The following programs are available in residence and hybrid. Students using the VA Benefits can only be used for residence program. They may be taken in order as a program or individual courses depending on your prior knowledge and career goals. We encourage you to read through each course and see which resonates with your personality and career goals. Every class session promotes active participation, encouraging both faculty and students to engage in questions and answers throughout the entire duration.

CYBER SECURITY CAREER

With a Cyber Security Career, the student gains the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments. The student will apply critical thinking and judgment across a broad spectrum of security disciplines. Learn to propose and implement sustainable security solutions that map to organizational strategies. As a student you will learn to translate business needs into security requirements, analyze risk impact and the response to security incidents. The program is tailored for students to take additional certifications. (i.e.) Microsoft, Cisco, CompTIA and more. Upon successful completion of the program, you will be awarded a certificate.

RISK MANAGEMENT FRAMEWORK PROGRAM

Course Number: RMF 101	Course Title	Clock Hours
	Risk Management Framework	120

INTRODUCTION TO CYBER SECURITY - RMF 101

This course will provide an in-depth and relatable form of job instruction training that is solely based on the Risk Management Framework (RMF). The training includes in-class hands-on exercises and take-home assignments that will demonstrate the process for identifying, implementing, assessing, and authorizing information systems. The training is industry-driven, meaning, training will **only** cover process steps as identified in the RMF, and an employers' expectation of the compliance professional.

Upon completing the training, trainees will be able to:

- Understand the basics of Network Security and System Environment.
- Understand FISMA/FedRAMP
- Explain the RMF steps and processes
- Perform Information System Security Officer (ISSO) responsibilities
- Assessor responsibilities

UPON SUCCESSFUL COMPLETION OF THE PROGRAM, YOU WILL BE AWARDED A CERTIFICATE.

ADVANCED SECURITY PRACTITIONER (CASP) CERTIFICATION

Course Number CIS 203	Course Title	Clock Hours
	CASP	40

ADVANCED SECURITY PRACTITIONER (CASP) CERTIFICATION CIS 203

The MDTS Advanced Security Practitioner (CASP) Certification is a vendor-neutral credential. The CASP exam is an internationally targeted validation of advanced-level security skills and knowledge. While there is no required prerequisite, the CASP certification is intended to follow the MDTS Security+ or equivalent experience and has a technical, "hands-on" focus at the enterprise level.

The CASP Course will certify that the candidate has the technical knowledge and skills required to conceptualize, engineer, integrate and implement secure solutions across complex environments. The candidate will apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies, translate business needs into security requirements, analyzes risk impact and respond to security incidents. Upon successful completion of the program, you will be awarded a certificate.

SECURITY PLUS CERTIFICATION (Security +)

Course Number: CIS 202 Security+	Course Title	Clock Hours
	Security+	40

SECURITY+ CIS 202

The MDTS Security+ Certification is a vendor neutral credential. The Security+ exam is an internationally recognized validation of foundation-level security skills and knowledge and is used by organizations and security professionals around the globe. The CompTIA Security+ exam will certify that the successful candidate has the knowledge and skills required to identify risk, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, the successful candidate will apply security controls to maintain confidentiality, integrity, and availability, identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of applicable policies, laws, and regulations. Upon successful completion of the program, you will be awarded a certificate.

CYBERSECURITY FUNDAMENTALS

Course Number: CIS 101	Course Title	Clock Hours
	Cybersecurity Fundamentals	20

INTRODUCTION TO CYBER SECURITY – CIS 101 Cybersecurity Fundamentals

In this course students will examine the core concepts and terminology of cyber security and information assurance, integrating the importance of user involvement and vulnerability management. Moreover, analyzing network architecture, threats, and organization security posture in respects to private and DoD (Department of Defense) standards. Upon completion students will establish an intermediate understanding in preparation for industry certifications. Upon successful completion of the program, you will be awarded a certificate. Upon successful completion of the program, you will be awarded a certificate.

