Professional Science Masters in

*Cyber Defense and Information Assurance*  
(*CyberDIA*)

Department of Computer and Information Sciences  

College of Science and Technology  

Temple University  

October 2, 2015  

Draft Version (with Revenue Model)

The 2015 *Global Information Security Workforce Study* conducted by Frost & Sullivan, with nearly 140,000 respondents globally, projects that the shortage of global information security workforce will reach an astounding 1,500,000 (1.5 M) in 5 years.
Steering Committee:

Dr. James Du (CST/CIS)
Dr. Krishna Kant (CST/CIS)
Sally Kyvernitis (CST/CIS)
Rose McGinnis (CST/CIS)
Dr. Justin Shi (CST/CIS)
Dr. Avinash Srinivasan (CST/CIS)
Dr. Qiang Zhang (CST/CIS)
Dr. Saroj Biswas (CoE/ECE)
Dr. Li Bai (CoE/ECE)

External Advisory Committee (Tentative):

Mr. Mitch Parker – CISO, TUH, Philadelphia
Mr. Edward Wagner – CISO, SAP National Security Services, D.C.
Dr. Frank Ferrese – Lead Research Engineer, Naval Surface Warfare Center, Philadelphia
Mr. Dave Snyder – Chief Information Security Leader, IBX, Philadelphia
Mr. John Baek – Director of Technical Services, BTB Security, Philadelphia
Mr. Joseph Sciscio – Chief of Police, Penndel Borough, PA
Mr. Joe Menichini – Global Head of Cyber Security, JPMorgan Chase & Co., NYC
# Contents

1 Executive Summary ......................................................... 4

2 Proposed PSM Unique Strategic Point .................................. 5
   2.1 Balanced Curriculum .................................................. 5
   2.2 Key Strengths .......................................................... 5
   2.3 Targeted Professional Certifications ................................. 6

3 Competition – Local and National ....................................... 6

4 Potential Student Pool ...................................................... 7

5 Program Admission Requirements ....................................... 8

6 Program’s Student Learning Outcomes .................................. 8

7 Professional Goals and Career Opportunities ......................... 9
   7.1 Employment Opportunities in the Region for PSM Students ... 11

8 Program Administrative Structure ....................................... 13
   8.1 Steering Committee .................................................... 13
   8.2 External Advisory Committee ....................................... 13

9 Program Resources, Estimated Costs, and Revenue Stream ........ 13
   9.1 Available Program Resources ....................................... 13
   9.2 Estimated Costs (Preliminary estimates) ........................... 14

10 Program Course Requirements .......................................... 16
    10.1 Required Courses .................................................... 16
    10.2 Elective Courses .................................................... 18
    10.3 Project ................................................................ 20
    10.4 Plan of Study, Certificates, and Program Burden ............... 21
1 Executive Summary

Today, our physical and digital worlds are interwoven into a highly complex yet tantalizingly delicate web of interdependence. This web of interdependence is increasingly fading away the distinction between physical and cyberspace infrastructures. Cyber-infrastructures, undoubtedly, enable new business models, enhance communications, makes our personal lives more convenient, and contributes to our national defense. However, on the flip side, this has rendered citizens extremely vulnerable to threats against our cyber-infrastructure, since cybercriminals can inflict crippling blows to pockets or even the entire nation. For instance, network outages, data compromised by hackers, virus distribution, and other incidents affect our lives in ways that can range from mere inconvenience to life-threatening incidents.

Security sectors of both government organizations and business enterprises are highly diverse and involve many levels of job functions, each requiring different specialty, experience, knowledge, and education, which is also confirmed in a recent study conducted by Frost & Sullivan\(^1\). Security professionals, at all levels, must be aware of appropriate and applicable corporate laws in the states in which they provide services, to reduce their vulnerability to liability and financial risk. Corporate security professionals, at all levels, must also possess a variety of skills and specialty training on a continuing basis to effectively and efficiently thwart malicious attempts that threaten organizational resources and employees. Executive level knowledge and awareness of security in the security marketplace demands the highest levels of professionalism, business leadership ethics and discipline, and above all education on a continuing basis. At the highest levels, a Chief Information Security Officer (CISO) must understand the full spectrum of strategic risks to the organization, including financial, physical, and most importantly intangibles such as customer goodwill, patronage, and reputation risk. The C-level executives can no longer dismiss necessary discussions and deny budgetary and personnel requirements of the security technology and management needs.

