant, valid information from materials and cite sources of information.

1.2.2. Deliver formal and informal presentations.

1.2.3. Identify and use verbal, nonverbal, and active listening skills to communicate effectively.

1.2.4. Use negotiation and conflict-resolution skills to reach solutions.

1.2.5. Communicate information (e.g., directions, ideas, vision, workplace expectations) for an intended audience and purpose.

1.2.6. Use proper grammar and expression in all aspects of communication.

1.2.7. Use problem-solving and consensus-building techniques to draw conclusions and determine next steps.

1.2.8. Identify the strengths, weaknesses, and characteristics of leadership styles that influence internal and external workplace relationships.

1.2.9. Identify advantages and disadvantages involving digital and/or electronic communications (e.g., common content for large audience, control of tone, speed, cost, lack of non-verbal cues, potential for forwarding information, longevity).

1.2.10. Use interpersonal skills to provide group leadership, promote collaboration, and work in a team.

1.2.11. Write professional correspondence, documents, job applications, and resumés.

1.2.12. Use technical writing skills to complete forms and create reports.

1.2.13. Identify stakeholders and solicit their opinions.

1.2.14. Use motivational strategies to accomplish goals.

OUTCOME 1.3. BUSINESS ETHICS AND LAW

Analyze how professional, ethical, and legal behavior contributes to continuous improvement in organizational performance and regulatory compliance.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X	X	X	X	X

Competencies

1.3.1. Analyze how regulatory compliance affects business operations and organizational performance.

1.3.2. Follow protocols and practices necessary to maintain a clean, safe, and healthy work environment.

1.3.3. Use ethical character traits consistent with workplace standards (e.g., honesty, personal integrity, compassion, justice).

1.3.4. Identify how federal and state consumer protection laws affect products and services.

1.3.5. Access and implement safety compliance measures (e.g., quality assurance information, safety data sheets [SDSs], product safety data sheets [PSDSs], United States Environmental Protection Agency [EPA], United States Occupational Safety and Health Administration [OSHA]) that contribute to the continuous improvement of the organization.

1.3.6. Identify deceptive practices (e.g., bait and switch, identity theft, unlawful door-to-door sales, deceptive service estimates, fraudulent misrepresentations) and their overall impact on organizational performance.

1.3.7. Identify the labor laws that affect employment and the consequences of noncompliance for both employee and employer (e.g., harassment, labor, employment, employment interview, testing, minor labor laws, Americans with Disabilities Act, Fair Labor Standards Acts, Equal Employment Opportunity Commission [EEOC]).

1.3.8. Verify compliance with computer and intellectual property laws and regulations.

1.3.9. Identify potential conflicts of interest (e.g., personal gain, project bidding) between personal, organizational, and professional ethical standards.

OUTCOME 1.4. KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY

Demonstrate current and emerging strategies and technologies used to collect, analyze, record, and share information in business operations.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X	X	X	X	X

Competencies

1.4.1. Use office equipment to communicate (e.g., phone, radio equipment, fax machine, scanner, public address systems).

1.4.2. Select and use software applications to locate, record, analyze, and present information (e.g., word processing, e-mail, spreadsheet, databases, presentation,
Internet search engines).

1.4.3. Verify compliance with security rules, regulations, and codes (e.g., property, privacy, access, accuracy issues, client and patient record confidentiality) pertaining to technology specific to the industry pathway.

1.4.4. Use system hardware to support software applications.

1.4.5. Use information technology tools to maintain, secure, and monitor business records.

1.4.6. Use an electronic database to access and create business and technical information.

1.4.7. Use personal information management and productivity applications to optimize assigned tasks (e.g., lists, calendars, address books).

1.4.8. Use electronic media to communicate and follow network etiquette guidelines.

STRAND 4. INFRASTRUCTURE SYSTEMS

Learners apply principles of networking and infrastructure related to the installation, administration, and maintenance of computer networks and components. Knowledge and skills may be applied to network connectivity, cabling, protocols, architecture, classification, topologies, operating systems, Open Systems Interconnection (OSI) standards, data encoding, Quality of Service (QoS), Internet Protocol (IP) addressing, and wide area network (WAN) design.

OUTCOME 4.1. NETWORK INFRASTRUCTURE

Build a multinode network.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X		X		X

Competencies

4.1.1. Determine the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, mesh, hybrid) and identify broadband and baseband (e.g., Ethernet) transmission methods and standards.

4.1.2. Explain packet-switching techniques.

4.1.3. Compare the characteristics of connection-oriented and connectionless protocols and select protocols based on given criteria.

4.1.4. Identify standard and emerging network technologies (e.g., broadband, satellite, optic, cellular, Local-Area Network (LAN) and WiFi).

4.1.5. Describe how Unified Communication (UC) integrates voice, data, and video communications.

4.1.6. Configure and build a network.

OUTCOME 4.2. OPEN SYSTEMS INTERCONNECTION

Describe the Open Systems Interconnection (OSI) standard (International Organization for Standardization [ISO] Standard 7498).

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X		X		X

Competencies

4.2.1. Identify the benefits of using a layered network model.

4.2.2. Compare Open Systems Interconnection stack positions and their relationships to one another.

4.2.3. Compare the seven layers of the Open Systems Interconnection stack to the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

4.2.4. Compare the basics of Transmission Control Protocol/Internet layers, components, and functions.

4.2.5. Describe actions to be performed at each of the Open Systems Interconnection layers.

4.2.6. Explain how the Open Systems Interconnection layers relate to the elements of network communication.

OUTCOME 4.3. NETWORK MEDIA

Select, assemble, terminate, and test media.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X	X	X		X

Competencies

4.3.1. Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, cost).

4.3.2. Differentiate between media types (e.g., coaxial, twisted pair, fiber optic) and interfaces.

4.3.3. Compare media categories (e.g., single mode, multimode, CAT5, CAT5E, CAT6+).

4.3.4. Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], Registered Jack [RJ]-45, LC, ST) and grounding techniques.

4.3.5. Identify media standards (e.g., American National Standards Institute [ANSI], Electronic Industries Alliance/Telecommunications Industry Association [EIA/TIA] -568, EIA/TIA-568A and 568B).

4.3.6. Identify the advantages and disadvantages of cabling systems.

4.3.7. Describe typical problems associated with cable installation.

4.3.8. Assemble and test Ethernet cable (e.g., straight-through, crossover, loopback).

OUTCOME 4.4. WIRELESS COMMUNICATIONS

Explain wireless communications.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X		X		X

Competencies

4.4.1. Compare wireless standards in common use (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11, Cellular, Bluetooth, Worldwide Interoperability for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC]).

4.4.2. Compare characteristics of wireless signals (e.g., reflection, diffraction, scattering, fading).

4.4.3. Differentiate media access methods used by wireless.

4.4.4. Describe appropriate applications of wireless technologies to specific communication scenarios.

4.4.5. Compare Radio Frequency (RF) functions and principles.

OUTCOME 4.5. WIRELESS NETWORK SOLUTIONS

Design and implement wireless network solutions.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X		X		X

Competencies

4.5.1. Compare secure wireless solutions operating in ad-hoc mode and infrastructure mode.

4.5.2. Describe the frequency ranges and associated rules in the wireless spectrum as managed by the Federal Communication Commission (FCC).

4.5.3. Describe the Service Set Identifier (SSID) as used in wireless communications.

4.5.4. Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey.

4.5.5. Troubleshoot Wireless Local Area Networks (WLANs) using system logs, vendor-provided utilities, and diagnostic tools.

4.5.6. Secure the wireless network.

OUTCOME 4.6. NETWORK PROTOCOLS

Compare and contrast network protocols.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X		X		X

Competencies

4.6.1. Explain network protocols (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP], User Datagram Protocol [UDP], Internet Protocol Version 4 [IPv4], Internet Protocol Version 6 [IPv6]).

4.6.2. Identify the advantages of protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Hypertext Transfer Protocol [HTTP], Telecommunications Network [Telnet], Remote Desktop Protocol [RDP]], Secure Shell [SSH]) and associated port numbers.

4.6.3. Explain the purposes of encapsulation and decapsulation and their relationship to the Open Systems Interconnection (OSI) model.

