Cybersecurity and Information Assurance Program Plan

The cybersecurity program is rigorous and offers a comprehensive coverage of fundamental technical and non-technical concepts, including cybersecurity policy, software assurance, network defense, and programming including scripting. The curriculum prepares learners to identify key business assets, associated threats and vulnerabilities, identify security controls and defense tools, methods, and components. Students are required to demonstrate the conceptual and practical aspects of Cybersecurity. Additionally, successful students will receive four CompTIA certifications as part of the curriculum. Providing these certifications to the students as part of the curriculum makes WGU unique.

PROGRAM LEARNING OUTCOMES:
1)   The graduate will be able to evaluate security of a given system design according to defined security goals.
2)   The graduate will be able to mitigate security concerns related to network, cellular, mand wireless technologies.
3)   The graduate will be able to evaluate the effectiveness of an organization's cyber operations to protect and preserve data.
4)   The graduate will be able to conduct digital forensics as part of an incident response plan.

4. **USNCC NAVAL STUDIES CERTIFICATE PROGRAM PLAN (15 CREDITS):**

The five Naval Studies certificate courses satisfy the WGU GenEd requirements for Critical Thinking and Logic 3CU, Introduction to Geography 3CU, American Politics and the US Constitution 3CU, Introduction to Communication 3CU, and Ethics in Technology 3CU.

5. **WGU General Education Areas (21 Credits: 15 Naval Studes, 6 WGU GenEd):**

Required Gen Ed Course   **Credits**

6. **WGU Certificate Course Descriptions & Learning Outcomes:**

   a. **Introduction to IT**

   ███

   are presented with various IT disciplines including systems and services, network and security, scripting and programming, data management, and business of IT, with a survey of technologies in every area and how they relate to each other and to the business.

The graduate defines security principles and cyber defense concepts to support security practices within an organization.

The graduate identifies how security principles and cyber defense concepts impact organizational policies and practices.

The graduate identifies security principles and cyber defense concepts that have been violated in common security failures.

The graduate identifies security principles and cyber defense concepts to protect an organization's assets.

The graduate identifies how confidentiality, integrity, and availability define security requirements for an organization.

The graduate identifies guidelines in privacy and compliance as applied to cybersecurity.

c. Web Development Foundations

This course introduces students to web design and development by presenting them with HTML5 and Cascading Style Sheets (CSS), the foundational languages of the web, by reviewing media strategies and by using tools and techniques commonly employed in web development.
This course covers the following competencies:

The graduate creates web pages using a graphic user interface (GUI) editor as well as basic HTML5 and CSS 3 elements.

The graduate develops a plan for creating and maintaining a website that addresses specific business needs while maintaining industry and ethical standards.

d. Network and Security   Foundations

Network and Security - Foundations introduces students to the components of a computer network and the concept and role of communication protocols. The course covers widely used categorical classifications of networks (e.g., LAN, MAN, WAN,WLAN, PAN, SAN, CAN, and VPN) as well as network topologies, physical devices, and layered abstraction. The course also introduces students to basic concepts of security, covering vulnerabilities of networks and mitigation techniques, security of physical media, and security policies and procedures.
This course covers the following competencies:

Begin your course by discussing your course planning tool report with your instructor and creating your personalized course plan together.

The graduate identifies fundamental networking concepts to support an organization.

The graduate identifies the fundamentals of network security concepts to support an organization.

The graduate determines appropriate network security operations to protect an organization's assets.

e. Digital Forensics in Cybersecurity

Digital forensics, the science of investigating cybercrimes, seeks evidence that reveals who, what, when, where, and how threats compromise information. This course examines the relationships between incident categories, evidence handling, and incident management. Students identify consequences associated with cyber threats and security laws using a variety of tools to recognize and recover from unauthorized, malicious activities.

This course covers the following competencies:

The graduate identifies types of digital evidence, digital evidence examination rules, and digital evidence consideration by crime category.

The graduate describes digital forensics procedures from the initial recognition of an incident through the steps of evidence gathering, preservation, analysis, and through the completion of legal proceedings.

The graduate identifies laws, rules, policies, and procedures that affect digital forensics.

The graduate conducts analysis on gathered evidence using forensic cyber tools to determine the nature of a security breach.

The graduate executes recovery procedures for deleted data.

The graduate identifies steganography and its techniques as it relates to concealed data.

