The GBC MISI Academy Centers of Academic Excellence in Cybersecurity (CAE-C) Program

The GBC MISI Academy Centers of Academic Excellence in Cybersecurity (CAE-C) Program

about the program

The National Security Agency (NSA) in partnership with the Maryland Innovation & Security Institute (MISI) and the GBC MISI Academy seek applicants for an 8-week paid internship program designed for college seniors about to enter the technical workforce currently enrolled in an institution designated as a CAE-CD or CAE-CO by the National Security Agency Center of Academic Excellence in Cybersecurity. The GBC MISI Academy Centers of Academic Excellence in Cybersecurity (CAE-C) Program seeks out students who are self-motivated, dedicated to solving challenging problems, and have a passion for cybersecurity. The organization provides internships that are virtual and in person internships at MISI's Columbia Maryland headquarters or MISI'S MindScape facility. Beginning March 7, 2022, through April 29, 2022, MISI and the GBC MISI Academy will host a virtual internship for a maximum of 20 students.

The GBC MISI Academy CAE-C Program runs Monday through Friday, with live and asynchronous events, hands-on and self-paced learning. Participants are expected to complete 20 hours a week and will be paid a stipend of $20/hour for eight weeks. We understand that some participants will already be enrolled in their spring term courses and will be unavailable during those times. Participants with class or work scheduling conflicts may provide documentation of those conflicts and will be excused for up to eight hours per week, provided the participant views the recorded sessions within the same week. The Program will strive to schedule live sessions between the hours of noon and 5:00 pm (Eastern Standard Time) to allow for geographic separation. Participants are expected to have a reliable internet connection and computer with audio and camera capabilities sufficient for participation in virtual meetings.

Participants in the Program will receive hands-on experience at the GBC MISI Academy with access to a physical and virtual cyber range and technical skills training content partners that include Elastic, Cybrary, AWS, and numerous others. This rich library of on-demand and live technical cyber skills training enhances the internship with real-world hands-on experiences. Interns will also work on diverse assignments related to Defense Industrial Base (DIB) cyber challenges and will have the opportunity to work with mentors to solve real-world problems.

Completed applications are due no later than January 7, 2022, at 3:00 p.m. Eastern Time for consideration. Applications must be submitted via the site: https://www.misiacademy.tech. Questions about the application process can be sent to applications@misiacademy.tech.

Candidates will be notified by email starting the week of January 17 if they are selected for an interview. Interviews will be conducted via Zoom. Selections will be notified by February 14; if selected, applicants will need to immediately complete the background check. MISI will provide instructions on how to submit the information required for the background check.

Program Tracks

The virtual Internship tracks outlined below are typical of the program but could change and be replaced with other offerings. Among all tracks, the intern will understand how the skills learned and industry recognized certificates achieved align with the NICE framework.

DoD Cybersecurity Policy – The threats facing the DoD's classified and unclassified information are on the rise as nation states attempt to outmaneuver US innovation in commercial and defense of the nation related technologies. The US is an ever more connected society as we provide more services online, digitally store data, and rely on contractors for a variety of information technology services. The move to the cloud, advent of 5G, quantum, artificial intelligence, and more are technological advances that will propel the United States, but also our adversaries, in the continued race for superiority in cyberspace

This track will delve into the DoD and other US government cyber policy directives such as DFARS 7012, 7019, 7020 and the CMMC 2.0 and others. Interns will work alongside MISI staff to assist DoD defense industrial base companies to understand and comply with DoD cybersecurity policies. The internship will expose the intern to the development of cyber policies such as those required by DFARS 7012 and others. The intern will support supply chain risk assessments using data gathered from defense companies through surveys and from MISI sensors the gaps in cyber compliance of the target company but also the types of cyber vulnerabilities and threats requiring mitigation to achieve compliance assessment readiness.

DoD Cybersecurity Policy

The threats facing the DoD's classified and unclassified information are on the rise as nation states attempt to outmaneuver US innovation in commercial and defense of the nation related technologies. The US is an ever more connected society as we provide more services online, digitally store data, and rely on contractors for a variety of information technology services. Technology such as the move to the cloud and the advent of 5G, quantum and artificial intelligence and more are advances that will propel the US but also our adversaries in the continued race for superiority in cyberspace.
This track will delve into the DoD and other US government cyber policy directives such as DFARS 7012, 7019, 7020 and the CMMC 2.0 and others. Interns will work alongside MISI staff to assist DoD defense industrial base companies to understand and comply with DoD cybersecurity policies. The internship will expose the intern to the development of cyber policies such as those required by DFARS 7012 and others.