4.6.4. Explain the difference between User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

4.6.5. Identify Transmission Control Protocol (TCP)and User Datagram Protocol (UDP) conventional ports (e.g., Simple Mail Transfer Protocol [SMTP], Telnet, Hypertext Transfer Protocol [HTTP], File Transfer Protocol [FTP]).

4.6.6. Explain Transmission Control Protocol/Internet Protocol (TCP/IP) protocol details (Internet addresses, Address Resolution Protocol [ARP], Reverse Address Resolution Protocol [RARP], IP datagram format, routing IP datagrams, TCP segment format, IPv4, IPv6).

4.6.7. Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP]).

4.6.8. Capture and analyze data packets.

OUTCOME 4.7. TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP)

Describe IP addressing schemes and create subnet masks.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
		X		X

Competencies

4.7.1. Explain Fully Qualified Domain Names (FQDNs) and how they are used.
4.7.2. Explain the IP addressing scheme and how it is used.
4.7.3. Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used.
4.7.4. Identify the class of network to which a given address belongs.
4.7.5. Differentiate between default subnet masks and custom subnet masks.
4.7.6. Explain the relationship between an IP address and its associated subnet mask.
4.7.7. Identify the differences between classful and classless addressing schemes.
4.7.8. Identify multicasting addresses and explain why they are used.
4.7.9. Create custom subnet masks to meet network design requirements.
4.7.10. Compare Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6).

OUTCOME 4.8. NETWORK ARCHITECTURE

Describe network architecture.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
		X		X

Competencies

4.8.1. Describe media-access protocols (e.g., Carrier Sense Multiple Access with Collision Detection [CSMA/CD], Carrier Sense Multiple Access with Collision Avoidance [CSMA/CA]).

4.8.2. Identify the components and relationships within the Institute of Electrical and Electronics Engineers (IEEE) 802 standards.

4.8.3. Identify Local Area Network (LAN) performance factors (e.g., signal attenuation, signal propagation delay).

4.8.4. Explain the role of the Internet Engineering Task Force (IETF) in facilitating protocol development.

4.8.5. Implement and maintain Virtual Local Area Networks (VLANs).

OUTCOME 4.9. NETWORK OPERATING SYSTEMS

Describe and install network operating systems (OSs).

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
		X		X

Competencies

4.9.1. Explain how the components of a network operating system (i.e., server platform, network services software, network redirection software, communications software) support network operations.

4.9.2. Identify licensing requirements.
4.9.3. Describe the characteristics of the tiered model (e.g., peer-to-peer, thin client, thick client, cloud).

4.9.4. Analyze the advantages and disadvantages of the client/server model.
4.9.5. Select network, desktop, and mobile Operating Systems.
4.9.6. Install, test, and patch network Operating Systems manually and using automation.
4.9.7. Log in to a network device (e.g., router, Secure File Transfer Protocol [SFTP] server, directory server).

4.9.8. Evaluate the performance of the network Operating System.

OUTCOME 4.10. NETWORK ADMINISTRATION

Administer network operating systems and services.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
		X		X

Competencies

4.10.1. Select physical and logical topology.
4.10.2. Connect devices to network systems.
4.10.3. Create domain trusts.
4.10.4. Maintain domain controllers.
4.10.5. Create user accounts, groups, and login scripts.
4.10.6. Establish shared network resources.
4.10.7. Define and set access controls on files, folders, shares, and directories.
4.10.8. Configure network domain accounts and profiles.
4.10.9. Create roaming user profiles and use Group Policy Objects (GPO) to manage the user environment.
4.10.10. Troubleshoot network performance connectivity (e.g., performance monitor, command line utilities).

4.10.11. Explain the fundamentals of Quality of Service (QoS).
4.10.12. Securely delegate standard management tasks.

OUTCOME 4.11. CLOUD COMPUTING

Implement a hypervisor.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
		X	X	X

Competencies

4.11.1. Differentiate between public, private, and hybrid clouds and describe the fundamental cloud components (e.g., shared or dedicated processing, storage, memory, networking, hypervisor).

4.11.2. Provision cloud services (e.g., Software as a Service [SaaS], Platform as a Service [PaaS], Infrastructure as a Service [IaaS], Security as a Service).

OUTCOME 4.12. WIDE AREA NETWORK

Design a wide area network (WAN).

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
		X		X

Competencies

4.12.1. Select Wide Area Network (WAN) connections (e.g., satellite, broadband, lease line, cellular, Multiprotocol Label Switching [MPLS], SD-WAN, Asynchronous Transfer Mode [ATM]).

4.12.2. Describe point-to-point (PTP) and point-to-multipoint (PTMP) interconnection.

4.12.3. Evaluate and select basic telecommunications services (e.g., satellite, circuit switching, wireless, packet switching) and carriers for WAN requirements.

4.12.4. Identify advantages to a software defined WAN (SD-WAN).

4.12.5. Determine availability from Local Area Network (LAN) to meet WAN requirements.

4.12.6. Determine the speed needed between sites to access applications.

4.12.7. Determine the subnets needed on the WAN (e.g., Variable Length Subnet Masking [VLSM]).

4.12.8. Evaluate and select transmission options.

4.12.9. Evaluate and select routing protocols (e.g., Border Gateway Routing Protocol [BGRP], Open Shortest Path First [OSPF], Routing Information Protocol Version 2 [RIPv2]).

4.12.10. Implement and maintain routing tables (e.g., static, default and dynamic routes).

4.12.11. Implement and maintain Network Address Translation (NAT) and Port Address Translation (PAT).

OUTCOME 4.13. DISASTER RECOVERY

Recommend disaster recovery and business continuity plans.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
X		X		X

Competencies

4.13.1. Differentiate between disaster recovery and business continuity.
4.13.2. Identify common backup devices.
4.13.3. Identify the criteria for selecting a backup system.
4.13.4. Establish a process for archiving files.
4.13.5. Develop a disaster recovery plan.

STRAND 9. CYBERSECURITY

Learners apply principles of Cybersecurity to secure and defend information technology systems, selection and implementation of methods and tools to secure physical and digital assets, mange threats, deploy countermeasures, and establish strategies to protect business information using risk and incident management.

OUTCOME 9.1. CYBERSECURITY

Examine and employ principles of Cybersecurity.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.1.1. Identify the goals, objectives and purposes of cybersecurity.
9.1.2. Describe the concepts of malware attack vectors.
9.1.3. Maintain data security using data labeling, handling and, disposal as prescribed by policy and law.

9.1.4. Mitigate threats by remaining abreast of industry information.
9.1.5. Identify types of controls (e.g., Deterrent, Preventive, Detective, Compensating, Technical, and Administrative).

9.1.6. Manage physical and digital assets.

OUTCOME 9.2. ACCESS CONTROL AND ASSET SECURITY

Apply identification (ID), authorization, and physical asset security.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.2.1. Perform authorization control (e.g., least privilege, separation of duties, mandatory access, discretionary access, rule-based access control, role-based access control, time of day restrictions, location distractions).

9.2.2. Implement authentication techniques (e.g., Tokens, Common access card, Smart card, Multifactor authentication, Single sign-on, Biometrics, Personal identification verification card, Username, Federation, Transitive trust/authentication).

9.2.3. Use authentication factors (e.g., Something you are, something you have, something you know).

9.2.4. Mitigate security implications of third-party connectivity and access.

9.2.5. Implement Data Loss Prevention (DLP).

9.2.6. Implement perimeter security (e.g., Fencing, Proximity readers, Access list, Proper lighting, Mantraps, Video Surveillance, Signs, Guards, Barricades, Biometrics, Protected distribution (cabling), Alarms, Motion detection).

9.2.7. Inventory devices.

OUTCOME 9.3. APPLICATION DEVELOPMENT SECURITY

Develop and maintain application security.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.3.1. Identify application vulnerabilities (e.g., Cross-site scripting, SQL injection, LDAP injection, XML injection, Directory traversal/command injection, Buffer overflow, Integer overflow, Zero-day, Cookies and attachments, Locally Shared Objects (LSOs), Flash cookies, Malicious add-ons, Session hijacking, Header manipulation, Arbitrary code execution/remote code execution).

9.3.2. Mitigate application attacks (e.g., SANS, OWASP).

9.3.3. Implement secure coding concepts (e.g., Error and exception handling, Input validation, Cross-site scripting prevention, Cross-site Request Forgery, (XSRF) prevention, OWASP).

