COMPUTER / IT PROGRAMS

CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST

Certificate of Completion
23 credit hours

This program is based on the National Security Agency (NSA) CAE Workforce Development Grant. The Certificate program meets the NSA Cybersecurity Center of Excellence/Cyber Defense (CAE/CD) knowledge unit's designation, NIST National Initiative in Cybersecurity Education Framework (NICE) and is specifically designed to prepare students as Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011 and CNSSI No. 4016 Entry Level Risk Analysts or provide current Information Systems professionals with an Information Systems security certification to meet the needs of current and future employer requirements based on the NICE Work Roles for Operate and Maintain, Protect and Defend, and Operate. Upon completion of this program students will be receiving college certification of completion, ACT WorkKeys National Career Readiness Certificate, and the following Industry Stackable Certifications: CompTIA A+, Security+, and EC Council ECH Ethical Hacking. *Note, the labs use the INFOSEC virtual labs for hands-on training and the National Cyber League (NCL) Competition.* Students also receive an NCL Scouting report showing their knowledge skills and abilities in the following cybersecurity areas: The following are the categories of cybersecurity scenarios that you were evaluated against:

- Cryptography – Identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plain text.
- Enumeration and Exploitation – Identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.
- Log Analysis – Utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.
- Network Traffic Analysis – Identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.
- Open Source Intelligence – Utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.
- Password Cracking – Identify types of password hashes and apply various techniques to efficiently determine plain text passwords.
- Scanning – Identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.
- Web Application Exploitation – Identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.
- Wireless Access Exploitation – Identify the security posture of wireless networks from network captures.

**Additional hours may be required for program requirements for transfer students who are NMGEC complete.*

Any student who is ineligible for state, national, or industry licensure or certification is ineligible for entry into this program.

Institutional and Related Requirements –
Not applicable

Program Requirements – 23 hours

CIST 1409 – IT Essentials I: PC Hardware, Software, and Practical Applications (4)
CIST 1413 – Network Administration concepts (4)
CIST 2881 – Cybersecurity Fundamentals (3)
CIST 1181 – Business Continuity and Disaster Recovery (3)
CIST 1111 – Introduction (Foundation) of Information Systems (3)
CIST 2854 – National Cyber League (NCL) (0)
CIST 2887 – Ethical Hacking (3)
CIST 2858 – Cyber Ethics, Professionalism, and Career Development (3)

New Mexico General Education Curriculum (NMGEC) –
Not applicable

Revised August 2025