CYBERSECURITY TECHNICAL IMPLEMENTATION GUIDE (STIGs)

Course Number: STI 101	Course Title	Clock Hours
	STI 101 STIGs	20

INTRODUCTION TO CYBER SECURITY – STI 101 STIGs

STIG 150 is designed to answer core questions and provide guidance on the implementation of STIGs. Students will develop a cybersecurity vulnerability management lens in respects to conceptualizing and addressing DISA STIGs, and its relationship within the RMF (Risk Management Framework) life cycle.

Extensive hands-on experience within a virtual lab environment will allow students to execute the SCC SCAP Tool and STIG Viewer, with the most current benchmarks and STIGs by diagnosing virtual hosts within their virtual environments. Upon successful completion of the program, you will be awarded a certificate.

JR. NETWORK ENGINEER CAREER CERTIFICATION

The Jr. Network Engineer course will prepare students with the skillset that will allow them to perform on the job. This training's primary focus is on providing the student hands-on training with Cisco Routers and Switch Training instrumental in securing their first DoD IT Job. This course is 100% hands-on Network training. Students will learn how to build EIGRP and OSPF Networks, configure IP Addresses on devices, wire the devices, create VLANs and more. After completing this track, you will be able to build and manage Cisco networks. Specifically, you will learn how to design, create and manage networks. This program consists of two (2) courses: Introduction to Jr Network Engineer, Intermediate to Jr Network Engineer and Advanced to Jr Network Engineer. Upon successful completion of the program, you will be awarded a certificate.

JR. NETWORK ENGINEER CAREER CERTIFICATION

Course Number: CIS 101	Course Title	Clock Hours
	Introduction to Jr Network Engineer	160

INTRODUCTION TO JR NETWORK ENGINEER – CIS 101

Introduces the principles and techniques necessary for network engineers. Training will provide the student with the ability to build EIGRP and OSPF Networks, Configure IP Addresses on devices, wire the devices, create VLANs and more. Learns to manage an entire computer network of a company. They are responsible for making sure the systems are functioning as intended. A network engineer must link all computers with the central computer and ensure that all software and files are available to each computer as necessary. They must also link computers to machines such as fax machines, printers, and telephones. Communication device management such as cellular phone maintenance also falls under this job description. The network engineer is responsible for developing, installing, updating, and maintaining everything associated with the network including upgrading software and hardware and incorporating new devices.
Prerequisite for this course: A High School Diploma or Equivalent or who are beyond the age of compulsory high school attendance.

CISCO CERTIFIED NETWORK ADMINISTRATOR CERTIFICATION (CCNA)

Course Number: CIS 201 CCNA	Course Title	Clock Hours
	Certified Cisco Network Administrator	80

CISCO CERTIFIED NETWORK ADMINISTRATION CIS 201

This course will prepare you for your CCNA certification. Once certified, you will have the skills and certification to install, maintain and troubleshoot small networks or a branch of an enterprise network, and implement basic network security. CCNA Routing and Switching is a Certification Course for Entry-Level Network Engineers maximizing your investment in foundational networking knowledge and increasing the value of your employer's network. The CCNA Routers and Switches are for Network Specialists, Network Administrators, and Network Support Engineers with 0-3 years of experience. The CCNA Routing and Switching exam validates the ability to install, configure, operate, and troubleshoot medium-size routed and switched networks. Upon successful completion of the program, you will be awarded a certificate.

HELPDESK SUPPORT SPECIALIST

HELPDESK SPECIALIST CERTIFICATE

The Helpdesk Specialist course is 100% hands-on training. This course prepares students with Helpdesk skillset that allows them to perform successfully on the job. The focus is to provide students with hands-on training instrumental in securing their first IT job.
These courses assume you are familiar with using personal computers, mouse and keyboard (basic typing skills are recommended). You should be comfortable in the Windows environment and be able to use Windows to manage information on your computer. Specifically, you should be able to launch and close programs, navigate to information stored on the computer and manage files and folders. Upon successful completion of the program, you will be awarded a certificate.