9.3.4. Implement secure application configuration (e.g., Application hardening, Application patch management).

9.3.5. Discover and mitigate common database vulnerabilities and attacks.

9.3.6. Differentiate between Server-side vs. client-side validation.

OUTCOME 9.4. SETUP A SECURE NETWORK

Setup and maintain network security.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.4.1. Setup and maintain secure roles and system management techniques (e.g., password, group, and user privilege policies and monitoring).

9.4.2. Secure use of network Protocols (e.g., IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SCP, ICMP).

9.4.3. Apply principles of IPv4 and IPv6 securely.

9.4.4. Apply wireless security configurations (e.g., Disable SSID broadcast, TKIP, CCMP, Antenna placement, Power level controls).

9.4.5. Manage PKI and certificates (Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures).

9.4.6. Use of algorithms/protocols with transport encryption (e.g., SSL, TLS, IPSec, SSH, HTTPS).

9.4.7. Install and configure network devices (firewalls, switches, load balancers, proxies, web security gateways, VPN concentrators).

9.4.8. Install and configure network security devices. (Protocol analyzers, Spam filter, UTM security appliances, URL filter, Content inspection, Malware inspection).

9.4.9. Implement port security.

9.4.10. Monitor and manage network Unified Threat Management.

9.4.11. Mitigate network threats (e.g., Flood guards, Loop protection, Implicit deny, Network separation, Log analysis, Unified threat management, peripheral and removable media).

9.4.12. Apply the principles of secure Network Design (e.g., DMZ, Subnetting, NAT/PAT, Remote access, Telephony, Virtualization).

OUTCOME 9.5. THREAT MANAGEMENT

Mitigate common threats.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.5.1. Describe, locate, and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Logic bomb, Botnets, Ransomware, Polymorphic malware).

9.5.2. Describe and discover vulnerabilities to and mitigate network attacks. (e.g., Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Spit and other attacks).

9.5.3. Configure defenses for Password attacks (e.g., Brute Force, Dictionary attacks, Hybrid, Birthday attacks, Rainbow tables).

9.5.4. Describe, appraise for, and mitigate Social Engineering attacks (e.g., Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Phishing, Spear Phishing, Whaling, Vishing, Principles, URL hijacking, Watering Hole).

9.5.5. Perform penetration testing.

OUTCOME 9.6. CYBERSECURITY LAW

Adhere to Cybersecurity laws.

An “X” indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.6.1. Adhere to licensing and intellectual property laws (e.g., copyright, trademark, digital-rights management).

9.6.2. Adhere to regulatory and industry standards (e.g., PCIDSS, PADSS).

OUTCOME 9.7. DIGITAL FORENSICS

Capture and analyze information using digital tools.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.7.1. Recognize digital reconnaissance techniques (e.g., packet capture, OS fingerprinting, topology discovery, DNS harvesting).

9.7.2. Use tools and procedures for digital reconnaissance (e.g., host scanning, network mapping, NMAP, packet analyzer, vulnerability scanner).

9.7.3. Analyze reconnaissance results (data correlation, data analytics, point-in-time, data logs, packet captures).

9.7.4. Collect digital evidence according to established policies and protocols (e.g., system image, packet captures).

9.7.5. Maintain chain of custody on evidence.

9.7.6. Generate file hash.

OUTCOME 9.8. COUNTERMEASURES

Use countermeasures to monitor systems and reduce risk.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.8.1. Design and implement network segmentation.

9.8.2. Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, Camera vs. guard).

9.8.3. Use discovery tools and utilities to identify threats (e.g., Protocol analyzer, Vulnerability scanner, Honeypots, Honeynets, Port scanner).

9.8.4. Create, edit and use roles and system management tools.

9.8.5. Implement endpoint security.

9.8.6. Implement Access Control Lists (ACL).

9.8.7. Deploy a server hardening plan.

9.8.8. Implement a Network Access Control (NAC) plan.

9.8.9. Interpret alarms and alert trends.

9.8.10. Apply Incident response procedures (e.g., Preparation, Incident identification, Escalation and notification, Mitigation steps, Lessons learned, Reporting, Recovery procedures, First responder, Incident isolation, Quarantine, Device removal, Data breach).

9.8.11. Differentiate between types of Penetration testing (e.g., Black box, White box, Gray box).

OUTCOME 9.9. DISASTER RECOVERY AND BUSINESS CONTINUITY

Apply fundamentals of disaster recovery and business continuity.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.9.1. Describe the concepts of Risk Management (e.g., Business continuity concepts, Business impact analysis, Identification of critical systems and components, Removing single points of failure).

9.9.2. Describe the concepts of Risk assessment (e.g., Disaster recovery plan, IT contingency planning - Succession planning, Redundancy).

9.9.3. Describe and plan Fault tolerance (e.g., Hardware, RAID, Clustering, Load balancing, Disaster recovery concepts, Backup plans/policies, Backup execution/frequency).

OUTCOME 9.10. RISK MANAGEMENT

Apply concepts of risk management.

An "X" indicates that the pathway applies to the outcome.

Information Support and Services	Interactive Media	Network Systems	Programming and Software	Cybersecurity
				X

Competencies

9.10.1. Enforce concepts related to threat vectors and probability/threat likelihood.

9.10.2. Identify concepts of risk calculation (ALE, Impact, SLE, ARO, MTTR, MTTF, MTBF).

9.10.3. Implement Governance, risk management and Compliance Management processes (risk mitigation, govern compliance).

OHIO CYBER RANGE EXPANDS TO NORTHEAST OHIO LOCATION

"Ohio's statewide cyber range established in 2018 to train the cybersecurity workforce has been expanded. The Ohio Adjutant General's Department, the Ohio Department of Higher Education and the University of Akron announced that a memorandum of understanding has been signed to expand the Ohio Cyber Range by funding a new Ohio Cyber Range Core Services Site. The $1.18 million agreement will double the current capacity of the Ohio Cyber Range by adding servers, storage and programing at the University of Akron site. It joins the range network that includes a demonstration site that opened in May 2018 at the University of Cincinnati."

"The University of Akron has a strong existing cybersecurity program and a commitment to helping all of Ohio improve cyber education. This new site of the Ohio Cyber Range will bring range services closer to the residents of northeast Ohio and provide access to new learning tools for cybersecurity," said Maj. Gen. Mark E. Bartman, Ohio adjutant general. "With the Ohio Cyber Range and other innovative initiatives, Ohio can be a model for the rest of the country in cybersecurity." Rex Ramsier, executive vice president and chief administrative officer of the University of Akron, said, "We are excited to host the second site of the Ohio Cyber Range at the University of Akron. These new resources, combined with our existing programs in cybersecurity, will allow us to grow the number of graduates, as well as assist us in reaching out to students in regional high schools as we strive to increase the number of students who are going into this important field."

Reference: https://www.uakron.edu/im/news/ua-joins-ohio-cyber-range-in-1-18m-agreement/

STATE APPROVED CYBERSECURITY PROGRAMS IN OHIO

SCHOOL NAME	PROGRAMS
Air Force Institute of Technology – Graduate School of Engineering & Management	• Master of Science in Cyber Operations
American National University	• Bachelor of Science Degree in Cyber Security
Antioch University Midwest	• Bachelor of Arts in Liberal studies, Information Technology—Cyber Security Concentration
Baldwin Wallace University	• Bachelor of Science in Computer Network Security • Master of Business Administration in Computer Network Security
Belmont College	• Workforce development programs
Bryant & Stratton College	• Associate of Science Degree in Security Technology
Case Western Reserve University	• Graduate Certificate in Security in Computing
Cedarville University	• Cyber Security Track/Specialization in both Undergraduate Computer Science Degrees (Bachelor of Science) • Ph.D. Computer Science Degree
Clark State Community College	• Associate of Science degree in Cyber Security/Information Assurance Technology • Cyber Security Short Term Technical Certificate • Agreement with Wright State to major in Cyber Security (Clark State – Wright State)
Columbus State Community College	• Associate of Science Degree in Cyber Security • Cyber Security Certificate
Cuyahoga Community College	• Cyber Security Analytics Certificate
Defiance College	• Bachelor of Science in digital forensic science
Edison State Community College	• Associate in Applied Business in Network and Security
Fortis College - Centerville	• Associate of Science Degree in Cyber Security
Franklin University	• Bachelor of Science Degree offered in Cyber Security
Hocking College	• Associates of Applied Science in Network Systems Technology – Cyber Security Major
Kent State University	• Bachelor of Science in Computer Science with a Specialization in Information Security
Lakeland Community College	• Short Course/Training in Office Operations—Cyber Security for Managers
Lorain County Community College	• Computer Information Systems-Information Security for Business Short-Term Certificate • Computer Information Systems –Network Security Foundations Short-Term Certificate • Computer & Digital Forensics One-Year Certificate • Associate of Applied Science in Computer Engineering Technology- Computer and Digital Forensics Major
Marion Technical College	• Networking Major Associate of Applied Business
North Central State College	• Associate of Science degree in IT Cyber Security • Security Essentials Certificate • Network Security Essentials Certificate • Network Security Administration Certificate • Network Security Administration/Management Certificate • Cyber Security Network Defense Certificate

