
WEST VIRGINIA STATE
UNIVERSITY

# BACHELOR OF SCIENCE IN CYBERSECURITY PROPOSAL

December 13, 2024

| | |
|---|---|
| **Institution:** | West Virginia State University |
| **Date:** | December 13, 2024 |
| **Category of Action:** | Proposal |
| **Title of Degree:** | Bachelor of Science in Cybersecurity |
| **Location:** | WVSU, Institute, WV 25112 |
| **Projected Program Implementation Date:** | Fall 2025 |

# TABLE OF CONTENTS

**To:**
Chancellor and Vice Chancellor for Academic Affairs,
West Virginia Higher Education Policy Commission

**Subject:**
Bachelor of Science in Cybersecurity

**Date:**
November 18, 2024

---

## §133-11-5.2.1.a: EDUCATIONAL OBJECTIVES

The Bachelor of Science in Cybersecurity at West Virginia State University (WVSU) equips graduates with the knowledge and skills needed for successful careers in cybersecurity. The program emphasizes the protection of critical infrastructure, including Supervisory Control and Data Acquisition (SCADA) systems, industrial control systems (ICS), and the cybersecurity of strategic sectors like agriculture. Upon graduation, students will be able to:

1. **Design and Secure Critical Infrastructure Systems**: Apply cybersecurity principles, methodologies, and tools to design, implement, and maintain secure information systems, with a focus on protecting critical infrastructure such as SCADA and ICS systems in sectors like power, water treatment, and agriculture.
2. **Analyze Cyber Threats and Vulnerabilities**: Identify, evaluate, and prioritize cybersecurity threats, risks, and vulnerabilities specific to critical infrastructure. Graduates will develop comprehensive threat models and perform risk assessments to protect essential public and private sector systems.
3. **Develop and Implement Defense Mechanisms**: Formulate and apply advanced cybersecurity strategies and countermeasures to prevent, detect, and respond to cyberattacks on critical infrastructure. This includes leveraging hands-on experience from the CyberHive lab and Cybersecurity Clinic for real-world vulnerability assessments and defense applications.
4. **Investigate and Mitigate Cybercrimes**: Conduct in-depth investigations of cybercrimes using digital forensics techniques to gather, analyze, and preserve evidence. Graduates will be skilled in mitigating the impact of cyberattacks on SCADA, ICS, and other critical infrastructure, particularly in agriculture and public utilities.
5. **Draft, Implement, and Enforce Security Policies**: Develop, enforce, and monitor security policies, standards, and procedures that align with industry best practices. Graduates will ensure regulatory compliance and minimize risks across various sectors, with a focus on critical infrastructure protection.
6. **Apply Cryptography and Secure Communication Techniques**: Utilize cryptographic methods, algorithms, and mathematical principles to secure communications and data across

critical systems. Graduates will design and implement encryption solutions tailored to the needs of critical infrastructure, ensuring the integrity and confidentiality of sensitive data.

7. **Collaborate Across Disciplines for Public Interest Cybersecurity**: Leverage interdisciplinary knowledge across fields such as agriculture, information management systems, and criminal justice to address cybersecurity challenges. Graduates will work with diverse stakeholders to secure public infrastructure and apply cybersecurity solutions for community-serving organizations.

These learning objectives ensure that graduates are prepared to address evolving cybersecurity challenges, particularly in securing critical infrastructure and engaging in practical, real-world applications through the program's industry partnerships and community-focused initiatives.

## §133-11-5.2.1.b: Mission Alignment Statement

The WVSU mission statement is: “West Virginia State University is a diverse 1890 land-grant institution that advances knowledge through access and opportunity, innovative teaching and learning, interdisciplinary research, and impactful service. Our learners are equipped to meet the economic and social needs of the state, region, and nation, and contribute solutions to complex global challenges.”

WVSU president in his State of the University interview on Mar 20, 2024, announced that WVSU currently offers a minor in cybersecurity, with the goal of expanding it into a Bachelor of Science program. Our commitment is to ensure that our students are well-equipped to thrive in this rapidly emerging field, making cybersecurity a key achievement of our university's recent progress.

The program's focus on both the theoretical and practical aspects of securing critical infrastructure, such as SCADA systems in water treatment plants and automated agricultural systems, reflects the University's commitment to innovative teaching and learning. By preparing graduates to design secure systems, analyze threats, develop countermeasures, and investigate cybercrimes, the program contributes to meeting the economic and social needs of the state, region, and nation. Additionally, the program's emphasis on developing security policies and applying cryptographic techniques supports interdisciplinary research and the creation of impactful solutions to complex global challenges. Through this alignment, WVSU continues to advance knowledge and prepare learners to contribute meaningfully to the cybersecurity field and to the broader community. To further validate the program’s excellence, WVSU will seek designation from the Center of Academic Excellence in Cyber Defense (CAE-CD) from The National Centers of Academic Excellence in Cybersecurity program.

Special features of WVSU that make it suitable for this program are: First, it is a historically black university and, hence, has always had a mission to educate minorities and other underrepresented populations. Second, as a land-grant University, WVSU is charged with providing educational opportunities for students, citizens, and surrounding communities via its tripartite mission of teaching, research, and extension. Third, continuing with the land grant mission, WVSU has growing academic programs in agriculture and well-established agriculture research programs, and this proposed program will integrate cybersecurity principles into existing agriculture activities (education, research, and outreach). Consequently, it will significantly enhance the safety and effectiveness of agricultural systems and advancements at WVSU. Fourth, WVSU has already

established a Cybersecurity Innovation Center (with grants from the Department of Education, Google, and Kanawha County Commission) and IBM Cybersecurity Leadership Center (one of only 20 such centers at HBCUs across the United States) where cybersecurity awareness, learning, and research activities are already taking place. This program will underpin these activities besides WVSU's mission to be instrumental in developing the future cybersecurity workforce.

## §133-11-5.2.2: PROGRAM DESCRIPTION

The Bachelor of Science in Cybersecurity (BSCyS) program at WVSU is designed to prepare students for dynamic and high-demand careers in cybersecurity. This program equips students with the technical skills, theoretical knowledge, and practical experience necessary to secure and defend public-interest organizations against cyber threats. This program stands out in West Virginia for its targeted focus on industrial control systems (ICS), including SCADA systems, and cybersecurity in agriculture, offering students practical experience through partnerships with IBM, Google, and local community entities.

### (i) Program Highlights

- **Jobs-Oriented Curriculum:** This program will adopt the cybersecurity workforce framework 1.0 by the National Initiative for Cybersecurity Education (NICE). Department of Homeland Security (DHS) partnered with industry, academia, and government to develop this Workforce Framework. It is being implemented across the Federal Government and is accepted as a best practice resource to define the field of cybersecurity. This framework represents a collaborative effort between government, academia, and industry focused on enhancing cybersecurity education, training, and workforce development. By incorporating the NICE Framework, students will acquire a comprehensive understanding of cybersecurity management, incident response, security threat assessment, and the broader societal impacts of cybersecurity. The curriculum will also address critical topics such as cybercrime, policy, human factors, risk management, and ethics, ensuring graduates emerge as well-rounded professionals equipped to handle the diverse challenges in the cybersecurity field.

- **Cybersecurity Concepts and Tools:** Students are introduced to core cybersecurity concepts, such as preventing, detecting, responding to, and mitigating cyber-attacks. The program provides hands-on experience with cybersecurity tools and technologies, enabling students to design and implement robust security measures.