HELPDESK SPECIALIST CERTIFICATE

Course Number: HEL 101	Course Title	Clock Hours
	Introduction to HEL	80

INTRODUCTION TO HELPDESK SUPPORT SPECIALIST – HEL 101

MD Technical School Helpdesk Support Specialist course is 100% hands-on training. In this course, the student learns how to take calls, fix user's systems issues, install and configure printers and more. This course will provide you with the skillset to take on a career as a Helpdesk Support Specialist.

DEVOPS SPECIALIST CERTIFICATE

The DevOps Specialist track is comprised of three modules. Module 1 provides a comprehensive overview of DevOps practices, models, and techniques, along with coverage of DevOps benefits, challenges and business and technology drivers. Also explained is how DevOps compares to traditional solution development and release approaches and how the application of DevOps can be monitored and measured for concrete business value. Module 2 delves into the application of DevOps practices and models by exploring how the DevOps lifecycle and its associated stages can be carried out and further identifying related challenges and considerations. In-depth coverage is provided for the application of Continuous Integration (CI) and Continuous Delivery (CD) approaches, along with an exploration of creating deployment pipelines and managing data flow, solution versions and tracking solution dependencies. The final course module consists of a series of lab exercises that require participants to apply their knowledge of the preceding courses in order to fulfill project requirements and solve real world problems. A Certified DevOps Specialist has demonstrated proficiency in DevOps processes, metrics and models and has acquired specialized skills to put DevOps techniques into real-world practice. There are no prerequisites for the course required except for a general IT background. Upon successful completion of the program, you will be awarded a certificate.

DEVOPS SPECIALIST CERTIFICATE

Course Number: DO90.01	Course Title	Clock Hours
	DevOps Specialist	8

DEVOPS SPECIALIST – DO90.01

The DevOps Specialist program develops skills in DevOps practices, processes, metrics and models. Students who complete this program can take an exam to attain the DevOps Specialist certification. A certified DevOps Specialist understands the requirements to successfully apply DevOps in support of achieving project objectives and realizing strategic business goals. Along with a solid understanding of DevOps process stages, techniques and models, a Certified DevOps Specialist is also required to be proficient in the monitoring and measuring of DevOps initiatives to ensure that entire project lifecycles are carried out as planned.

ARTIFICIAL INTELLIGENCE SPECIALIST CERTIFICATE

The Artificial Intelligence (AI) Specialist track is comprised of three modules. Module 1 provides essential coverage of artificial intelligence and neural networks in easy-to-understand, plain English. The course provides concrete coverage of the primary parts of AI, including learning approaches, functional areas that AI systems are used for and a thorough introduction to neural networks, how they exist, how they work and how they can be used to process information. The course establishes the five primary business requirements AI systems and neural networks are used for, and then maps individual practices, learning approaches, functionalities, and neural network types to these business categories and to each other, so that there is a clear understanding of the purpose and role of each topic covered. The course further establishes a step-by-step process for assembling an AI system, thereby illustrating how and when different practices and components of AI systems with neural networks need to be defined and applied. Finally, the course provides a set of key principles and best practices for AI projects. Module 2 covers a series of practices for preparing and working with data for training and running contemporary AI systems and neural networks. It further provides techniques for designing and optimizing neural networks, including approaches for measuring and tuning neural network model performance. The practices and techniques are documented as design patterns that can be applied individually or in different combinations to address a range of common AI system problems and requirements. The patterns are further mapped to the learning approaches, functional areas and neural network types that were introduced in Module 1: Fundamental Artificial Intelligence. The final course module consists of a series of lab exercises that require participants to apply their knowledge of the preceding courses in order to fulfill project requirements and solve real world problems. A Certified Artificial Intelligence Specialist has demonstrated proficiency in artificial intelligence (AI) approaches and algorithms, and proven skills for designing and validating AI solutions and modeling neural networks. There are no prerequisites for the course required except for a general IT background. Upon successful completion of the program, you will be awarded a certificate.