Northwest State Community College	• Associate in Applied Business in Information Technology with a specialization in Internet Security (A.A.B)
Owens Community College	• Associate in Applied Business Degree in System Security and Information Assurance Network and Systems Security Certificate
Rhodes State College	• Cyber security certificate • Associate of Applied Science in Network security
Sinclair College	• Associate of Applied Science--Cyber Investigation Technology • Associate of Applied Science-- Computer Information Systems/Secure System Administration • Workforce development training programs • Information Systems Security – Short Term Certificate • Network Engineering Security Associate – Short Term Certificate • Cyber Investigation – One-Year Technical Certificate
Southern State Community College	• Associate Degree in Cyber Security and Forensics
Stark State Community College	• Associate of Science in Cyber Security and Computer Forensics • Associate of Computer Network Administration and Security Technology
Terra State Community College	• Associate degree in Systems and Networking Support (includes all of Terra State's cyber security courses)
Tiffin University	• Bachelor of Arts in Cyber-Defense and Information Assurance
The Ohio State University	• Bachelor of Science in Computer Science and Engineering – Focus in Information Security
University of Akron	• Bachelor of Science Degree in Computer Information Systems (with security component) • Associate degree in Computer Information Systems (with security component)
University of Cincinnati	• Undergraduate level Cyber Security Certificate/Minor • Graduate Level Cyber Operations Certificate
University of Dayton	• Graduate Level certificate in Cyber Security • MIS, Operations Management, and Decision Sciences • Courses in the Department of Computer Science • Electrical and Computer Engineering
University of Findlay	• Bachelor of Science Degree in Computer Science with an emphasis in Information Assurance • Certificate in Information Assurance • Master of Science in Applied Security and Analytics
University of Mount Union	• Minor in Computer and Network Security
University of Northwestern Ohio	• Associate degree in IT Network Security
University of Toledo	• Minor in cyber security
Washington State Community College	• Associate of Technical Studies in Cyber Security
Western Governor's University	• Master of Science, Cyber Security and Information Assurance
Wittenberg University	• Computer Science with a Concentration in Cyber Security • Mathematics and Computer Science Department • Courses offered through the Computer Science Department
Wright State University	• Certificate in Cyber Security Analytics • Graduate level certificate in Cyber Security • Master of Science in Cyber Security
Youngstown State University	• Major in Computer Information Systems • Master of Computing and Information Sciences
Zane State College	• Associate in Information Assurance and Security Strategies • One-Year Certificate in Information Assurance and Security Strategies • Short-Term IT Security Certificate

OHIO TRANSFER AND ARTICULATION PROGRAMS

Because individual degree and certificate programs have varied purposes, learning outcomes, and course requirements, universal application of all credit is not feasible. Attempts to do so would, in many cases, seriously compromise program integrity and disadvantage student career readiness and advanced study. Consequently, certain credits will be recorded on the student transcript even when they will not necessarily apply to all or any degree or certificate programs at the receiving institution. As receiving institutions accept credit and then apply it towards graduation and specific program or major requirements, credit acceptance and application must always occur within the provisions of this Policy.

The provisions of this policy define pre-planned sets of courses and/or agreed-upon credit awarding structures for degree applicability, such as the Ohio Transfer Module (OTM), Transfer Assurance Guides (TAGs), Career-Technical Assurance Guides (CTAGs), Military Transfer Assurance Guides (MTAGs), course equivalency alignments to Advanced Placement (AP) exams, College-Level Examination Program (CLEP), apprenticeship programs, One-Year Option, and certain prior learning assessments, each of which is specifically designed to guarantee both the acceptance and application of credit to discrete courses that are required or program electives courses.

OHIO TRANSFER MODULE (OTM) REQUIREMENTS

Public institutions of higher education require all students to complete a set of liberal education courses within associate and baccalaureate degrees. These courses are commonly known as the general education requirements, but may be called "General Requirements", "University Requirements", "Core Requirements", or "Liberal Education Requirements". Because of the higher ratio of technical courses required in applied associate degree and technical study degree programs, these types of two-year degrees have a smaller set of general education requirements than other degree programs.

Similarly, the Ohio Transfer Module (OTM) is defined as either a subset or the complete set of an institution’s general education requirements in Associate of Arts (AA), Associate of Science (AS), and baccalaureate degrees. Applied and technical studies associate degrees have a smaller general education component as previously noted; therefore, students in these degrees may choose to go beyond the general education requirements of their program or degree and complete additional courses to fulfill more or all of the OTM requirements.

Institutions often have general education requirements which go beyond the OTM or have individual degree programs with specific requirements in the liberal education area which go beyond those required to meet the institution's general education requirements. Such additional requirements may be prerequisites for more advanced courses in the program, external professional accreditation association requirements, or part of the pedagogy of the field or the philosophical intent of the degree. For example, foreign language requirements of Colleges of Arts and Sciences are generally part of the philosophical basis of the degree. Likewise, foreign languages recommended in a chemistry degree may be helpful in the field and for graduate study. Such requirements determined by the institution provide each program its distinct character and must consistently apply to both native and transfer students alike.

As the philosophical and educational basis for the general education requirements may vary across programs and majors, the structuring of these requirements, through the total number and type of courses and/or credit hours required and the method of course delivery, may also vary among institutions and even among programs within institutions. Nonetheless, most institutions require a common body of knowledge and academic skills within the general education requirements. For this reason, receiving institutions have typically been able to apply transfer credit to many of their general education requirements for equivalent or similar courses.

OTM Guidelines were established after examining general education requirements of AA, AS, and baccalaureate degrees offered by Ohio public institutions of higher education and the legal definitions of general education requirements.

The Ohio Transfer Module contains 36-40 semester or 54-60 quarter hours of course credit in English composition (minimum of 3 semester or 5 quarter hours); mathematics, statistics, and logic (minimum of 3 semester or 3 quarter hours); arts and humanities (minimum of 6 semester or 9 quarter hours); social and behavioral sciences (minimum of 6 semester or 9 quarter hours); and natural sciences (minimum of 6 semester or 9 quarter hours).

Courses in oral communication and interdisciplinary areas may be included as elective credit hours by individual institutions to satisfy OTM requirements. Courses for the OTM should be at the lower-division level general education courses commonly completed during the first two years of a full-time student's residency.

1) Transfer students with an earned AA or AS degree which includes an identifiable OTM will have met the OTM requirements of the receiving institution. An institution will apply transferred courses to general education requirements which go beyond those included in the OTM on a course-by-course basis.
2) Transfer students who have completed the OTM as certified by the sending institution will have met the OTM requirements of the receiving institution. An institution will apply transferred courses to general education requirements which go beyond those included in the OTM on a course-by-course basis.
3) Students will receive credit for successfully completed courses from the OTM without having completed the entire module. The applicability of individual OTM-approved courses will depend on the approval type within the OTM. OTM courses reviewed and approved using only the established statewide learning outcomes will be guaranteed to be applied as equivalent courses at the receiving institution. If an equivalent course is unavailable, the credit hours associated with the course will be applied toward the appropriate area on a course-by-course basis. Credit hours associated with OTM-approved courses that were reviewed and approved using a hybrid of established statewide guidelines and learning outcomes will be guaranteed to transfer among public institutions of higher education and be applied appropriately on a course-by-course basis.
4) Completion of the OTM or the entire set of general education requirements may not constitute completion of specific program requirements unless the specified requirements are successfully completed as part of the OTM or the broader institutional general education requirements. In such cases, the receiving institution will apply transfer credit to these specific requirements at its discretion on a course-by-course basis.
5) OTM course credit applies to degree-specific general education course requirements on a course-by-course basis. For example, a student majoring in business needs to complete micro- and macroeconomics as part of the OTM Social and Behavioral Sciences when these courses are required for business degree-specific general education course requirements. Some of the OTM approved courses are also guaranteed to transfer and apply as equivalent pre-major/beginning major courses in accordance with the Transfer Assurance Guide (TAG) policy.