- **Cybersecurity in Agriculture**: In response to the growing digitization of agricultural technologies (e.g., smart farming, precision agriculture, and automated systems), the program includes a focus on securing agricultural data and infrastructure. Students will learn to protect food supply chains and agricultural systems from potential cyber threats, ensuring the integrity of a critical sector within the economy.

- **Interdisciplinary Focus**: The program promotes interdisciplinary learning by integrating knowledge from other fields such as agriculture, business, healthcare, and criminal justice. Through collaborations with other WVSU departments and external partners, students will gain a well-rounded understanding of how cybersecurity intersects with and enhances various industries, positioning them to tackle complex challenges across sectors.

- **Critical Infrastructure Security:** A key focus of the BSCyS program is securing critical infrastructure. Utilizing WVSU's state-of-the-art cybersecurity labs acquired through a joint grant from the Department of Education with Marshall University, students gain practical experience in defending critical systems. The CyberHive, a dedicated facility within the labs, houses a physical SCADA learning system, providing a realistic environment for students to understand and address the unique challenges of securing critical infrastructure.

- **Cybersecurity Clinic Experience:** Starting in 2025, the program will be supported by the University's Cybersecurity Clinic, established through a $1 million grant from Google. This clinic offers students the opportunity to engage in real-world cybersecurity challenges, particularly in conducting Cyberattack Vulnerability Assessments. Students will evaluate and assess public infrastructure, gaining invaluable practical experience that bridges the gap between theoretical knowledge and real-world application. The public critical infrastructure will benefit from the free vulnerability assessments and cyberattack evaluations.

- **Partnerships with Industry Leaders**: As one of only 20 HBCUs with an IBM Cybersecurity Leadership Center, WVSU's program offers students the opportunity to earn industry-recognized certifications and badges, enhancing their employability in the cybersecurity workforce. The students can access those resources free of cost. For example, WVSU has started the IBM Freshmen Initiative by requiring every student in GED 101 (Freshmen Experience class) to take at least one of the three IBM foundational badges (Cybersecurity, AI, or Data Science). The new Cybersecurity program will use the IBM resources by embedding them in the program curriculum to provide direct or supplemental education. Access to all these resources from IBM is free of cost to WVSU and its students.

- **Commitment to Diversity and Community Impact:** As an HBCU and land-grant institution, WVSU is committed to providing access to cybersecurity education for underrepresented minorities and underprivileged students, ensuring a more diverse and inclusive cybersecurity workforce.

### (ii) Program Details

This program is dedicated to producing graduates who are not only technically proficient but also strategically skilled, ready to lead cybersecurity initiatives in both public and private sectors. With a focus on critical infrastructure security, including agriculture, and a practical, hands-on learning approach, this program positions students at the forefront of the cybersecurity industry.

The proposed Bachelor of Science in Cybersecurity requires the completion of 120 credit hours for graduation. This workforce-oriented program is designed with courses to provide the required knowledge and skills to conduct cybersecurity tasks for the defined NICE framework Cybersecurity roles. For detailed descriptions of NICE work roles, please refer to Appendix 2. The program offers two areas of concentration:

- **Option A:** Cybersecurity
- **Option B:** Agriculture Cybersecurity

The tables below outline the program curriculum, including Core courses (Table 1), concentration-specific courses (Table 2), Cognates (Table 3), General Education requirements (Table 4), and the summary of the program required credit hours (Table 5). New courses introduced as part of the program are marked with an asterisk (*). For detailed course descriptions, please refer to Appendix 1.

*Table 1 Majors Courses*

| **Core Courses (45 credit hours)** | | |
|---|---|---|
| **Catalog Number** | **Course Title** | **Credit Hours** |
| CS 101 | Programming Fundamentals | 3 |
| CS 102 | The Object-Oriented Paradigm | 3 |
| CS 215 | Introduction to Unix/Linux systems | 3 |
| CS 230 | Database Management Systems | 3 |
| CS 240 | Data Communications and Networking | 3 |
| CS 250 | Data Structures and Algorithms | 3 |
| CS 316 | Cybersecurity Principles and Practice | 3 |
| CS 336 | Scripting Languages | 3 |
| CS 408 | Senior Seminar | 2 |
| CS416 | Computer Forensics and Penetration Assessment | 3 |
| CYB 101* | Cybersecurity Fundamentals | 3 |
| CYB 201* | Cybersecurity Law and Ethics | 1 |
| CYB 317* | Cyber Incident Response | 3 |
| CYB 340* | Network Security | 3 |
| CYB 409* | Secure Software Development | 3 |
| CYB 360* | AI and Machine Learning in Cyber Defense | 3 |

*Table 2 Concentration Courses*

| **Option A: Cybersecurity (9 credit hours)** | | |
|---|---|---|
| CS 309 | Software Engineering | 3 |
| CS 410 | Systems Administration | 3 |
| CYB 411* | Industrial Control Systems Cybersecurity | 3 |
| **Option B: Agriculture Cybersecurity (9-10 credit hours)** | | |
| CYB 412* | IoT Security | 3 |
| AFNR 101* | Introduction to Agriculture, Food and Natural Resources | 3 |
| One of the following courses: (also fulfills General Education Scientific Reasoning requirement) | | |
| BIOL 108 | Environmental Biology | 4 |
| BIOL 110 | Economic Biology | 4 |
| CHEM 132 | Introductory Environmental Chemistry | 3 |

*Table 3 Cognate Courses*

| Cognate Courses | | |
|---|---|---|
| **Catalog Number** | **Course Title** | **Credit Hours** |
| **Option A: Cybersecurity (18-19 credit hours)** | | |
| MATH 120 | College Algebra | 3 |
| MATH 205 | Discrete Mathematics | 3 |
| MATH 305* | Introduction to Cryptography | 3 |
| PHYS 217 | Electronics and Microcontrollers Laboratories | 2 |
| CJ101 | Introduction to Criminal Justice | 3 |
| One option from below: | | |
| (CHEM 105 and | General Chemistry I | 3 |
| CHEM 107) | General Chemistry Lab I | 2 |
| or | | |
| BIO 120 | Fundamentals of Biology - fulfills General Education Scientific Reasoning requirement. | 4 |
| **Option B: Agriculture Cybersecurity (18-19 credit hours)** | | |
| MATH 120 | College Algebra | 3 |
| MATH 205 | Discrete Mathematics | 3 |
| MATH 305* | Introduction to Cryptography | 3 |
| PHYS 217 | Electronics and Microcontrollers Laboratories | 2 |
| PHYS 352 | Introduction to Geographical Information Systems | 3 |
| One course from below: | | |
| (CHEM 105 and | General Chemistry I | 3 |
| CHEM 107) | General Chemistry Lab I | 2 |
| or | | |
| BIO 120 | Fundamentals of Biology - fulfills General Education Natural Science requirement. | 4 |

*Table 4 General Education Courses*

| General Education Courses (38 credit hours) | |
|---|---|
| **General Education Area** | **Credit Hours** |
| First Year Experience | 3 |
| Written Communications I | 3 |
| Written Communications II | 3 |
| Oral Communications | 3 |
| Mathematics | 3 |
| Scientific Reasoning | 3-4 |
| Arts | 3 |
| Humanities | 3 |
| International Perspectives | 3 |
| History | 3 |
| Natural Sciences | 3-4 |
| Social Sciences | 3 |
| Wellness | 2 |