ARTIFICIAL INTELLIGENCE

Course Number: AI90.01	Course Title	Clock Hours
	Artificial Intelligence	8

ARTIFICIAL INTELLIGENCE SPECIALIST – AI90.01

The Artificial Intelligence (AI) Specialist program develops skills in AI practices and learning approaches, as well as Neural Network architectures, cell types and activation functions. Students who complete this program can take an exam to attain the Artificial Intelligence Specialist certification. A Certified Artificial Intelligence Specialist understands how AI practices can be utilized to perform data analysis and autonomous data processing with unprecedented functionality and business value. In addition to a demonstrated proficiency of AI learning approaches and functional designs, the Certified Artificial Intelligence Specialist has comprehensive knowledge of Neural Network architecture models, associated layers and neuron cell types.

BLOCKCHAIN ARCHITECT CERTIFICATE

The Blockchain Architect track is comprised of three modules. Module 1 provides a clear, end-to-end understanding of how blockchain works. It breaks down blockchain technology and architecture in easy-to-understand concepts, terms and building blocks. Industry drivers and impacts of blockchain are explained, followed by plain English descriptions of each primary part of a blockchain system and step-by-step descriptions of how these parts work together. Module 2 delves into blockchain technology architecture and the inner workings of blockchains by exploring a series of key design patterns, techniques and related architectural models, along with common technology mechanisms used to customize and optimize blockchain application designs in support of fulfilling business requirements. The final course module consists of a series of lab exercises that require participants to apply their knowledge of the preceding courses in order to fulfill project requirements and solve real world problems. A Certified Blockchain Architect has demonstrated proficiency in Blockchain functions, architecture and security and has acquired specialized skills to assess and design real-world Blockchain solutions. There are no prerequisites for the course required except for a general IT background. Upon successful completion of the program, you will be awarded a certificate. Upon successful completion of the program, you will be awarded a certificate.

BLOCKCHAIN

Course Number: BC90.01	Course Title	Clock Hours
	Blockchain Architect	8

Blockchain Architect– BC90.01

The Blockchain Architect program develops skills in Blockchain functions, architectural models, technology and security. Students who complete this program can take an exam to attain the Blockchain Architect certification. A Certified Blockchain Architect understands the business value and technology architecture behind Blockchain, as well as the inner workings of Blockchain technologies and solutions. In addition to a proven understanding of the distributed ledger, immutable data storage and consensus processing, a Certified Blockchain Architect has proficiency with Blockchain architectural models, distributed ledger co-existence models and Blockchain security threats and countermeasures.

INTERNET OF THINGS CERTIFICATE

The IoT Architect track is comprised of three modules. Module 1 covers the essentials of the field of Internet of Things (IoT) from both business and technical aspects. Fundamental IoT use cases, concepts, models, and technologies are covered in plain English, along with introductory coverage of IoT architecture and IoT messaging with REST, HTTP and CoAp. Module 2 provides a drill-down into key areas of IoT technology architecture and enabling technologies by breaking down IoT environments into individual building blocks via design patterns and associated implementation mechanisms. Layered architectural models are covered, along with design techniques and feature-sets covering the processing of telemetry data, positioning of control logic, performance optimization, as well as addressing scalability and reliability concerns. The final course module consists of a series of lab exercises that require participants to apply their knowledge of the preceding courses in order to fulfill project requirements and solve real world problems. A Certified IoT Architect has demonstrated proficiency in IoT technology architecture, protocols, mechanisms and security, and has acquired specialized skills to assess, design and deliver real-world IoT solutions. There are no prerequisites for the course required except for a general IT background. Upon successful completion of the program, you will be awarded a certificate.

INTERNET OF THINGS

Course Number: IoT90.01	Course Title	Clock Hours
	Internet of Things	8

Internet of Things– IoT90.01

The IoT Architect program develops skills in Internet of Things (IoT) technology and architecture, along with proficiency in radio protocols, telemetry messaging and IoT architecture layers. Students who complete this program can take an exam to attain the IoT Architect certification. A Certified IoT Architect understands the business value behind the utilization of the Internet of Things and has demonstrated proficiency in the design of IoT devices and solutions with scalable connectivity and based on a range of functional distribution models, including models based on edge computing.