The objective of this proposal is to propose the establishment of a new Professional Science Master (PSM) program in Cyber Defense and Information Assurance (CyberDIA). The current and projected shortage in cybersecurity workforce is worrisome. Frost & Sullivan projects that the dearth of global information security workforce will reach a staggering 1.5 million in 5 years. This critical need for skilled workforce is so critical that the current administration has issued directives and memorandums emphasizing its support to meet this urgent need. There has also been initiatives adopted at the highest office needing immediate actions to this effect including – the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) - National Cybersecurity Workforce Framework (NCWF) and the National Initiative for Cybersecurity Education (NICE). NICE is intended to establish an operational, sustainable, and continually improving cybersecurity education program for multiple segments of the nation on correct application of sound cyber practices, the success of which will see the enhancement of the overall security posture of the nation. Frost & Sullivan has also confirmed the above facts through an extensive study of organizations reporting on their security workforce issues including recruitment failures, high attrition rates, and lack of skilled candidates, among other things\(^1\). Frost & Sullivan has also studied the participating organizations focus areas for future security workforce needs\(^1\).

\(^1\)2015 Global Information Security Workforce Study.
2 Proposed PSM Unique Strategic Point

The proposed PSM in *Cyber Defense and Information Assurance (CyberDIA)* is designed keeping in mind 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 design of the curriculum is balanced with topics from a multitude of cyberspace domains – primarily focusing on *Network Security* and *Digital Forensics*. The multidisciplinary program design borrows knowledge, skills, and expertise from different academic disciplines including – Computer and Information Sciences, Electrical and Computer Engineering, FOX School of Business, and Beasley School of Law.

2.1 Balanced Curriculum

In designing the CyberDIA program curriculum, the key focus has been on a holistic cybersecurity framework – one that is built around the core principles of preventive, detective, and corrective security mechanisms. While the CyberDIA curriculum is quite technology intensive, significant efforts have been channeled towards bridging the ever-increasing gap between cybersecurity technology and the overarching cybersecurity policies. The curriculum addresses following four core knowledge areas –

1. Technology (60%)
2. Leadership and Ethics (10%)
3. Laws, Regulations, and Governance (15%)
4. Policies, Procedures, and Compliance (15%)

2.2 Key Strengths

The program is designed for aspiring technical professionals at all career levels – entry-level, mid-career, and senior executives – who wish to equip themselves with skills necessary to protect their organization, and the nation as a whole, from increasing cyber-threats. The program is designed for providing students with a broad analytical framework for evaluating and solving cybersecurity problems through a multidisciplinary approach, in which candidates have the option of choosing elective courses across Temple’s academic units including College of Engineering, Beasley School of Law, FOX School of Business, and College of Science and Technology. Through a unique blend of cross disciplinary course work, the CyberDIA PSM will differentiate itself from other such programs both within TU and outside. Some unique courses offered by CyberDIA encompassing a comprehensive knowledge base for cyber defense and information assurance include –

1. Computer Networks
2. Digital Forensics
3. Network Security
4. Cyber-Physical Systems and Critical Infrastructure
5. Systems Security
2.3 Targeted Professional Certifications

Finally, the CyberDIA program is developed to meet the requirements of real-world business enterprises. Hence, it is tailored around the knowledge domains tested in three highly in-demand professional certifications. Therefore, after successful completion of the CyberDIA PSM program, students will be equipped with necessary knowledge, skills and tools to appear for the following professional certifications:

- Certified Ethical Hacker (CEH) – by EC-Council
- Computer Hacking Forensics Investigator (CFHI) – by EC-Council
- Certified Information Systems Security Professional (CISSP) – by ISC²

The critical need for professional certifications has also been reported in the Frost & Sullivan study¹, which is also presented in figure 2, in which 63% of respondents considered it very critical.