*Table 5 Program Credits Hours Summary*

| | **Program Credit Hours Summary** | | | | | |
|---|---|---|---|---|---|---|
| | General Education* | Core | Concentration courses | Cognates | Free Elective | Total |
| **Option A** | 38-40 | 45 | 9 | 18-19 | 7-10 | 120 |
| **Option B** | 35-36 | 45 | 9-10 | 18-19 | 11-13 | 120 |

** Some courses (for example BIOL 120, BIOL 108, BIOL 110, CHEM 132) in the Bachelor of Science in Cybersecurity curriculum fulfill General Education requirements*

### (iii) Program Learning Outcomes (PLOs)

1. Demonstrate a strong understanding of computer science fundamentals, cybersecurity principles, and legal and ethical frameworks in cybersecurity.
2. Analyze complex computing problems and apply principles of computing and cybersecurity to identify effective solutions.
3. Detect, analyze, and respond to cybersecurity incidents using appropriate tools and techniques.
4. Conduct forensic analysis and apply secure software development practices to ensure the integrity and security of systems.
5. Manage and secure computer networks.
6. Design and implement secure architectures to mitigate vulnerabilities in Industrial Control Systems (ICS) and Internet of Things (IoT) ecosystems.
7. Communicate effectively in a variety of professional settings.

### (iv) Program Assessment Plan

The PLOs in the Cybersecurity program will be assessed by using five assessment instruments, including three multiple-choice assessment tests administered at the end of CS 215, CYB 340, and CS 408 respectively, and two design projects along with their presentations during CYB 411 and CYB 412, as shown in Table 6.

*Table 6 Program Assessment Plan*

| Course | Tools | PLOs assessed |
|---|---|---|
| CS 215 | Test | 1,2 |
| CYB 340 | Test | 1,2,3,4,5 |
| CYB 411 & CYB 412 | Project & presentation | 6,7 |
| CS 408 | Test<br>Project & presentation | 1,2,3,4,5<br>6,7 |

### (v) Program Identification

The Bachelor of Science in Cybersecurity is classified under the Computer and Information Systems Security/Auditing/Information Assurance category of the National Center for Educational Statistics (NECS), Classification of Instruction Programs (CIP) 11.1003. This category is defined as a "A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting."

## §133-11-5.2.3: COMPLIANCE WITH STANDARDS

### (i) Compliance with Academic Standards

The proposed program will comply with the academic standards outlined in 133 C.S.R. 10, Policy Regarding Program Review and Planning. The curriculum crafted to meet the highest standards of cybersecurity education, with ongoing assessments to ensure alignment with industry needs and technological advancements.
The requirements for admission to the Bachelor of Science in Cybersecurity program at West Virginia State University are the same as the minimum requirements for admission to the university and are stated on pages 22-25 of WVSU's Catalog for AY 2024-25. To maintain higher standards in the Bachelor of Science in Cybersecurity program, the students must pass certain key classes with a grade of at least C.

### (ii) Alignment with Industrial Standards

The proposed Bachelor of Science in Cybersecurity program is designed as a workforce-oriented program that equips students with the essential knowledge and skills to perform cybersecurity tasks across the 52 roles defined in the NICE Framework Version 1.0. This alignment ensures a standardized, industry-recognized structure for defining cybersecurity roles, competencies, and knowledge areas, positioning graduates for success in real-world cybersecurity careers.

The curriculum emphasizes the seven categories outlined in the NICE Framework: Oversee and Govern (OV), Design and Development (DD), Implementation and Operation (IO), Protect and Defend (PR), Investigate (IN), Cyberspace Intelligence (CI), Cyberspace Effects (CE). For detailed NICE work roles' descriptions, please refer to Appendix 2.


*Figure I: NICE* Framework *Work Role Categories (v.1.0.0)*

By integrating the NICE Framework, this program bridges the gap between academic preparation and workforce demands, ensuring students are well-prepared to meet the challenges of the modern cybersecurity landscape. It provides a solid foundation for graduates to excel in roles ranging from Incident Responders and Cyber Defense Analysts to Digital Forensics Experts and Cyber Policy Planners.

**(iii) Alignment with the NICE Framework Benefits:**

Industry Relevance: By structuring the curriculum around the NICE Framework, the program ensures graduates possess the precise skills and knowledge demanded by cybersecurity employers, enhancing their job readiness.

Clear Learning Objectives: The framework provides a consistent language for describing cybersecurity tasks and roles, enabling focused curriculum development and clear, measurable learning outcomes.

Career Path Guidance: Students can identify potential cybersecurity career paths based on their interests and skills, guided by the framework's structure of categories, specialty areas, and work roles.

Standardized Curriculum and Job Descriptions: Alignment with industry-recognized standards allows the program to deliver targeted education while supporting employers in defining precise job roles for graduates.

Workforce Development: The program fosters a pipeline of skilled cybersecurity professionals

equipped to address evolving cyber threats, strengthening workforce capacity across the sector.

Collaboration with Industry: The framework promotes synergy between academia and industry, ensuring curricula remain responsive to current and emerging cybersecurity challenges through continuous feedback.

**(iv) Key Benefits for Educators, Students and Employers:**

Educators create programs aligned with real-world jobs, fostering competency-based learning. Students gain standardized skills and knowledge that meet employer expectations, enabling seamless entry into the workforce.
Employers benefit from a larger pool of qualified candidates whose competencies align with organizational needs.

## §133-11-5.2.4: SIMILAR PROGRAMS IN WEST VIRGINIA:

The following institutions in West Virginia offer similar programs:

1. **Marshall University**:
    - **Cyber Forensics and Security**
      (NCES ID: 11.1003, approved in 08/2013)
    - **Computer and Information Security**
      (NCES ID: 11.9999, approved in 07/2018)
2. **West Virginia University**:
    - **Computer and Information Systems Security/Information**
      (NCES ID: 11.1003, approved in 06/2018)

3. **Concord University**:
    - **Computer and Information Systems Security/Auditing/Information**
      (NCES ID: 11.1003, approved in 06/2023)

For each of the four programs listed above, we provide a brief program focus and a comparison with WVSU's proposed Bachelor of Science in Cybersecurity (BSCyS) program. This comparison and the summary below will establish the unique features of the proposed BSCyS program.

## 1. Marshall University

- **Cyber Forensics and Security (NCES ID: 11.1003)**
    - Program Focus: This program emphasizes cyber forensics and security, preparing students to investigate cybercrimes and secure systems. The key differentiation is its forensics focus, training students in identifying and gathering evidence of cybercrimes.
    - Comparison: While the WVSU program also teaches cybercrime investigation, it places a broader emphasis on securing critical infrastructure, including SCADA systems, and addressing emerging sectors such as agriculture.
- **Computer and Information Security (NCES ID: 11.9999)**

- Program Focus: This more generalized cybersecurity program prepares students to secure information systems (without a specific industry focus).
- Comparison: The WVSU program differs by offering a more industry-specific focus on critical infrastructure (specifically the agriculture sector) and includes a cybersecurity clinic to provide hands-on experience in vulnerability assessments for community-serving entities.

## 2. West Virginia University (WVU)

- **Computer and Information Systems Security/Information (NCES ID: 11.1003)**
  - Program Focus: WVU's program provides a general approach to information systems security (without a significant focus on specific sectors or hands-on infrastructure protection).
  - Comparison: WVSU's program stands out with its specific concentration on critical infrastructure security, SCADA systems, and agriculture, coupled with the Cybersecurity Clinic for practical, real-world application.