Courses evaluated to be equivalent to general education courses at the receiving institution will be applied to the General Education requirements of the receiving institution. Non-equivalent courses which were used to satisfy general education requirements at the sending institution, and which are in the general area of the courses used to satisfy the general education requirements at the receiving institution may be applied toward the general education requirements at the discretion of the receiving institution.

An institution's OTM must be explicitly defined in electronic and/or print catalogs and other appropriate places for the benefit of students and receiving institutions.

OVERALL SUMMARY OF OHIO CYBERSECURITY PATHWAYS

STATEWIDE CHALLENGES TO MAINTAINING CYBERSECURITY CAREER PATHWAY PROGRAMS

FACULTY

- Recruiting new cybersecurity faculty
- Retention of existing cybersecurity faculty
- Retirement of current cybersecurity faculty
- Salary discrepancy with business and industry

FACILITIES

- Security concerns
- Cost of programs and instructional facilities
- Need for new technologies and products
- Virtual and cloud based instructional content
- Updating instructional materials

OUTREACH

- More women and minorities
- Better outreach to middle and high schools

BUSINESS AND INDUSTRY

- More internships and apprentices
- Advisory members
- Adjunct faculty

STATEWIDE FINDINGS AND RECOMMENDATIONS

- The state of Ohio has a centralized Department of Education system. Career pathways in the state of Ohio are managed by their Department of Education. The state approves, tracks, and promotes cybersecurity curriculum from K-12 through the university system.
- The state has a very formalized process for periodic examination and updating of the career clusters framework, including cybersecurity programs.
- Cybersecurity pathway programs in Ohio are primarily found in the information technology-related programs and computer science. Ohio also has cybersecurity certificates and majors available in their business schools.
- The state of Ohio has a statewide articulation and transfer agreement referred to as Career-Technical Credit Transfer (CT)2. This program provides students the opportunity to transfer career and technical courses between K-12, colleges, and universities. The agreement also enables institutions to grant articulated credit hours for students completing one year of a CTE program. The One Year Option allows graduates from the Ohio Technical Center with 600 or greater hour programs to earn a block of technical credit toward an Associates of Technical Studies.
- The state of Ohio promotes dual-credit, dual-enrollment, and tech prep programs. The state also has early college programs that are targeted to incorporate cybersecurity programs.
- Several of the major state universities offer cybersecurity programs. Cybersecurity programs range from high school courses through Master's programs.
- CyberOhio is a cybersecurity initiative spearheaded by Ohio's Attorney General, Mike DeWine. Similar to other cybersecurity initiatives of its kind, CyberOhio aims to help businesses defend themselves against the ever-changing threat landscape through three key areas: education, new data privacy legislation, and information sharing.

WISCONSIN

WISCONSIN CTE AND CAREER PATHWAYS SYSTEM

The state of Wisconsin has:

State of Wisconsin CTE and Career Pathways Systems	
510	Public High Schools
6	Public High Schools Offering Solely/Primarily CTE Courses
255,826	Public High School Enrollment
88,086	High School CTE Enrollment
32,255	High School CTE Concentrators
18	Public Community Colleges
156,751	Public Community Colleges Enrollment (full & part-time)
121,330	Postsecondary CTE Enrollment
68,596	Postsecondary CTE Concentrators

WISCONSIN CTE STRUCTURE

The state of Wisconsin CTE is offered, and career pathways are offered through the following institutions:

- Comprehensive high schools
- Charter Schools
- Technical colleges

WISCONSIN CTE CAREER CLUSTERS

Wisconsin structures its CTE standards around six career field technical subjects that are based primarily on the 16 Career Clusters, industry skills standards and state workforce requirements. In particular, Wisconsin's secondary CTE career field technical subject areas are:

1. Agriculture, Food and Natural Resources (AFNR)	2. Business and Information Technology (B&IT)
3. Family and Consumer Science (FCS)	4. Health Science (HS)
5. Marketing, Management and Entrepreneurship (MME)	6. Technology and Engineering (TE)

The Wisconsin Technical College System maintains the WICareer Pathways initiative, which utilizes the 16 Career Clusters.

WISCONSIN PROGRAMS OF STUDY/CAREER PATHWAYS

The Wisconsin Technical College System and Department of Public Instruction jointly publish the state's guide for implementing Programs of Study. The guide provides details on how to develop and implement Programs of Study within the context of the ten components of Programs of Study established by the U.S. Department of Education.

Wisconsin maintains programs of study in all 16 Career Clusters, which can be found on the Wisconsin Career Pathway website.

1. Agriculture, Food & Natural Resources Career Cluster	9. Architecture & Construction Career Cluster
2. Arts, A/V Technology & Communications Career Cluster	10. Business, Management & Administration Career Cluster
3. Education & Training Career Cluster	11. Finance Career Cluster
4. Government & Public Administration Career Cluster	12. Health Science Career Cluster
5. Hospitality & Tourism Career Cluster	13. Human Services Career Cluster
6. Information Technology Career Cluster	14. Law, Public Safety, Corrections & Security Career Cluster
7. Manufacturing Career Cluster	15. Marketing Career Cluster
8. Science, Technology, Engineering & Mathematics Career Cluster	16. Transportation, Distribution & Logistics Career Cluster

PERKINS ELIGIBLE AGENCY

Wisconsin Technical College System

STATE OFFICES AND DIRECTORS

Wisconsin Technical College System Annette Severson, Associate Vice President WTCS Office of Instruction Phone: 608-267-9064 Email: annette.severson@wtcsystem.edu	**Madison Area Technical College** Kristin Long, Career Pathways Coordinator Madison Area Technical College Phone: 608-258-2422 Email: kklong@matcmadison.edu
Sandy Schmit, Education Director Electronics, Transportation and Automotive Phone: 608-266-1599 Email: sandra.schmit@wtcsystem.edu	**Wisconsin Department of Public Instruction** Sharon Wendt, Director Career and Technical Education Phone: 608-267-9251 Email: sharon.wendt@dpi.wi.gov
Ann Westrich, Education Director Career Prep and Transfer Information Phone: 608-261-4588 Email: ann.westrich@wtcsystem.edu	Barbara Bitters, Assistant Director Career and Technical Education (CTE) Phone: 608-266-9609 Email: barbara.bitters@dpi.wi.gov
Mark Johnson, Education Director Adult High School and Developmental Studies Phone: 608-266-1272 Email: mark.johnson@wtcsystem.edu	Wisconsin Department of Workforce Development Grant Westfall Information Development and Economic Analysis Phone: 608-266-5313 Email: grant.westfall@dwd.wisconsin.gov