3 Competition – Local and National

There are many cybersecurity education programs both locally and nationally, ranging anywhere from online certificates to undergraduate and graduate programs. Some of the top institutions of higher education in the US including – Princeton, Dartmouth, Georgia Tech, Carnegie Mellon and Johns Hopkins – have security programs and designated centers of excellence in information assurance. Regionally, peer institutions including Drexel, Penn State, and U-Penn, all have very strong security programs at various levels and program offerings. Even smaller institutions like West Chester University of PA and Villanova are designated Centers of Academic Excellence (CAE).

In the Philadelphia region, the following programs are available:

<table>
<thead>
<tr>
<th>Institution</th>
<th>Program Offered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drexel University</td>
<td>MS in Cybersecurity</td>
</tr>
<tr>
<td>La Salle University</td>
<td>Graduate Certificate in Cybersecurity</td>
</tr>
<tr>
<td>Penn State Great Valley</td>
<td>Graduate Cyber Security Certificate</td>
</tr>
<tr>
<td>Temple University</td>
<td>UG Certificate in Computer Security and Digital Forensics</td>
</tr>
<tr>
<td></td>
<td>MS in IT Auditing &amp; Cybersecurity (ITACS)</td>
</tr>
<tr>
<td></td>
<td>PSM in Cyber Defense and Information Assurance (CyberDIA)²</td>
</tr>
<tr>
<td>University of Delaware</td>
<td>MS in Cybersecurity</td>
</tr>
<tr>
<td>Villanova University</td>
<td>MS Cybersecurity Engineering</td>
</tr>
<tr>
<td>West Chester University</td>
<td>Undergraduate and Graduate Certificates</td>
</tr>
</tbody>
</table>

Table 1: Cybersecurity and related academic programs in the Philadelphia suburban area.

According to the PSM governing body’s website³, and to the best of our knowledge, as of September 14, 2015, among all the cybersecurity and information assurance programs in the country, only two are offered in the PSM model. These two programs are offered at – California University of PA and University of West Florida. There are a handful of other institutions that have security programs

²This Proposal is to build the CyberDIA program.
³http://www.sciencemasters.com/
but are basically traditional Master of Science program. We believe that this phenomenon could possibly be attributed to the fact that higher education institutions are yet to embrace the field of security and information assurance as a convergence of professional and science disciplines.

Therefore, with this information, Temple University will be the first Carnegie classified “Research Active” institution to establish a PSM in CyberDIA. Such a program will not only be the only one in the Philadelphia metropolitan area and the PA-NJ-DE tristate area, but also the PSM program in the nation. This will allow Temple University to set precedence to other institutions and provide national recognition as a leader in the domain of cybersecurity. One possible explanation to this phenomenon would be the shortage of qualified faculty capable of teaching the subject matters. Cybersecurity and information assurance matters are highly practical and often entangled with business and government rules and regulations. The National Security Agency (NSA) has published standard cybersecurity and information assurance curriculum modules and requirements necessary for an institution to be recognized and designated as a national center of academic excellence.

4 Potential Student Pool

Our pool of potential students is expected to be diverse in age and experience, and from the following broad groups:

- students with undergraduate degrees in STEM disciplines
- professionals seeking an advanced degree
- domestic and international applicants

The steering committee, with help from the external advisory committee, will focus on taking a more strategic approach to recruitment in an effort to attract students who are a right fit for the proposed PSM. Efforts will also be made in association with the Alumni Affairs office towards targeted outreach marketing to population more likely to return to Temple. The CIS department at Temple University has a very strong women students' presence through the “Women in Computing” group and the group attends the Grace Hopper Conference annually in ever-increasing numbers. The steering committee will work with the group’s mentors and other members to recruit potential candidates. This is also a focal point of addressing the dearth of women in cybersecurity.