## 3. Concord University

- **Computer and Information Systems Security/Auditing/Information (NCES ID: 11.1003)**
  - Program Focus: This program emphasizes auditing and information security with a particular focus on the financial or regulatory aspects of cybersecurity.
  - Comparison: WVSU's program, while covering similar areas such as policy drafting and risk management, sets itself apart by its focus on securing physical and agricultural infrastructure and its interdisciplinary approach linking fields like agriculture and criminal justice.

## Key Differentiators of the WVSU Program

- Focus on Critical Infrastructure: A core distinction is the emphasis on securing critical infrastructure, particularly SCADA systems (in power, chemical, water treatment plants, etc.) and agricultural infrastructure, which is largely absent in other programs.
- Cybersecurity in Agriculture: WVSU's program is uniquely positioned to address the cybersecurity challenges in the growing field of smart farming and precision agriculture, an area not explicitly covered by other programs.
- Interdisciplinary Approach: WVSU promotes cross-disciplinary collaboration, integrating cybersecurity with fields like information management systems and criminal justice.
- Cybersecurity Clinic: Beginning in 2025, WVSU will offer a Cybersecurity Clinic funded by Google, providing students with hands-on experience in vulnerability assessments and offering community stakeholders free evaluations of their infrastructure.
- IBM Partnership: As one of only 20 HBCUs with an IBM Cybersecurity Leadership Center, WVSU offers unique opportunities to its students to access cybersecurity curricula,

cybersecurity software, and multiple badge-earning courses free of cost. This partnership will enhance our proposed program's accessibility and industry alignment.

In summary, the new Bachelor of Science in Cybersecurity at WVSU occupies a distinct niche in West Virginia's cybersecurity education landscape. With its strong emphasis on the agriculture sector, the critical infrastructure security, hands-on lab training, and practical experience through the Cybersecurity Clinic, the program offers students unique opportunities to apply their skills in real-world settings. Strategic partnerships with USDA, IBM, and Google further distinguish WVSU's program from the more generalized offerings at Marshall, Concord, and WVU. A key differentiator is the focus on public-interest cybersecurity, particularly the protection of SCADA systems, alongside community engagement through vulnerability assessments. This prepares graduates to tackle specialized challenges in the cybersecurity field while aligning with WVSU's mission as a land-grant, HBCU institution serving diverse communities. Additionally, WVSU will collaborate with other state institutions to share resources and expertise, ensuring that the program complements, rather than duplicates, existing offerings in the state.

## §133-11-5.2.5.a: WORKFORCE NEED

As technological advancements accelerate and the digital landscape expands, cybersecurity has emerged as a critical concern for individuals, businesses, and governments. The rapid evolution of technology has significantly increased global interconnectedness, thereby amplifying the risk of cyber threats that challenge national security and economic stability. The United States faces a notable shortage of qualified cybersecurity professionals, underscoring the urgent need for an expanded and highly skilled workforce to address these evolving threats.

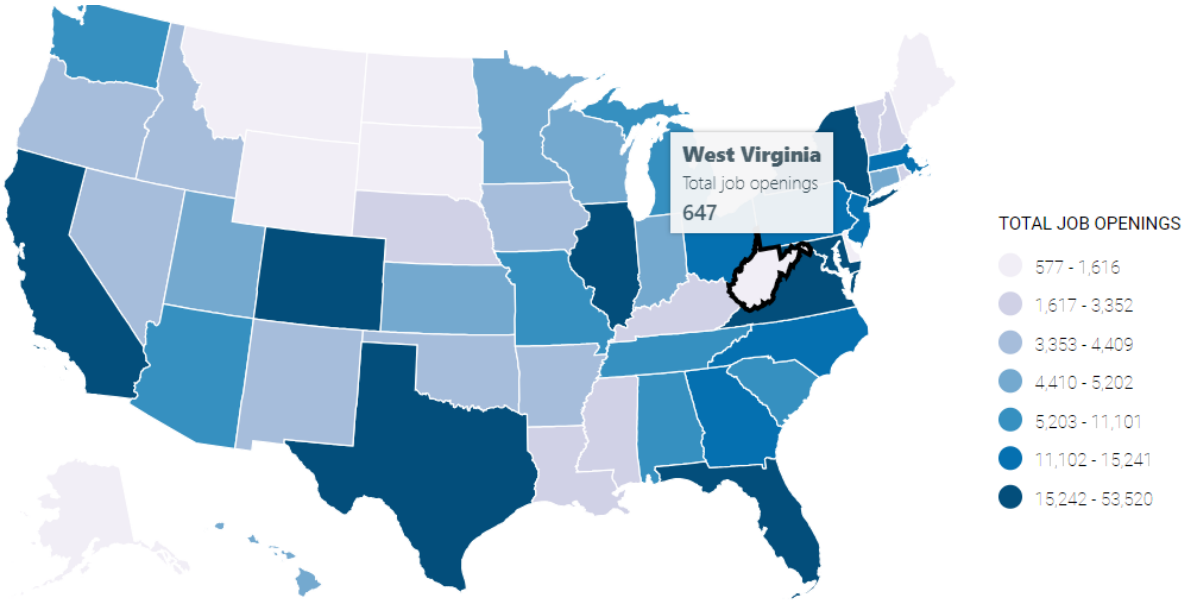
**Cybersecurity Expanding Workforce Demand and Growing Shortages**: According to the National Institute of Standards and Technology (NIST), there is a projected global deficit of nearly four million cybersecurity positions by 2024, highlighting a severe shortage within the United States [1]. The 2023 Cybersecurity Workforce Study by the International Information System Security Certification Consortium (ISC2) [2] has found that the global cybersecurity workforce need has reached record levels. As shown in Figure I, the global cybersecurity workforce has grown substantially, reaching a record 5.5 million in 2023, an increase of 8.7% over 2022.


Figure II: 2023 Global Cybersecurity Workforce Expansion from ISC2

However, this growth has not been sufficient to meet the soaring demand for cybersecurity professionals, which has widened the workforce gap. While workforce numbers continue to rise, the demand is expanding at a faster rate. For example, according to ISC2 research [2], in 2022, the gap was 3.4 million professionals, but this increased to 4 million by 2023. North America has an obvious demand with a workforce increase of 19.7% in 2023, but also faces a significant shortfall of 522,000 professionals, equating to an increased gap of 19.7% compared to the 2022 ISC2 Workforce Study as shown in Figure II.


Figure III 2023 Global Cybersecurity Workforce Gap from ISC2

Forbes [7] highlights that the U.S. accounts for a large share of the nearly 4 million unfilled cybersecurity positions globally, emphasizing the urgent need for skilled professionals to protect national infrastructure and businesses from cyber threats. The Cyberseek initiative (a collaboration between NIST's NICE program, CompTIA, and Lightfast) provides detailed, actionable insights into the U.S. cybersecurity job market. According to their 2024 data [9], talent shortages exist nationwide. Figure III, a heat map of job openings, offers a granular view of supply and demand for cybersecurity roles at state and metro levels, illustrating the workforce challenges and



opportunities. Notably, West Virginia currently has 647 open cybersecurity positions, reflecting the state's critical need for talent.