The graduate identifies common methods and concepts for password cracking, email tracking, file logging, and mobile forensics.

f. Scripting and Programming Foundations

Scripting and Programming - Foundations provides an introduction to programming, covering basic elements such as variables, data types, flow control, and design concepts. The course is language-agnostic in nature, ending in a survey of languages and introduces the distinction between interpreted and compiled languages. This course covers the following competencies:

The graduate examines basic computer programming elements, including data types, constants, variables, operators, and expressions.

The graduate determines how to achieve programming goals through functions and control structure.

The graduate interprets algorithms.

The graduate describes steps of the software design process.

The graduate compares various scripting and programming languages.

The non-certificate course descriptions and competencies are:

a. IT Foundations

IT Foundations is the first course in a two-part series that will prepare you for the CompTIA A+ exam, Part I. This course focuses mostly on hardware and will afford you the skills you need to support five core components: Mobile Devices; Networking; Hardware; Virtualization and Cloud Computing; and Network and Hardware Troubleshooting. These are essential skills to set up and troubleshoot any system. Whether you work in a data center or an office, most of your work as an IT professional will execute in a hardware platform; understanding the hardware layer of the IT infrastructure will allow you to work more efficiently,

provide solutions for business requirements, and be a key contributor in your company. This course covers the following competencies:

‹ The graduate configures client-side virtualization to meet organizational requirements.
‹ The graduate determines appropriate diagnostic and repair strategies for common personal computer hardware, access to network resources, and network connectivity.
‹ The graduate recommends appropriate strategies for classifying, installing, configuring, optimizing, upgrading, and troubleshooting laptops and mobile devices.
‹ The graduate recommends appropriate strategies for classifying, installing, configuring, optimizing, and upgrading basic network types.
‹ The graduate demonstrates an understanding of personal computer components and their function in a desktop system.

b. IT Applications

IT Applications provides students with an understanding of personal computer components and their functions in a desktop system. Also covered is computer data storage and retrieval including classifying, installing, configuring, optimizing, upgrading, and troubleshooting printers, laptops, portable devices, operating systems, networks, and system security. Other areas include recommending appropriate tools, diagnostic procedures, preventative maintenance, and troubleshooting techniques for personal computer components in a desktop system. The course then finishes with strategies for identifying, preventing, and reporting safety hazards and environmental/human accidents in a technological environment, and effective communication with colleagues and clients as well as job-related professional behavior. This course is designed to build the skills to support 4 core components: Operating Systems, Security, Software Troubleshooting, and Operational Procedures. These are core competencies for IT professionals from cloud engineers to data analysts, and will empower you with a better understanding of the tools used during your career. This course covers the following competencies:

‹ The graduate determines appropriate tools, diagnostic procedures, preventive maintenance, security, malware removal, and troubleshooting techniques for common personal computer and mobile operating systems (mobile and personal computer) and applications.
‹ The graduate determines appropriate strategies to implement documentation, change management and disaster recovery, and explain common safety, environmental concerns; explain addressing prohibited content; use professional communication techniques.
‹ The graduate determines appropriate strategies for classifying, installing, configuring, optimizing, upgrading, and troubleshooting computer operating systems.
‹ The graduate determines appropriate strategies for classifying, controlling

should be completed prior to beginning Networks, C480. This course covers the following competencies:

‹ The graduate configures basic networking components to support an organization's operations.
‹ The graduate manages a network infrastructure to support an organization's operations.
‹ The graduate manages networks to support an organization's operations.
‹ The graduate troubleshoots network issues in support of an organization's operations.
‹ The graduate manages network security to protect an organization.

d. Composition: Writing with a Strategy
Composition: Writing with a Strategy introduces candidates to the types of writing and thinking that are valued in college and beyond. Candidates will practice writing in several genres with emphasis placed on writing and revising academic arguments. Instruction and exercises in grammar, mechanics, research documentation, and style are paired with each module so that writers can practice these skills as necessary. Composition: Writing with a Strategy is a foundational course designed to help candidates prepare for success at the college level. There are no prerequisites for Composition: Writing with a Strategy. This course covers the following competencies: • The graduate applies appropriate grammatical rules, sentence structure, and writing conventions. • The graduate selects appropriate rhetorical strategies that improve writing and argumentation. • The graduate appropriately uses a given writing style. • The graduate uses appropriate writing and revision strategies. • The graduate integrates credible and relevant sources into written arguments. • The graduate composes an appropriate narrative for a given con.t   ive(n

computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students learn how to leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, effectively respond to and recover from incidents handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling. This course prepares students for the CompTIA Cybersecurity Analyst (CySA+) certification exam.

USNCC NAV course sequence, or any questions you might have related to