The intern will support supply chain risk assessments using data gathered from defense companies through surveys and from MISI sensors the gaps in cyber compliance of the target company but also the types of cyber vulnerabilities and threats requiring mitigation to achieve compliance assessment readiness. To put more real-world context to this track, the intern will be exposed to subject matter expert sessions on zero trust, multi-factor authentication, digital rights management, firmware compromises and supply chain security challenges and solutions.

Track 2

Security Operations Center (SOC) Tier 1

In this track the intern will learn the fundamentals of security operations center functions, tools, and daily operational processes and techniques. The intern will participate in hands on labs and skill development utilizing the Elastic learning environment to establish fundamental knowledge and skills. Throughout the internship the intern will progressively be exposed to the MISI cloud based live SOC environment and work with a MISI subject matter expert using various aspects of the SOC environment. As the internship progresses the intern will become part of the cyber threat hunt and analytic team at MISI. The intern will analyze possible threats, discuss findings with peers and establish the courses of action necessary to mitigate real cyber threats found on the target network. The intern will learn the various techniques, tools and processes needed to conduct and validate cyber threat information. The intern will also write threat reports and develop visualizations using Elastic's Kibana.

Track 3

Fundamentals of Industrial Control Cybersecurity

In this track interns will learn about the systems, software and technology that control the very basic functions of everyday life such as the manufacturing of medicine, automobiles, computers and weapon systems but also that control elevators, the energy grid and water supply. The intern will be exposed virtually to the MISI industrial control lab and range to establish a fundamental understanding of the components, functions, protocols and operational capabilities of programmable logic controllers, Human Machine Interface, actuators, and other aspects of industrial control systems. The intern will be exposed to common cyber-attacks and how they impact these systems and the defensive cyber tools and techniques used to detect cyber and adversarial threats to the nation's critical infrastructure.

This internship experience will include sessions on maritime related industrial control cyber. The intern will be exposed to, learn and participate in offensive cyber-attacks using the MISI lab environment to better understand the nature of cyber-attacks such as ransomware. The intern will support supply chain risk assessments using data gathered from defense companies through surveys and MISI sensors. The data gathered will also identify the target companys gaps in cyber compliance and the types of cyber vulnerabilities and threats requiring mitigation to achieve compliance assessment readiness.

In addition to the core tracks described above the intern will learn about security clearances, the various authorities of the DoD and civilian agencies as they pertain to cyber, gain knowledge of the legislative and budget constructs used to propel US cyber policy such as the National Defense Authorization Act (NDAA), Defense Federal Acquisition Regulations (DFARS), the National Institute of Standards and Technology and it role in cyber best practices and standards, the diverse career tracks that comprise the cybersecurity field, real world interview skills and access to a life skills coach to better prepare you to enter the workforce.

The internship will also include interviews with government and industry partners who are seeking future graduates to staff their cybersecurity openings.

Application Details

Successful completion of a background check and verification of U.S. citizenship are required for participation in the Program. The cost of the background check is paid for or reimbursed by the MISI Academy.

To apply to the MISI Academy CAE-C Program students must:

a) Be a current senior (at least 90 earned credits) enrolled at least half-time in a College or University that is designated as a CAE-CD or CAE-CO by the National Security Agency Center of Academic Excellence in Cybersecurity.
b) Have a minimum 3.0 cumulative GPA and be in good academic standing.
c) Applicants are required to have completed a minimum of nine credit hours in the subjects listed below or equivalent subject matter. The application must include a transcript or official grade report.
Cybersecurity Fundamentals (or equivalent)

- Network Administration/Security
- Data Science
- Applications Security
- Information Assurance
- Network Engineering
- Systems Engineering
- Software Engineering (Python, C, C++, Assembly language, embedded programming)
- Data Communications (or equivalent)
- Database Security
- Computer and Network Forensics (or equivalent)
- A recent certification (within 2 years) from an industry recognized cybersecurity professional trade organization (e.g., EC-Council, CompTIA, (ISC)2) may substitute for a course.

d) Be a US Citizen.
e) Be able to pass a background check.
f) Have strong moral character, good communication skills, and a demonstrated interest in a cybersecurity career field through successful course work, internships, after school programs, clubs, professional organizations, independent learning, or other cyber related activities.

Completed applications will consist of:

a) Cover Letter
b) Resume
c) Transcript: electronic version (PDF or JPEG) of an official or unofficial transcript. If unable to obtain transcripts, please send in report cards capturing all semesters of enrollment and highlighting courses required for this program.
d) Letter of Recommendation from a professor or employer who can speak to the applicant's abilities in any of the technical areas listed in 1c).
e) List of Spring 2022 registered courses with dates and times indicated. Include course registration number and section or professor/instructor contact information.

Preference will be given to:

a) Students with more than the minimum nine credit hours listed above.
b) Applicants with minimal conflicts during the hours of 12:00 and 5:00 pm EST.