Figure IV: 2024 Cybersecurity Supply/Demand Heat Map from Cyberseek.org

**Economic Impact of Cybersecurity Threats**: The economic consequences of cybercrime are significant. Cybersecurity Ventures projects that cybercrime will cost the global economy $9.5 trillion in 2024, with an annual growth rate of 15% over the next two years, potentially reaching $10.5 trillion by 2025. This marks a substantial increase from $3 trillion in 2015. The article notes, *"If cybercrime were a country, it would be the world's third-largest economy, following the U.S. and China."* This substantial financial burden underscores the urgent need to enhance the cybersecurity workforce to safeguard both the U.S. economy and national security [3].

**Workforce Statistics and Analysis**: The Department of Labor's Official Cybersecurity Jobs Report [4] indicates a 94% increase in cybersecurity job postings over the past six years, reflecting a heightened demand for cybersecurity skills across multiple industries, including finance, healthcare, and government.

Furthermore, the Bureau of Labor Statistics through their Employment Projections program stated that employment for Information Security Analysts is projected to grow by an impressive 33% from 2023 to 2033, far outpacing the average growth across all occupations. This expansion represents approximately 17,300 job openings annually, driven not only by new positions but also by the replacement of retired workers or those transitioning to other fields.

As shown in Figure V, despite this critical demand, only 5% of U.S. universities offer cybersecurity programs [5], and many of these lack a workforce-oriented approach or fail to address specialized fields such as agricultural cybersecurity. The current academic landscape remains heavily focused on broader computer information technology majors, leaving a significant gap in the preparation of graduates for the specific challenges and opportunities within cybersecurity.

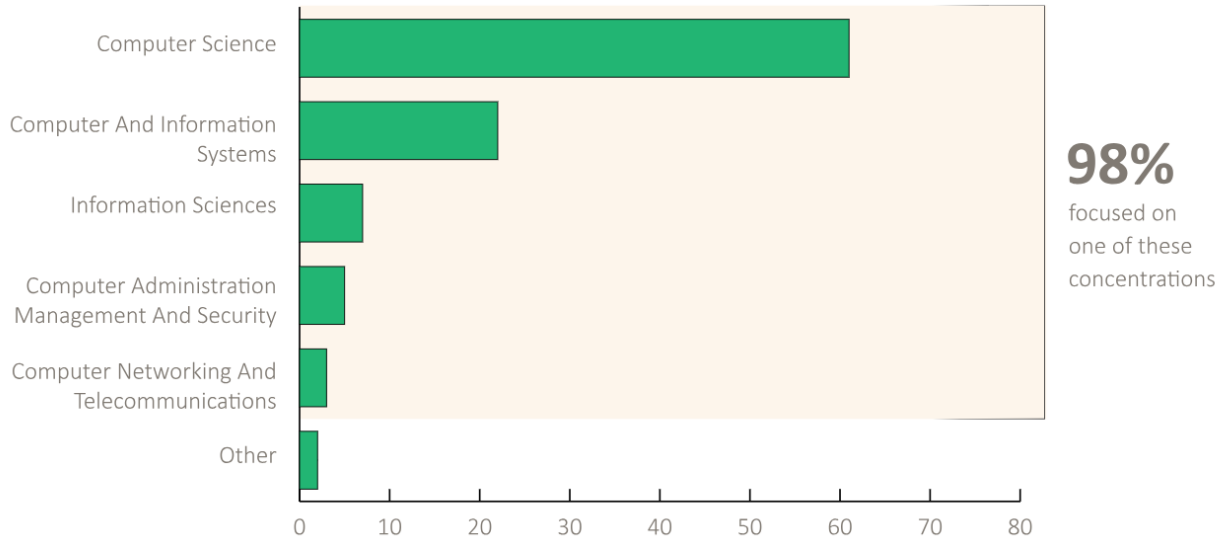



Figure V Computer and Information Technology Majors [5]

The ISC2 Cybersecurity Workforce Study in 2023 [6] corroborates this by emphasizing the need for a significant expansion of the U.S. cybersecurity workforce to address the rising demand and close the workforce gap to counteract increasing cyber threats.

The evidence provided demonstrates a critical and growing demand for cybersecurity professionals in the United States, driven by an evolving threat landscape and substantial economic risks associated with cybercrime. Addressing this workforce gap is vital for securing critical infrastructure and maintaining economic stability. Investments in education and training programs, such as those proposed by WVSU, are essential for developing the skilled professionals required to meet this growing demand. As cyber threats continue to evolve, the need for cybersecurity expertise will persistently increase [8], particularly within sectors critical to national infrastructure.

The increasing sophistication and frequency of cyber-attacks on U.S. critical infrastructure, as discussed in the recent article [7], further emphasize the urgency of expanding the cybersecurity workforce. This article highlights that many of these attacks are executed by foreign adversaries exploiting vulnerabilities, reinforcing the importance of a well-prepared cybersecurity workforce.

## **§133-11-5.2.5.b :** Student Interest Survey

A survey was conducted among 60 students from departments related to cybersecurity, including Computer Science, Criminal Justice, and Management Information Systems at WVSU. The results indicate a strong interest in the proposed Bachelor of Science in Cybersecurity program at our university, as detailed below:

**Question title:** Would you consider enrolling in a Bachelor of Science in Cybersecurity program if it were offered at our university?

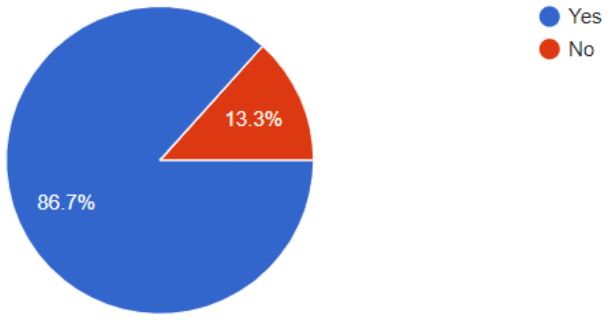



Figure VI First Question results

**Question title:** Do you believe that a degree in cybersecurity would enhance your job prospects in the current job market?

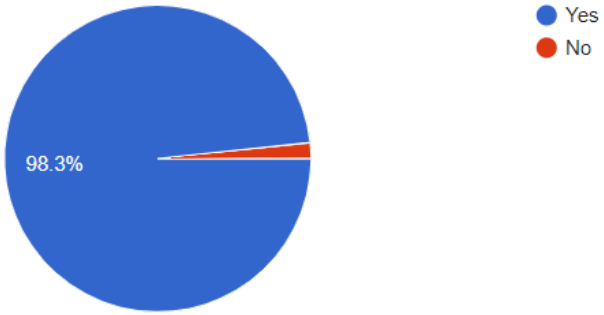



Figure VII Second Question Results

**Survey Results Analysis**

Interest in Enrollment: When asked if they would consider enrolling in the program, an overwhelming majority of 52 students (86.7%) responded positively, indicating a significant interest in pursuing this specialized degree. Only eight students (13.3%) expressed that they would not consider enrolling.

Perception of Job Market Benefits: The second question addressed the perceived value of a cybersecurity degree in enhancing job prospects. Here, an even greater consensus was observed, with 59 students (98.3%) agreeing that such a degree would improve their employment opportunities in the current job market. Only one student (1.7%) did not share this belief.

These results highlight a clear and substantial demand for the Bachelor of Science in Cybersecurity program, with the vast majority of respondents recognizing both the importance of cybersecurity skills and the potential career benefits associated with obtaining this degree. This strong student interest underscores the relevance and timeliness of introducing this program to meet the educational and professional needs of our students.

## §133-11-5.2.6: Financial Needs and Resources

### (i) Program enrollment projections and revenue

Table 7 provides the enrollment projections and the resulting tuition revenue for the program's first five years. We have used the current in-state full-time student tuition for all five years to calculate the tuition revenue projection.