FINDINGS

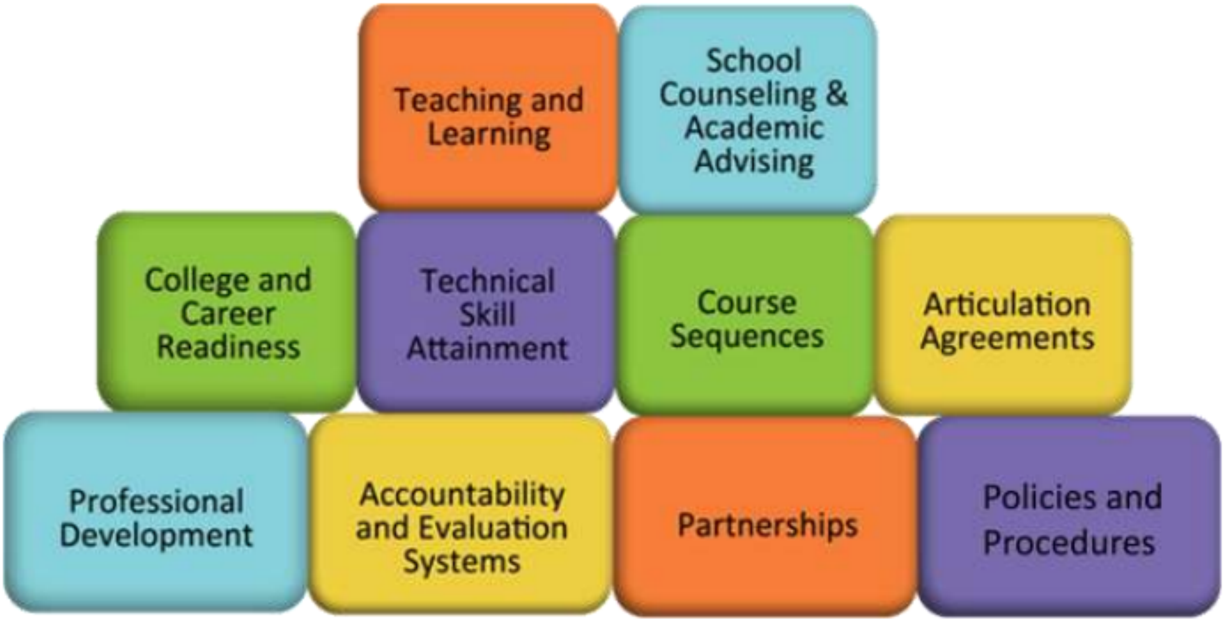
Wisconsin has many resources available for student interested in careers in cybersecurity. Wisconsin has a unique K-12 CTE Pathways program in that the state supports a group of technical colleges distributed across the state. These colleges focus on career and technical education and have made cybersecurity a priority in the state. Wisconsin also provides many opportunities for students to matriculate from K-12 programs all the way through university level cybersecurity programs. The technical centers serve as a bridge between K-12 programs, the workforce and advanced degrees.

WISCONSIN K-12 CTE CYBERSECURITY PREPARATION PROGRAMS

- AP Computer Science Principles Course - School District New Berlin (SDNB) includes cybersecurity as a topic
- Information Technology Academy (ITA) - is a pre-college initiative with the goal of increasing enrollment rates of diverse students at the University of Wisconsin-Madison
- SDNB Academic and Career Planning Guide
- Wisconsin’s K-12 Digital Learning Plan
- Inspire Wisconsin - Career Based Learning Activities for K-12 Students (Class Speakers, Field Trips, Online Career Coaches, Job Shadow, Internships, etc.). Sign Up your Business now to foster the next generation of IT professionals!
- Pathways Wisconsin - Regional IT Career Development for high school students
- Academic & Career Planning (Broad category) - Regional IT Career Development for high school students
- Wisconsin Department of Public Instruction - Bringing CyberSecurity Career Awareness to Your Business & Information Technology Education Course
- CyberPatriot - The National Youth Cyber Education Program created by the Air Force Association (AFA) to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future.
- SkillsUSA - SkillsUSA is a partnership of students, teachers and industry working together to ensure America has a skilled workforce. They provide educational programs, events and competitions that support career and technical education (CTE) in the nation’s classrooms.
- Cybersecurity Survival Guide - This guide provides a valuable overview of today’s threat landscape and describes the tools and technology required to defend against today’s cyber-attacks.

THE TEN COMPONENTS WISCONSIN POS

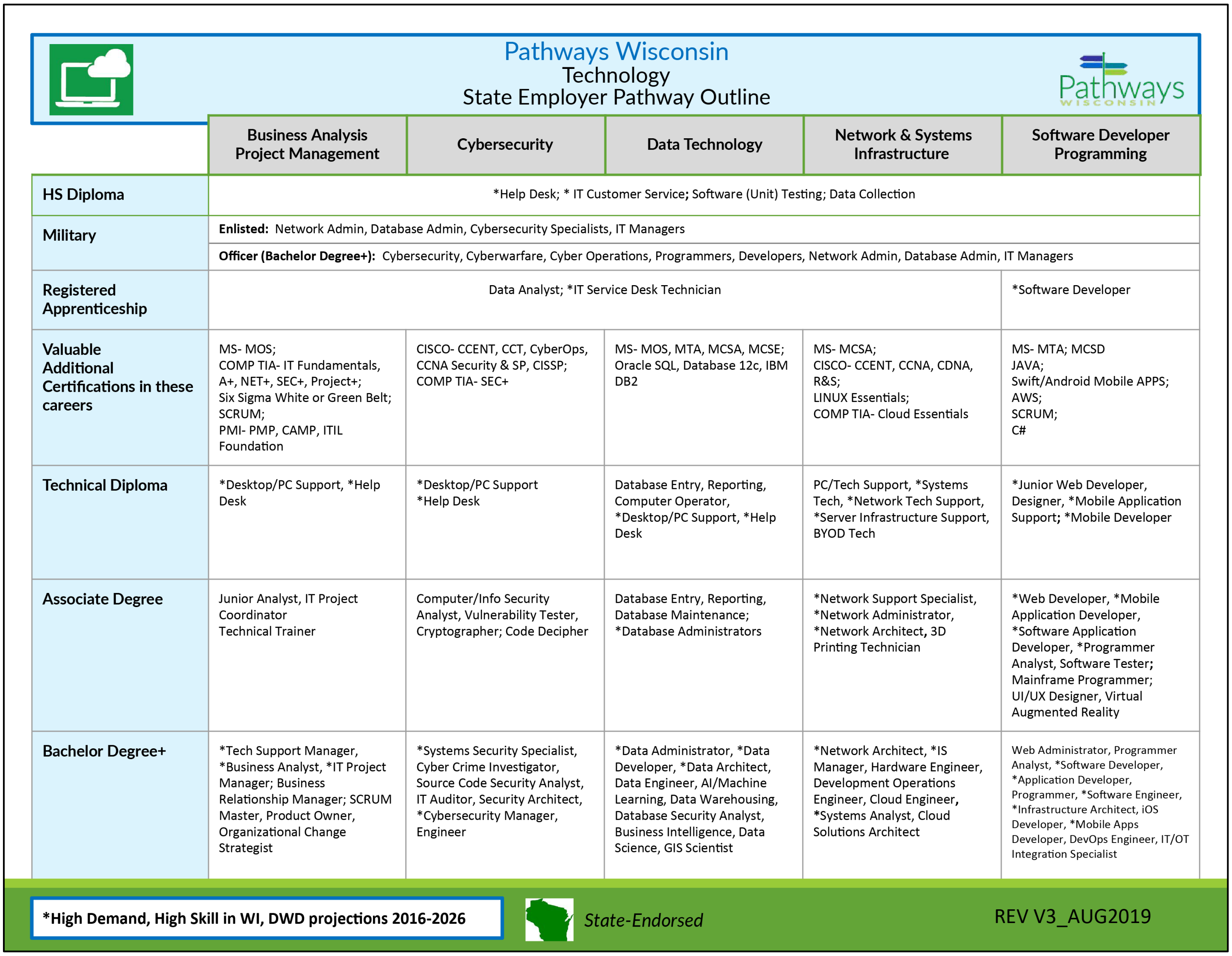
The Ten Components of POS implementation offered in this guide are from those published by the Office of Vocational and Adult Education (OVAE), U.S. Department of Education. OVAE's components are developed in collaboration with major national associations, organizations, and states. Please see the figure below for the chart of the 10 Components, provided by OVAE. These components are like building a brick foundation—each component is important and provides part of the foundation needed for a successful framework for Program of Study Implementation in Wisconsin. Working through the framework, educators can build a successful program of study.


