CCBC
CYBERSECURITY INSTITUTE

CCBC Cybersecurity Institute Launches Accelerated Stackable Credential Series For Work on Government Networks Spring 2018

Registration is underway for enrollment in the *Accelerated Stackable Credentials Series* available *through the* CCBC Cybersecurity Institute. The program is designed for cybersecurity professionals to rapidly obtain several industry certifications required for work on government networks.

The four courses leading to industry-recognized certifications in Cybersecurity include Network+, Security+, Operating Systems Security (SCMP) and Certified Ethical Hacking (CEH).

The entire four-course series may be completed in 16 weeks. Courses are delivered in four-week blended formats (two evening per week in the classroom, with additional online studies). Classes meet on Tuesday and Thursday evenings at a CCBC campus.

Individuals successfully completing the series will earn 15 college credits and be eligible to take industry certification examinations at the Pearson VUE Authorized Test Center conveniently located at CCBC Essex.

The *Accelerated Stackable Credentials Series* program supports cybersecurity professionals currently or planning to work in government positions or as government contractors on jobs requiring the DoD 8570.1 certifications.

For more information, including cost and location of classes, please contact Ron Hinkel – Director of the Cybersecurity Institute at 443-840-3932 or rhinkel@ccbcmd.edu or Noell Damron, Chair of Network Technology at 443-840-2811 or ndamron@ccbcmd.edu.

To register for the Accelerated Stackable Credential series, please contact CCBC Enrollment Services at 443-840-2222.

# # #

CCBC Cybersecurity Institute – Spring 2018
Accelerated Stackable Certification Series
For Work on Government Networks

Block I: DCOM 251 – Local Area Networks

Local Area Networks explores planning, installing, configuring, administering and troubleshooting a computer network. This is accomplished through hands-on exercises and lecture material covering the fundamental building blocks that form a modern network, such as protocols, topologies, hardware, and network operating systems. This class is intended to serve the needs of students with an interest in mastering foundational, vendor-independent networking concepts, as well as those interested in taking the CompTIA Network+ certification exam.

Week One	Introduction to Networking; Networking Models and Standards; Transmission Basics and Networking Media
Week Two	Network Protocols; Networking Hardware; Topologies and Access Methods
Week Three	Wide Area Networks; Network Operating Systems
Week Four	Integrity and Availability; Information Security

Block II: DCOM 258 – Introduction to Information Security

Introduction to Information Security serves the needs of students interested in understanding the field of Information Security and its relation to other areas of Information Technology (IT). The material covered in this class provides the broad-based knowledge and skills necessary to prepare students for further study in specialized security fields, or may be used by those interested in a general introduction to the field. This course is also intended to serve the needs of those seeking to pass the CompTIA Security+ certification.

Week One	Introduction to Information Security; System Threats and Risks
Week Two	Protecting Systems; Network Vulnerabilities, Attacks, and Defenses; Wireless Network Security
Week Three	Access Control Fundamentals; Authentication; Performing Vulnerability Assessments and Audits
Week Four	Basic Cryptography, Cryptographic Protocols, and Public Key Infrastructure (PKI); Business Continuity Planning and Procedures; Policies and Legislation

Block III: DCOM 214 – Operating Systems Security

Operating Systems Security provides students with the hands-on skills needed to protect networks from the inside-out by focusing on Linux and Windows system hardening. The class is designed to help students prepare for professional careers in the information and communication technology field and the Security Certified Network Professional (SCNP) certification exam.

Week One	Cryptography and Data Security; Ethical Hacking Tools and Techniques
Week Two	Hardening Linux and Windows Systems; Security on the Internet and the WWW
Week Three	Risk Analysis; Information Security Policies and Procedures
Week Four	Traffic Analysis

Block IV: DCOM 215 – Ethical Hacking and Systems Defense

Ethical Hacking and Systems Defense is the capstone course that combines an ethical hacking methodology with the hands-on application of security tools to better help students secure their systems. Students are introduced to common counter-measures that effectively reduce and/or mitigate attacks. The class is designed to help students prepare for professional careers in the information and communication technology field.

Week One	Ethical Hacking; Penetration Testing Professional Certifications
Week Two	Online/Print Resources; Foot-Printing
Week Three	Scanning; Enumeration
Week Four	Exploitation; Post-Exploitation