Table 7 Enrollment Projections

| | AY 2025-26 | AY 2026-27 | AY 2027-28 | AY 2028-29 | AY 2029-30 |
|---|---|---|---|---|---|
| **Projected full-time majors** | 5 | 14 | 22 | 29 | 35 |
| **In-state tuition** | $8,930 | $8,930 | $8,930 | $8,930 | $8,930 |
| **Total Tuition** | **$44,650** | **$125,020** | **$196,460** | **$258,970** | **$312,550** |

### (ii) Faculty instructional requirements and cost

Table 8 provides instructional needs and staffing costs to deliver the program during the first five years. In the first year, we plan to hire an adjunct faculty to teach three courses (two 3-credit courses and one 1-credit course). In the subsequent years, the new and adjunct faculty (indicated in the table) will teach the new cybersecurity courses and any additional section(s) of the existing CS courses in the curriculum, as needed.

Table 8 Instructional Requirements and Cost

| | AY 2025-26 | AY 2026-27 | AY 2027-28 | AY 2028-29 | AY 2029-30 |
|---|---|---|---|---|---|
| **Full-time Faculty** | | 1 | 2 | 2 | 2 |
| **Adjunct Faculty** | 3 | 1 | 3 | 3 | 3 |
| | | | | | |
| **Full-time Faculty Cost** | $0 | $120,000 | $240,000 | $240,000 | $240,000 |
| **Adjunct Faculty Cost** | $4,900 | $2,100 | $5,600 | $5,600 | $5,600 |
| **Faculty Recruitment and support** | | $10,000 | $10,000 | | |
| **Total instructional Cost** | **$4,900** | **$132,100** | **$255,600** | **$245,600** | **$245,600** |

The two full-time faculty we will hire for the program will have a PhD in Computer Science or Cybersecurity related area and will be hired as tenure-track assistant professors.

### (iii) Final Revenue-Cost analysis

WVSU has secured a $1M grant from Google. The grant provides support for a new faculty

member ($100,000 per year for three years) to teach and train (run Google Clinics) and hence prepare a skilled workforce to protect critical infrastructures' security. This grant will supplement the cost of hiring the new instructional faculty for the proposed cybersecurity program at WVSU. Incorporating this support from the Google grant as "revenue" for the program, Table 9 provides the comprehensive revenue of the B.S. in cybersecurity program at WVSU.

Table 9 Comprehensive Program Revenue

| | AY 2025-26 | AY 2026-27 | AY 2027-28 | AY 2028-29 | AY 2029-30 |
|---|---|---|---|---|---|
| **Full-time majors** | 5 | 14 | 22 | 29 | 35 |
| **In-state tuition** | $8,930 | $8,930 | $8,930 | $8,930 | $8,930 |
| **Tuition revenue** | $44,650 | $125,020 | $196,460 | $258,970 | $312,550 |
| **Google Grant support** | | $100,000 | $100,000 | $100,000 | |
| **Total Revenue** | **$44,650** | **$225,020** | **$296,460** | **$358,970** | **$321,550** |

Table 10 comprehensive Program Instructional Cost

| | AY 2025-26 | AY 2026-27 | AY 2027-28 | AY 2028-29 | AY 2029-30 |
|---|---|---|---|---|---|
| **Full-time Faculty** | | 1 | 2 | 2 | 2 |
| **Adjunct Faculty** | 3 | 1 | 3 | 3 | 3 |
| **FT Fac. Cost** | $0 | $120,000 | $240,000 | $240,000 | $240,000 |
| **Adj. Fac. Cost** | $4,900 | $2,100 | $5,600 | $5,600 | $5,600 |
| **Faculty recruitment & support** | | $10,000 | $10,000 | | |
| **Total Cost** | **$4,900** | **$132,100** | **$255,600** | **$245,600** | **$245,600** |

As Table 9 and 10 shows, the projected revenue exceeds the expected program cost for each of the first five years.

WVSU has secured grants totaling approximately $3M for teaching, research, training, and workforce development from the Kanawha County Commission, Department of Education, and Google. We plan to continue securing additional grants for these purposes as well as equipment update needs. All of the current labs are equipped with new equipment.

## §133-11-5.2.7: Instructional Delivery Methodologies

The program will be delivered primarily on-site at WVSU, utilizing the Cybersecurity labs and CyberHive for practical, hands-on training. Additionally, some courses may be offered online or in hybrid formats to accommodate different learning preferences and increase accessibility to the program as below:

1. **Hybrid Learning Model**: The program will utilize a blended learning approach that combines traditional in-person classroom instruction with online coursework. This allows

students flexibility while maintaining access to hands-on learning experiences in WVSU's state-of-the-art cybersecurity labs.

2. **Hands-On Lab-Based Instruction**: Practical learning will be a cornerstone of the program. Students will spend a significant portion of their time in WVSU's CyberHive lab and the physical SCADA learning system, where they will gain hands-on experience securing critical infrastructure. This experiential learning will enable students to simulate real-world cyber threats and defenses in controlled environments.

3. **Project-Based Learning (PBL)**: PBL will immerse students in real-world cybersecurity challenges. Students will be tasked with working in teams to solve complex security problems, including conducting vulnerability assessments and developing security protocols for critical infrastructure systems. Projects will be integrated into the curriculum to simulate industry conditions.

4. **Cybersecurity Clinic Participation**: Students will actively participate in the University's Cybersecurity Clinic**,** funded by a $1 million grant from Google. The clinic will offer students opportunities to engage in real-world cybersecurity tasks, such as conducting Cyberattack Vulnerability Assessments on critical public infrastructure. This practical experience will be invaluable for understanding real-time threat environments.

5. **Scenario-Based Simulations**: Leveraging WVSU's cybersecurity labs, students will engage in scenario-based simulations that model cyberattacks on infrastructure systems like power grids, and water treatment plants. These high-fidelity simulations will prepare students for handling real-world incidents.

6. **Research and Critical Infrastructure Security Projects**: Students will be encouraged to participate in research initiatives focusing on cybersecurity for critical infrastructure. These research projects will offer deep dives into topics such as threat analysis, cyber resilience, and the protection of critical systems.

7. **Capstone Project**: The program will culminate in a capstone project where students will design and implement a cybersecurity solution for a simulated or real-world infrastructure system. The capstone will integrate knowledge from across the program and emphasize practical, innovative solutions to cybersecurity challenges.

These methodologies will ensure that students in WVSU's proposed Bachelor of Science in Cybersecurity program are not only well-versed in theory but are equipped with the hands-on experience and critical thinking skills needed to tackle the complex cybersecurity challenges of today and tomorrow.

# REFERENCES


[1] NIST, "Cybersecurity Workforce Demand," The National Institute of Standards and Technology, 2023.

[2] ISC2, "ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap," *The International Information System Security Certification Consortium,,* 2023.

[3] Steve Morgan, Sausalito, Calif, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine,* 2020.

[4] DOL, "Information-Security-Analysts," Occupational Outlook Handbook, 2024.

[5] Bureau of Labor Statistics-U.S. Department of Labor, "Occupational Outlook Handbook, Information Security Analysts," 2023. [Online]. Available: https://www.bls.gov/ooh/field-of-degree/computer-and-information/computer-and-information-technology-field-of-degree.htm.