Teaching and Learning
School Counseling & Academic Advising
College and Career Readiness
Technical Skill Attainment
Course Sequences
Articulation Agreements
Professional Development
Accountability and Evaluation Systems
Partnerships
Policies and Procedures

WISCONSIN POS IMPLEMENTATION PROCESS

There are five basic phases of work in implementing a program of study in Wisconsin:

1. Laying the Groundwork- Researching best practices and collecting data about model programs of study based on local labor market information.
2. Assembling a Team- gathering a representative group of all stakeholders who will work together to guide the creation of a Program of Study.
3. Designing and Building a POS- After selecting a specific pathway, team members analyze curriculum and determine development and improvement needs. The outcome of this phase is a detailed plan for the implementation of the program of study.
4. Implementing the Program of Study- the detailed Program of Study plan is put in place and students enroll in the program and continue on to post-secondary education.
5. Evaluating and refining the Program of Study- An evaluation plan is created that defines what data elements are needed, how they will be collected, what the benchmarks for success are, and who is responsible for providing the improvements in the Program of Study. Considerations for refinement of the Program of Study after a strong evaluation.



Pathways Wisconsin
Technology
State Employer Pathway Outline

	Business Analysis Project Management	Cybersecurity	Data Technology	Network & Systems Infrastructure	Software Developer Programming
HS Diploma	*Help Desk; * IT Customer Service; Software (Unit) Testing; Data Collection				
Military	**Enlisted:** Network Admin, Database Admin, Cybersecurity Specialists, IT Managers				
	Officer (Bachelor Degree+): Cybersecurity, Cyberwarfare, Cyber Operations, Programmers, Developers, Network Admin, Database Admin, IT Managers				
Registered Apprenticeship	Data Analyst; *IT Service Desk Technician				*Software Developer

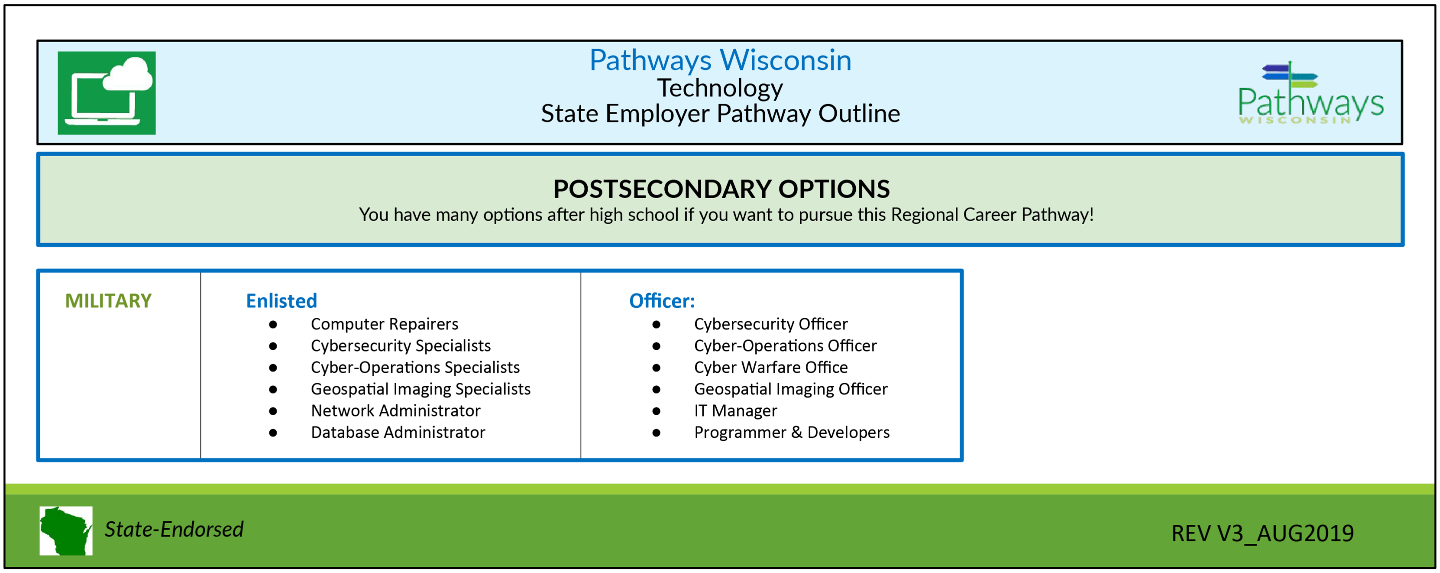
Valuable Additional Certifications in these careers	MS- MOS;
	COMP TIA- IT Fundamentals, A+, NET+, SEC+, Project+;
	Six Sigma White or Green Belt;
	SCRUM;
	PMI- PMP, CAMP, ITIL Foundation
		CISCO- CCENT, CCT, CyberOps, CCNA Security & SP, CISSP;
		COMP TIA- SEC+
			MS- MOS, MTA, MCSA, MCSE;
			Oracle SQL, Database 12c, IBM DB2
				MS- MCSA;
				CISCO- CCENT, CCNA, CDNA, R&S;
				LINUX Essentials;
				COMP TIA- Cloud Essentials
					MS- MTA; MCSD
					JAVA;
					Swift/Android Mobile APPS;
					AWS;
					SCRUM;
					C#

Technical Diploma	*Desktop/PC Support, *Help Desk	*Desktop/PC Support *Help Desk	Database Entry, Reporting, Computer Operator, *Desktop/PC Support, *Help Desk	PC/Tech Support, *Systems Tech, *Network Tech Support, *Server Infrastructure Support, BYOD Tech	*Junior Web Developer, Designer, *Mobile Application Support; *Mobile Developer
Associate Degree	Junior Analyst, IT Project Coordinator Technical Trainer	Computer/Info Security Analyst, Vulnerability Tester, Cryptographer; Code Decipher	Database Entry, Reporting, Database Maintenance; *Database Administrators	*Network Support Specialist, *Network Administrator, *Network Architect, 3D Printing Technician	*Web Developer, *Mobile Application Developer, *Software Application Developer, *Programmer Analyst, Software Tester; Mainframe Programmer; UI/UX Designer, Virtual Augmented Reality
Bachelor Degree+	*Tech Support Manager, *Business Analyst, *IT Project Manager; Business Relationship Manager; SCRUM Master, Product Owner, Organizational Change Strategist	*Systems Security Specialist, Cyber Crime Investigator, Source Code Security Analyst, IT Auditor, Security Architect, *Cybersecurity Manager, Engineer	*Data Administrator, *Data Developer, *Data Architect, Data Engineer, AI/Machine Learning, Data Warehousing, Database Security Analyst, Business Intelligence, Data Science, GIS Scientist	*Network Architect, *IS Manager, Hardware Engineer, Development Operations Engineer, Cloud Engineer, *Systems Analyst, Cloud Solutions Architect	Web Administrator, Programmer Analyst, *Software Developer, *Application Developer, Programmer, *Software Engineer, *Infrastructure Architect, iOS Developer, *Mobile Apps Developer, DevOps Engineer, IT/OT Integration Specialist

***High Demand, High Skill in WI, DWD projections 2016-2026**

State-Endorsed

REV V3_AUG2019



Pathways Wisconsin
Technology
State Employer Pathway Outline

POSTSECONDARY OPTIONS
You have many options after high school if you want to pursue this Regional Career Pathway!

MILITARY	**Enlisted** ● Computer Repairers ● Cybersecurity Specialists ● Cyber-Operations Specialists ● Geospatial Imaging Specialists ● Network Administrator ● Database Administrator	**Officer:** ● Cybersecurity Officer ● Cyber-Operations Officer ● Cyber Warfare Office ● Geospatial Imaging Officer ● IT Manager ● Programmer & Developers

State-Endorsed

REV V3_AUG2019

WISCONSIN ASSOCIATE DEGREE CYBERSECURITY PROGRAMS

- Bryant & Stratton College
- DeVry University
- Fox Valley Technical College
- Gateway Technical College
- Madison College
- Mid-State Technical College
- Milwaukee Area Technical College
- Moraine Park Technical College
- Waukesha County Technical College-Designated as a National Center of Academic Excellence in cybersecurity
- Wisconsin Indianhead Technical College

WISCONSIN BACHELOR OF SCIENCE DEGREE CYBERSECURITY PROGRAMS

UNIVERSITY OF WISCONSIN - MILWAUKEE CURRICULUM

- Bachelor of Business Administration - Information Technology Management
- Bachelor of Science - Computer Science
- Bachelor of Science - Information Science and Technology
- Cyber Career Paths with UW - Milwaukee