MACHINE LEARNING SPECIALIST CERTIFICATE

The Machine Learning Specialist track is comprised of three modules. Module 1 provides an easy-to-understand overview of machine learning for anyone interested in how it works, what it can and cannot do and how it is commonly utilized in support of business goals. The course covers common algorithm types and further explains how machine learning systems work behind the scenes. Module 2 delves into the many algorithms, methods, and models of contemporary machine learning practices to explore how a range of different business problems can be solved by utilizing and combining proven machine learning techniques.

The final course module consists of a series of lab exercises that require participants to apply their knowledge of the preceding courses in order to fulfill project requirements and solve real world problems. A Certified Machine Learning Specialist has demonstrated proficiency in machine learning methods, models and algorithms and can design scalable machine learning systems capable of solving complex business problems.
There are no prerequisites for the course required except for a general IT background. Upon successful completion of the program, you will be awarded a certificate.

MACHINE LEARNING

Course Number: ML90.01	Course Title	Clock Hours
	Machine Learning Specialist	8

Machine Learning Specialist – ML90.01

The Machine Learning Specialist program develops skills in Machine Learning practices, models and algorithms, as well as Machine Learning systems that can perform a range of data analysis processing tasks. Students who complete this program can take an exam to attain the Machine Learning Specialist certification. A Certified Machine Learning Specialist understands how and where Machine Learning techniques are best utilized to produce business value. Machine Learning algorithms and system design are of second nature to the Certified Machine Learning Specialist, who further possesses in-depth knowledge of model learning approaches, analysis practices and patterns. Upon successful completion of the program, you will be awarded a certificate.

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)

Program Outline		
Course Number	Course Title	Clock Hours
ITI 101	INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY	20
Total:		20

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY ITI 101

This course will prepare you for your ITIL Foundation certification. Once certified, you will have the skills and certification to manage IT Services. It enables candidates to look at IT service management through an end-to-end operating model for the creation, delivery and continual improvement of tech-enabled products and services. Upon successful completion of the program, you will be awarded a certificate.

CERTIFIED ETHICAL HACKER (C|EH)

Program Outline		
Course Number	Course Title	Clock Hours
CEH 101	CERTIFIED ETHICAL HACKER (C|EH)	30
Total:		30

CERTIFIED ETHICAL HACKER (C|EH) 101

This course will prepare you for your Certified Ethical Hacker certification. Once certified, you will have the skills and certification to provide ethical hacking IT Services. Will obtain the skillset around the Tactics and Procedures required to be a tactical cybersecurity professional. Focusing on the entire kill-chain process, C|EH covers a variety of topics from foot printing and reconnaissance, to scanning, gaining access, maintaining access, and covering your tracks. This 5-phase ethical hacking process applies to a variety of scenarios including traditional on-premises networks, cloud, hybrid, IoT systems, and stretches across a variety of topologies and application environments. Students will learn a variety of tools and techniques across this evaluation process as well as how hackers will utilize the same TTPs to hack into organizations. Every concept taught in C|EH is backed up by hands on labs hosted in our Cyber Range. Upon successful completion of the program, you will be awarded a certificate.

COMPUTER HACKING FORENSIC INVESTIGATOR (C|HFI)

Program Outline		
Course Number	Course Title	Clock Hours
CHFI 101	COMPUTER HACKING FORENSIC INVESTIGATOR (C|HFI)	40
Total:		40

COMPUTER HACKING FORENSIC INVESTIGATOR (C|HFI) 101

Hacking Forensic Investigator (C|HFI) is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. C|HFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around Dark Web, IoT, and Cloud Forensics. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies. The program equips candidates with the necessary skills to proactively investigate complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks. The course aligns with all the crucial forensic job roles across the globe. Upon successful completion of the program, you will be awarded a certificate.