[6] T. I. I. S. S. C. Consortium, "Cybersecurity_Workforce_Study," ISC2, Virginia, 2023.

[7] P. Mwangi, "Cybersecurity Threats and National Security in the Digital Age," *American Journal of International Relations,* no. Vol. 9 No. 1 (2024), 2024.

[8] S. D. N. P. Akshay Joshi, "Global Cybersecurity Outlook 2023," *Global Cybersecurity Outlook 2023,* 2023.

[9] C. Organization, "USA Cybersecurity Supply/Demand Heat Map," Cyberseek , 2024.

[10] Jack Kelly, "Nearly 4 Million Cybersecurity Jobs Are Vacant: Here's Why You Should Consider Breaking Into This Sector," *Forbes,* 2024.

# APPENDIX 1
## Courses Description

CYB 101 Cybersecurity Fundamentals (3 credits)

Fundamentals of data security, system security, network security, personal security, societal security, risk management, and adversarial thinking. The global security landscape, including cyber law and warfare. Prerequisite(s): Eligible for Math 120.

CYB 201 Cybersecurity Law and Ethics (3 credits)

Cybersecurity policies and ethics; state, federal, and international laws regarding cybercrime and cybersecurity; legal frameworks, relationship between law and technology. Prerequisite(s): C or better in CYB 101; ENGL 101.

CYB 317 Cyber Incident Response (3 credits)

Cybersecurity operations with a focus on cybersecurity incident frameworks including contingency planning, emergency downtime minimizing, incident response and recovery techniques and tools like Security Information and Event Management (SIEM) systems, and case study analyses. Prerequisite(s): C or better in CS 316.

CYB 340 Network Security (3 credits)

Essential security principles for securing network infrastructure, including cryptography, secure access management, firewalls, VPNs, intrusion prevention and detection systems, and endpoint security. Topics span securing LANs and routers, implementing Authentication, Authorization, and Accounting (AAA) and secure protocols, and defending against modern threats. Prerequisite(s): C or better in CS 240.

CYB 360 AI and Machine Learning in Cyber Defense (3 credits)

Generative AI and large language models (LLMs) such as ChatGPT, hands-on experience in applying machine learning algorithms and their APIs to address threats through incident response, threat intelligence, and penetration testing. Utilize AI technologies such as, Microsoft Security CoPilot and Google Cloud Security AI Workbench and Colab to develop machine learning models, analyze real-world datasets. Prerequisites: CS 250, CS 116 or 336.

CYB 409 Secure Software Development (3 credits)

Secure Software design, implementation and testing, risk assessments, secure coding techniques in various programming languages to avoid vulnerabilities, threat modeling, malware analysis, Crypto, secure APIs, secure web and mobile application requirements and architecture. Prerequisite(s): C or better in CS 250; C or better in CS 336.

CYB 411 Industrial Control Systems Cybersecurity (3 credits)

Cybersecurity of ICS in the critical infrastructure through practical scenarios using CyberHive SCADA system, secure ICS architecture, PLC and HMI programming, Modbus & ENIP/CIP protocols, OT and IT, ICS networks scanning, manipulating, and securing from adversary TTPs. Prerequisite(s): C or better in CS 316

CYB 412 IoT Security (3 credits)

Basic concepts and applications of IoT architecture and technology, IoT attacks and threats such as Sybil attacks and malware propagation, IoT data security and authentication, controllers hardware and software security, IoT network security, wireless protocols, wireless sensors, device discovery, firmware analysis, vulnerability assessment, and best practices for securing IoT environments. Prerequisite(s): C or better in CYB 340.

CS 101. Programming Fundamentals (3 credits)

The fundamental concepts of programming using C. Historical and social context of computing and an overview of computer science as a discipline. Prerequisite(s): Eligibility for MATH 120.

CS 102. The Object-Oriented Paradigm (3 credits)

The fundamental concepts of object-oriented programming using languages such as C++, JAVA, or another object-oriented programming language of the instructor’s choice. Prerequisite(s): C or better in CS 101.

CS 215 - Introduction to Unix/Linux Systems (3 credits)

POSIX file system and directory structure, Linux administration, user authentication and permissions, basic network configuration, shell programming, virtual machines, high performance computing, cloud environments. Prerequisite(s): CS 101 or CS 116.

CS 230. Database Management Systems (3 credits)

This course presents the history of database management systems, the logical and physical structures of several current models, and deals in a practical, experiential way with the design of databases and the management systems that control them. Prerequisite(s): CS 102.

CS 240. Data Communications and Networking (3 credits)

An introduction to the theories, terminology, equipment and distribution media associated with data communications and networking. Prerequisite(s): CS 101.

CS 250. Data Structures and Algorithms (3 credits)

An introduction to the implementation and use of abstract data types including dynamic arrays, linked lists, stack, queues, three hash tables and heaps as well as algorithms that operate on these structures with a preliminary study of algorithmic complexity. Prerequisite(s): CS 102 and Math 205

CS 316. Cybersecurity Principles and Practice (3 credits)

Diagnostic software utilities, advanced network packet analysis, firewalls, intrusion detection rules, forensic investigation, penetration testing, human factors in cybersecurity. Prerequisite(s): CS 215 and CS 240.

CS 336. Scripting Languages (3 credits)

Shell scripts and batch files, programming using interpreted languages such as PERL, Python, PHP, JavaScript or VBScript for automation of system administration tasks and web programming. Prerequisite(s): CS 102

CS 408. Senior Seminar (2 credit hours)

Integrates the work completed in the various courses. Reading and research oriented. (To be taken in one of the last two semesters prior to graduation.)

CS 410. Systems Administration (3 credits)

Maintenance of a multi-user computer system, managing services, managing users, managing data, file systems, networking and security. Prerequisite(s): CS 240 and CS 336

CS 416. Computer Forensics and Penetration Assessment (3 credits)

Digital investigations, data and file recovery methods, digital forensics, data acquisition, virtual machines, networks, mobile devices, cloud forensics. Prerequisite(s): CS 316

MATH 120. College Algebra (3 credits)

Equations and inequalities, functions, systems of equations and inequalities, graphing, rational expressions, radical expressions, and applications of the above. Prerequisite(s): MATH 119 or ACT MATH 21+ or equivalent

MATH 205. Discrete Mathematics (3 credits)

The basic non-calculus mathematics for computer science in the areas of algebra, logic, combinations and graph theory. Prerequisite(s): MATH 120 and CS 101

MATH 305 Introduction to Cryptography (3 credits)

An introduction to modern cryptographic principles essential for digital security, including encryption, authentication, hash functions, and secure communication. large numbers, random number generation, secure key exchange, and digital signatures. Practical applications address password protection, data privacy, and anonymous transactions, with emphasis on analyzing algorithms, identifying vulnerabilities, and implementing secure protocols in real-world contexts. Prerequisite(s): MATH 205.

AFNR 101 – Introduction to Agriculture, Food and Natural Resources (3 credits)

This introductory survey course investigates and analyzes agriculture, food and natural resources in the context of the environment, public health and social justice. We primarily focus on the American agricultural systems but will explore some global systems as well. The biological, environmental, economic, cultural, social and ethical dimension of our agriculture systems—from farm to plate—are considered. We will look at some of the challenges faced in order to feed a growing world population, anticipated in exceeding 9 billion people by 2050. These challenges include risks from climate change, soil degradation and water shortages, pest pressure, dwindling diversity of genetic resources, increasing energy demands as well as controversies over adopting technologies and balancing the triple-bottom line, social justice and ethical considerations. We will consider whether, and how, agricultural production, food systems and maintaining our natural resources can be done in an environmentally friendly and sustainable way, and consider whether consumers can play a role through the choices they make.

