Certificate in Cyber Defense and Information Assurance

Graduate Certificate in Cyber Defense and Information Assurance

Please designate a responsible department and individual for this proposal:

Seema Freer Ph.D.,
Associate Professor,
Managing Director, PSM Programs

And

Jamie Payton Ph.D.,
Chair, Computer and Information Sciences
Associate Professor,
Department of Computer and Information Sciences
Certificate in Cyber Defense and Information Assurance

I. Overview and rationale

As our physical and digital worlds become more deeply interwoven, a web of interdependence is increasingly fading away the distinction between physical and cyberspace infrastructures. One consequence is that citizens are rendered extremely vulnerable to threats against our cyberinfrastructure by cybercriminals who can inflict crippling blows to pockets of society or even the entire nation. With projections that the dearth of a global information security workforce will reach a staggering 1.5 million by 2021, the federal government has expressed its support to meet this urgent need.

The Certificate in Cyber Defense and Information Assurance is a shorter version of the program for working professional seeking credentials in the field, but who are unable to commit to completing a capstone project which is part of the Professional Science Master's (P.S.M.) program in Cyber Defense and Information Assurance (CyberDIA). The program addresses the dynamic and cross-cutting nature of the current and continuously evolving cyberspace and the barrage of ever-increasing and never-ceasing threats it faces. The program is designed for aspiring technical professionals at all career levels – entry-level, mid-career, and senior executives – who want to equip themselves with skills necessary to protect their organization and the nation from increasing cyberthreats. The multidisciplinary program design borrows knowledge, skills, and expertise from different academic disciplines, including business, computer and information sciences, electrical and computer engineering, and law. The key focus is on a holistic cybersecurity framework, i.e., one that is built around the core principles of preventive, detective, and corrective security mechanisms. While the CyberDIA curriculum is technology intensive, focusing on network security and digital forensics, it also bridges the ever-increasing gap between cybersecurity technology and cybersecurity policies.

II. Relationship of Proposed Program to others in the College or University

The certificate will provide advanced academic credentials for the working professional seeking training beyond the baccalaureate degree. The certificate will be transcripted requiring the completion of up to and no more than 12 credits from the list of core classes in the current curriculum of the PSM in Cyber Defense and Information Assurance. It will also be a means for training of students who are unable to complete the rigors of a 4 - 5 semester degree program, in 1 - 2 semesters.

The Certificate in Cyber Defense and Information Assurance program will provide a mechanism to obtain a certificate in 1 - 2 semesters or for the part time student, the time required to complete 12 credits of core classes, with a GPA of 3.0. The classes will be taught by the same faculty as in the PSM in Cyber Defense and Information Assurance program, as students will be taking the same core classes as the PSM in Cyber Defense and Information Assurance students without committing to a capstone project or a graduate degree requiring 30 credits. The Certificate in Cyber Defense and Information Assurance will credential future leaders in the field through a curriculum chosen according to the student’s interest.

III. Curriculum:

Below is the list of core course which a student may take to complete the certificate in Cyber Defense and Information Assurance. Student advising will be provided to meet the specific interests for each student.
### Course List

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 5107</td>
<td>Comp Systems Security &amp; Privacy †</td>
<td>3</td>
</tr>
<tr>
<td>CIS 5017</td>
<td>Operating Systems and Architecture †</td>
<td>3</td>
</tr>
<tr>
<td>CIS 5405</td>
<td>Introduction to Digital Forensics †</td>
<td>3</td>
</tr>
<tr>
<td>CIS 5415</td>
<td>Ethical Hacking and Intrusion Forensics †</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td><strong>Total Credit Hours</strong></td>
<td><strong>12.00</strong></td>
</tr>
</tbody>
</table>

† Student may replace any ONE course from the list with a graduate level course approved by the advisor.

### IV Impact on Faculty and Students
This will not impact faculty or require new faculty.

### V Impact on Resources
This program is a tuition generating program and will contribute to the revenue stream already generated by the parent program.

### VII Assessment
A formal assessment will be conducted after the certificate has run for one or two years.

### VIII Summary of Peer or Aspirant Programs
A graduate certificate in Cyber Defense and Information Assurance is offered in a few universities a link and summary of 3 such programs is provided in Appendix A.

### IX Implementation
Pending approval, the certificate program is ready for a start date of Fall 2020.

### X Process for Proposal Development
The certificate program was developed by the Steering Committee based on reflection of graduate outcomes, conversations with students and the Committee’s observations of student progress in other PSM programs. The focus of developing this program was to provide a mechanism for students to succeed who, for various reasons whether financial, academic or work related could not continue in the program.

### APPENDIX A

**Universities offering equivalent Cyber Defense and Information Assurance Certificates**

**Rochester Institute of Technology**
**Golisano College of Computing and Information Sciences Graduate 12 credits**

Program name: Cybersecurity
Students learn to make computers and networks resistant to attack by closing off vulnerabilities and by monitoring intrusions. The application of forensics allows successful attacks on computer systems to be detected. This involves gathering information on the nature and extent of the attack for presentation in a court of law, as well as assessing the extent of the damage to an organization.

**Johns Hopkins University**
**Post Master’s Certificate 6 Courses**
Students in the Cybersecurity program at Johns Hopkins Engineering for Professionals become proficient in ensuring the confidentiality, availability and integrity of data, in preserving and
restoring systems, and in developing risk management skills. State-of-the-art computing facilities and tools are accessible either on-site or online. Combined with knowledge from instructors who are working to fight cybersecurity threats on the front lines, the continually evolving curriculum prepares students for lasting careers in this critical field.

Virginia Tech
Online Graduate Certificate in Information Security and Analytics
Program duration 1 year 12 credits
VT-MIT students have the opportunity to earn one of six graduate certificates as part of their master's degree program. Courses required for each certification are listed below. All certificate courses are either core or elective offerings within the VT-MIT program and count toward the full degree.