CERTIFIED NETWORK DEFENDER (C|ND)

Program Outline		
Course Number	Course Title	Clock Hours
CHFI 101	CERTIFIED NETWORK DEFENDER (C|ND)	40
Total:		40

CERTIFIED NETWORK DEFENDER (C|ND) 101

Certified Network Defender (C|ND) is the only comprehensive ANSI accredited, hands-on focused program in the market that gives organizations vendor-neutral training in Networking. C|ND provides its attendees with a firm grasp of networking security, presenting a detailed and methodological approach to securing networks. As a network administrator, how to identify what parts of an organization need to be reviewed and tested for security vulnerabilities and how to reduce, prevent, and mitigate risks in the network. CND is based on the cybersecurity education framework and work role task analysis presented by the National Infocomm Competency Framework (NICF). The program is also mapped to the Department of Defense (DoD) roles for system/network administrators as well as global work roles and responsibilities laid out by the revised NICE Framework. Upon successful completion of the program, you will be awarded a certificate.

CERTIFIED CLOUD ENGINEER (CCE)

Program Outline		
Course Number	Course Title	Clock Hours
CCE 101	CERTIFIED CLOUD ENGINEER (CCE)	40
Total:		40

CERTIFIED CLOUD ENGINEER (CCE) 101

Certified Cloud Security Engineer (C|CSE) is the only comprehensive ANSI accredited, hands-on focused program in the market that gives organizations vendor-neutral training in cloud security. C|CSE provides its attendees with a firm grasp of cloud security, presenting a detailed and methodological approach to security and evidence analysis that also pivots around the Cloud. The tools and techniques covered in this program will prepare the learner for cloud security practices, technologies, frameworks, and principles to deliver a well-balanced mix of the theoretical and practical skills you need to become a cloud security expert. Upon successful completion of the program, you will be awarded a certificate.

CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO)

Program Outline		
Course Number	Course Title	Clock Hours
CISO 101	CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO)	40
Total:		40

CERTIFIED CLOUD SECURITY ENGINEER (C|CSE) 101

Certified Chief Information Security Officer (C|CISO) Program has certified leading information security professionals around the world. A core group of high-level information security executives, the C|CISO Advisory Board, formed the foundation of the program and outlined the content covered by the exam, body of knowledge, and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks, and still others as instructors. Each segment of the program was developed with the aspiring and sitting CISO in mind and looks to transfer the knowledge of seasoned executives to the next generation of leaders in the areas that are most critical in the development and maintenance of a successful information security program. Upon successful completion of the program, you will be awarded a certificate.

CERTIFIED SOC ANALYST (C|SA)

Program Outline		
Course Number	Course Title	Clock Hours
CSA 101	CERTIFIED SOC ANALYST (C|SA)	40
Total:		40

CERTIFIED SOC ANALYST (C|SA) 101

C|SA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need. To read more about SOC and how they are important to many industries. Upon successful completion of the program, you will be awarded a certificate.

CERTIFIED CYBERSECURITY TECHNICIAN CERTIFICATION (C|CT)

Program Outline		
Course Number	Course Title	Clock Hours
CCT 101	CERTIFIED CYBERSECURITY TECHNICIAN CERTIFICATION (C|CT)	40
Total:		40

CERTIFIED CYBERSECURITY TECHNICIAN CERTIFICATION (C|CT) 101

The Certified Cybersecurity Technician (C|CT) is an entry-level cybersecurity program, to address the global demand for a qualified cybersecurity workforce. the C|CT to provide individuals starting their careers in IT and cybersecurity with a certification that validates their hands-on technical skills. The C|CT certification provides total foundational cybersecurity domain coverage with key concepts in each domain combined with practical hands-on labs and critical thinking challenges producing world-class cyber security technologists. Upon successful completion of the program, you will be awarded a certificate.

CERTIFIED SECURE COMPUTER USER (CSCU)

Program Outline		
Course Number	Course Title	Clock Hours
CSCU 101	CERTIFIED SECURE COMPUTER USER (CSCU)	40
Total:		40

CERTIFIED SECURE COMPUTER USER (CSCU) 101

Certified Secure Computer User (C|SCU) training program is to provide individuals with the necessary knowledge and skills to protect their information assets. This class will immerse students into an interactive environment where they will acquire a fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, virus and backdoors, emails hoaxes, sex offenders lurking online, loss of confidential information, hacking attacks and social engineering. More importantly, the skills learned from the class help students take the necessary steps to mitigate their security exposure. Upon successful completion of the program, you will be awarded a certificate.