PHYS 352: Geographic Information System (3 credits)
This course introduces students to Geographic Information Systems (GIS), specifically ESRI ArcGIS. The course creates a foundation for using GIS in a variety of settings focusing on spatial analysis, cartography and some data management. Over the course of the semester, students do exercises in class and complete a final project to develop their GIS skills.

PHYS 217. Electronics and Microcontrollers Laboratories (2 credit hours)

The course offers an introduction and hands-on experience with microcontrollers and electric circuits. Students will learn how to use microcontrollers, connect and design simple electric circuits to control a variety of sensors with a microcontroller. Prerequisite: Permission of the instructor.

# APPENDIX 2
## NICE Framework Categories and Roles

**Oversee and Govern (OV)**

| | |
|---|---|
| Cybersecurity Policy and Planning | Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. |
| Cybersecurity Curriculum Development | Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, or education content, methods, and techniques based on instructional needs and requirements. |
| Cybersecurity Instruction | Responsible for developing and conducting cybersecurity awareness, training, or education. |
| Cybersecurity Legal Advice | Responsible for providing cybersecurity legal advice and recommendations, including monitoring related legislation and regulations. |
| Privacy Compliance | Responsible for developing and overseeing an organization's privacy compliance program and staff, including establishing and managing privacy-related governance, policy, and incident response needs. |
| Product Support Management | Responsible for planning, estimating costs, budgeting, developing, implementing, and managing product support strategies in order to field and maintain the readiness and operational capability of systems and components. |
| Secure Project Management | Responsible for overseeing and directly managing technology projects. Ensures cybersecurity is built into projects to protect the organization's critical infrastructure and assets, reduce risk, and meet organizational goals. Tracks and communicates project status and demonstrates project value to the organization. |
| Security Control Assessment | Responsible for conducting independent comprehensive assessments of management, operational, and technical security controls and control enhancements employed within or inherited by a system to determine their overall effectiveness. |
| Systems Authorization | Responsible for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the nation. |

| | |
|---|---|
| Technology Program Auditing | Responsible for conducting evaluations of technology programs or their individual components to determine compliance with published standards. |

**Design and Development (DD)**

| | |
|---|---|
| Cybersecurity Architecture | Responsible for ensuring that security requirements are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes. |
| Enterprise Architecture | Responsible for developing and maintaining business, systems, and information processes to support enterprise mission needs. Develops technology rules and requirements that describe baseline and target architectures. |
| Secure Software Development | Responsible for developing, creating, modifying, and maintaining computer applications, software, or specialized utility programs. |
| Secure Systems Development | Responsible for the secure design, development, and testing of systems and the evaluation of system security throughout the systems development life cycle. |
| Software Security Assessment | Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs and delivering actionable results. |
| Systems Requirements Planning | Responsible for consulting with internal and external customers to evaluate and translate functional requirements and integrating security policies into technical solutions. |
| Systems Testing and Evaluation | Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings. |
| Technology Research and Development | Responsible for conducting software and systems engineering and software systems research to develop new capabilities with fully integrated cybersecurity. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems. |

**Implementation and Operation (IO)**

| | |
|---|---|
| Data Analysis | Responsible for analyzing data from multiple disparate sources to provide cybersecurity and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. |
| Database Administration | Responsible for administering databases and data management systems that allow for the secure storage, query, protection, and utilization of data. |
| Knowledge Management | Responsible for managing and administering processes and tools to identify, document, and access an organization's intellectual capital. |
| Network Operations | Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments. |
| Systems Administration | Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation. |
| Systems Security Analysis | Responsible for developing and analyzing the integration, testing, operations, and maintenance of systems security. Prepares, performs, and manages the security aspects of implementing and operating a system. |
| Technical Support | Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes. |

**Protect and Defend (PR)**

| | |
|---|---|
| Defensive Cybersecurity | Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks. |
| Digital Forensics | Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation. |
| Incident Response | Responsible for investigating, analyzing, and responding to network cybersecurity incidents. |
| Infrastructure Support | Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity. |
| Insider Threat Analysis | Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. |
| Threat Analysis | Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment. |
| Vulnerability Analysis | Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities. |

**Investigate (IN)**

| | |
|---|---|
| Cybercrime Investigation | Responsible for investigating cyberspace intrusion incidents and crimes. Applies tactics, techniques, and procedures for a full range of investigative tools and processes and appropriately balances the benefits of prosecution versus intelligence gathering. |

| | |
|---|---|
| Digital Evidence Analysis | Responsible for identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical and investigative techniques. |

**Cyberspace Intelligence (CI)**

| | |
|---|---|
| All-Source Analysis | Responsible for analyzing data and information from one or multiple sources to conduct preparation of the operational environment, respond to requests for information, and submit intelligence collection and production requirements in support of intelligence planning and operations. |
| All-Source Collection Management | Responsible for identifying intelligence collection authorities and environment; incorporating priority information requirements into intelligence collection management; and developing concepts to meet leadership's intent. Determines capabilities of available intelligence collection assets; constructs and disseminates intelligence collection plans; and monitors execution of intelligence collection tasks to ensure effective execution of collection plans. |
| All-Source Collection Requirements Management | Responsible for evaluating intelligence collection operations and developing effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of intelligence collection requirements. Evaluates performance of intelligence collection assets and operations. |
| Cyber Intelligence Planning | Responsible for developing intelligence plans to satisfy cyber operation requirements. Identifies, validates, and levies requirements for intelligence collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace. |
| Multi-Disciplined Language Analysis | Responsible for applying language and cultural expertise with target, threat, and technical knowledge to process, analyze, and disseminate intelligence information derived from lanugage, voice, and/or graphic materials. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter experise in foreign language-intensive or interdisciplinary projects. |

**Cyberspace Effects (CE)**

| | |
|---|---|
| Cyberspace Operations | Responsible for gathering evidence on criminal or foreign intelligence entities to mitigate and protect against possible or real-time threats. Conducts collection, processing, and geolocation of systems to exploit, locate, and track targets. Performs network navigation and tactical forensic analysis and executes on-net operations when directed. |
| Cyber Operations Planning | Responsible for developing cybersecurity operations plans; participating in targeting selection, validation, and synchronization; and enabling integration during the execution of cyber actions. |
| Exploitation Analysis | Responsible for identifying access and intelligence collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks. |
| Mission Assessment | Responsible for developing assessment plans and performance measures; conducting strategic and operational effectiveness assessments for cyber events; determining whether systems perform as expected; and providing input to the determination of operational effectiveness. |
| Partner Integration Planning | Responsible for advancing cooperation across organizaitonal or national borders betwen cyber operations partners. Provides guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions. |
| Target Analysis | Responsible for conducting target development at the system, component, and entity levels. Builds and maintains electronic target folders to include inputs from environment preparation and/or internal or external intelligence sources. Coordinates with partner target working groups and intelligence community members, and presents candidate targets for vetting and validation. Assesses and reports on damage resulting from the application of military force and coordinates federal support as required. |

| | |
|---|---|
| Target Network Analysis | Responsible for conducting advanced analysis of collection and open-source data to ensure target continuity; profiling targets and their activities; and developing techniques to gain target information. Determines how targets communicate, move, operate, and live based on knowledge of target technologies, digital networks, and applications. |