UNIVERSITY OF WISCONSIN - STOUT CURRICULUM

- Designated as a National Center of Academic Excellence in Cybersecurity
- Bachelor of Science - Applied Mathematics and Computer Science
- Bachelor of Science - Computer Science
- Bachelor of Science - Computer Networking and Information Technology
- Bachelor of Science - Information and Communication Technologies
- Cisco Certified Network Associate (CCNA) Exam Preparation [Undergraduate]
- Cisco Certified Network Professional (CCNP) Exam Preparation [Undergraduate]
- Cyber Security & Cyber Defense Professional [Undergraduate]

UNIVERSITY OF WISCONSIN - WHITEWATER CURRICULUM

- Bachelor of Business Administration - Information Technology & Supply Chain Management
- Bachelor of Science - Computer Science
- Minor – Cybersecurity

MARQUETTE UNIVERSITY

Designated as a National Center of Academic Excellence in Cybersecurity

WISCONSIN MASTER OF SCIENCE DEGREE CYBERSECURITY PROGRAMS

MARQUETTE UNIVERSITY

Master of Science in Computing with a specialization Information Assurance and Cyber Defense, Marquette University designated as a National Center of Academic Excellence in Cyber Defense Educations (CAE-CDE)

UNIVERSITY OF WISCONSIN - MILWAUKEE CURRICULUM

Master of Science in Information Science & Technology

UNIVERSITY OF WISCONSIN - STOUT CURRICULUM

Master of Science in Information and Communication Technologies

STATE RECOGNIZED CYBERSECURITY INDUSTRY CERTIFICATIONS

- Certified Ethical Hacker (CEH) - often discussed among white-hat hackers and penetration testers
- Certified Information Security Manager (CISM) - geared towards people in managerial positions (e.g. CIO of IT security).
- Certified Information Systems Auditor (CISA) - designed for professionals who audit, control, monitor and assess information technology and business systems
- Certified Information Systems Security Professional (CISSP) - an information security certification developed by the International Information Systems Security Certification Consortium
- Cisco Certification Pathway - globally-recognized IT certification programs through Cisco career certifications that will provide valuable, measurable advancement to networking professionals, their managers, and organizations.
- CompTIA - IT certification in Cybersecurity.
- GIAC Certified Incident Handler (GCIH) - for incident handlers responsible for detecting, responding to and resolving computer security incidents
- InfoSec Institute - trains on industry standard certifications such as CISSP
- Offensive Security Certified Professional (OSCP) - designed for penetration testers and includes a rigorous 24-hour certification exam.
- Palo Alto Networks Certifications -Industry-leading professional certifications that help validate technical competencies and knowledge of the Palo Alto Networks Security Operating Platform.

HIGH SCHOOL STUDENT CYBERSECURITY COMPETITIONS

1. National Cyber league
2. CyberPatriot
3. CCDC
4. DOE CyberForce
5. CSAW
6. National Cyber Analyst Challenge and Conference (NCAC)

CAE CENTERS

1. Marquette University
2. University of Wisconsin-Stout
3. Waukesha County Technical College

OVERALL SUMMARY OF WISCONSIN CYBERSECURITY PATHWAYS

STATEWIDE CHALLENGES TO MAINTAINING CYBERSECURITY CAREER PATHWAY PROGRAMS

FACULTY

- Retirement of current cybersecurity faculty
- Salary discrepancy with business and industry
- Recruiting of new cybersecurity faculty
- Retention of existing cybersecurity faculty

FACILITIES

- Operating cost of programs and instructional facilities
- Cost of new technologies and products

OUTREACH

- More women and minorities
- Better outreach to middle and high schools

BUSINESS AND INDUSTRY

- More internships and apprentices
- Advisory members
- Adjunct faculty

CYBERSECURITY INDUSTRY ASSOCIATIONS

Association Name	Description
WiCyS - Women In Cybersecurity	WiCyS is the only non-profit membership organization with national reach that is dedicated to bringing together women in cybersecurity from academia, research and industry to share knowledge, experience, networking and mentoring. The initiative was created through an NSF grant (Award #1303441) by Dr. Ambareen Siraj at Tennessee Tech University six years ago, and has grown into a wonderful alliance among academia, government and industry.
The SANS Institute	SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.
OWASP - The Open Web Application Security Project	The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.
ISSA - Information Systems Security Association	Developing and Connecting Cybersecurity Leaders Globally - ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.
FIRST - Forum of Incident Response and Security Teams	FIRST is the Forum of Incident Response and Security Teams. The idea of FIRST goes back until 1989, only one year after the CERT(r) Coordination Center was created after the infamous Internet worm. Back then incidents already were impacting not only one closed user group or organization, but any number of networks interconnected by the Internet.
Center for Internet Security	The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration. CIS provides resources that help partners achieve security goals through expert guidance and cost-effective solutions.
ISF - Information Security Forum	The ISF is the world's leading authority on information risk management. A not-for-profit organization, we supply authoritative opinion and guidance on all aspects of information security. We deliver practical solutions to overcome the wide-ranging security challenges that impact business information today.

Association Name	Description
National Association of ISACs	The mission of the National Council of ISACs (NCI) is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Members of the Council are the individual Information Sharing and Analysis Centers (ISAC) that represent their respective sectors.
Internet Security Alliance	ISA was founded in 2000 in collaboration with Carnegie Mellon University. ISA membership is open to public and privately held entities and currently has substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries.
IAPP - International Association of Privacy Professionals	The IAPP is the largest and most comprehensive global information privacy community and resource. Founded in 2000, the IAPP is a not-for-profit organization that helps define, support and improve the privacy profession globally.
ISACA	As an independent, nonprofit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.
National Cyber Security Alliance	NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets.
FISSEA - Federal Information Systems Security Educators' Association	The Federal Information Systems Security Educators' Association (FISSEA), founded in 1987, is an organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, education, and certification responsibilities.
AEHIS - The Association for Executives in Healthcare Information Security	The Association for Executives in Healthcare Information Security (AEHIS) launched in 2014 as the first professional organization serving healthcare's senior IT security leaders. AEHIS offers CSO's and other top-ranking information security leaders the professional development and networking opportunities critical for their success. Members have access to the educational resources and support for addressing key industry specific privacy and security issues.
International Association for Cryptologic Research	The International Association for Cryptologic Research (IACR) is a non-profit scientific organization whose purpose is to further research in cryptology and related fields. Cryptology is the science and practice of designing computation and communication systems which are secure in the presence of adversaries.

Association Name	Description
IIA - The Institute of Internal Auditors	The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.
CIUSPA - The Credit Union Information Security Professionals Association	CUISPA is a national association of credit union information technology professionals focused on improving security and risk management through cooperation.
ISRA - Information Security Research Association	The Information Security Research Association (commonly known as ISRA) is a registered non-profit organization focused on various aspects of Information Security including security research and cyber security awareness activities.
AISP - Association of Information Security Professionals	To promote, develop, support and enhance the integrity, technical competence, management expertise, status and interests of information security professionals in Singapore.
AISA - Australian Information Security Association	The Australian Information Security Association (AISA) is an Australian representative industry body for the information security profession. Formed in 1999, AISA is focused on individual membership. AISA aims to foster and promote the development of the information security industry and encourage the professional development of our members.
IASAP - International Association of Security Awareness Professionals	Formed in 2012, the International Association of Security Awareness Professionals is an independent 501(c)6 non-profit association comprised of corporate members. Member participants are professionals who manage information security awareness programs for their organizations and are responsible for everyday awareness operations.
EWF - Executive Women's Forum on Information Security, Risk Management & Privacy	The Executive Women's Forum is the largest member organization serving emerging leaders as well as the most prominent and influential female executives in the Information Security, Risk Management and Privacy industries.
ISFS - Information Security & Forensics Society	Information Security and Forensics Society (ISFS) was registered under the Hong Kong Societies Ordinance in May 2000. Our mission is to advocate and enforce professionalism, integrity and innovation in Information Security and Computer Forensics in Hong Kong and the surrounding region.

Association Name	Description
Cyber, Space & Intelligence Association	Cyber, Space, & Intelligence Association was founded in early 2011 to provide an environment for a vital flow of ideas between national security thought leaders in Government, Industry, and Congress focused Cyber, Space, and Intelligence challenges and opportunities.
CSA - Cloud Security Alliance	The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.