The CIS department also has other student organizations “TUSec” which primarily focuses on bringing together student enthusiasts looking to further their knowledge in the domain of information and network security. The PSM program director, with support from the external advisory committee, will engage in active outreach with local industries. Alumni relations is another avenue we will actively pursue to recruit previous students. UG students graduating with BA/BS degrees in STEM discipline will be another strong pool we will be able to tap into. Career mentors and academic advisors within CIS and in CST will help publicize the program among the graduating students. Last but not the least, we believe that through word-of-mouth the program will grow given its quality and its benefits to graduating students.

5 Program Admission Requirements

Admittance into the CyberDIA PSM will be based on evidence of a strong academic record and preparation in the STEM disciplines, as well as a demonstrated strong desire to fully engage in the rapidly developing field of Cyber Defense and Information Assurance. Below are the broad requirements that will serve as the guidelines for admission into the program.

- Submit a completed application along with the required application fee (non-refundable), three letters of reference (preferably a mix of both academic and professional), official copy of undergraduate transcripts, and a letter of interest.
- Successfully complete a personal interview with the program director or members of the PSM admissions committee.
- Graduate Record Examination’s (GRE) General Test scores are required from all applicants.
- All international students are required to take the Test of English as a Foreign Language (TOEFL) and submit their score along with the application package.
- International applicants are also required to adhere to any other requirements specified by the Temple University International Student and Scholar Services (ISSS), which can be found at http://www.temple.edu/isss/

6 Program’s Student Learning Outcomes

Upon successful completion of the program, students will be able to demonstrate:

- Knowledge of fundamental principles used to address state-of-the-art methods and technologies to solve problems in cyber defense and information assurance
- An understanding of ethical standards of integrity, honesty and fairness within the Infosec profession
- Professional communication skills for oral and written presentations
- Skills in providing relevant technical support and customer assistance in product development
- Proficiency in collecting, analyzing, documenting and validating data
- Expertise in complying with national, state and local policies, protocols and standards expected in the field
- Leadership abilities to contribute effectively within the profession (e.g., lead lab teams, make development and planning decisions, lead in management and marketing decisions)
- Develop teamwork skills
<table>
<thead>
<tr>
<th>Tool Category</th>
<th>Tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sniffers</td>
<td>Wireshark, Cain and Abel, AirCrack, Snort, NetStubmler</td>
</tr>
<tr>
<td>Exploitation</td>
<td>Web Goat, Metasploit, Social Engineering Tool Kit</td>
</tr>
<tr>
<td>Password Cracking</td>
<td>Cain and Abel and John the Ripper</td>
</tr>
<tr>
<td>IDS</td>
<td>Snort and Bro</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Maltego, Social Engineering Tool Kit</td>
</tr>
<tr>
<td>Scanning and Enumeration</td>
<td>nmap, zemmap, netcat, WebScarab, Nessus, hping, hping2, User2SID, SID2User</td>
</tr>
<tr>
<td>Forensics</td>
<td>WinHex, FTK, HxD, BulkExtractor, The Sleuth Kit, Maltego, NetworkMinerHelix, Metasploit MAFIA, SIFT, FTK Imager, Forensic Replicator, CLI Imaging tools - dd, dcfldd, dc3dd, CLI Hash tools – md5, md5deep</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Ping, Telnet, Dig, Traceroute, whois, netstat, nslookup</td>
</tr>
</tbody>
</table>

Table 2: Security and forensics tools that students will gain hands-on experience and proficiency in using during the course of the proposed CyberDIA PSM program.

7 Professional Goals and Career Opportunities

Technical security professionals, commonly referred as Infosec professionals, are in very high demand today as specified in the Bureau of Labor Statistic’s projections, which is presented in figure ??.

Job titles and descriptions for Infosec professionals vary across industries and organizations listed below ia a representative list of the types of opportunities, which students who successfully complete the proposed CyberDIA PSM could obtain.

- **Security Analyst or Cyber Security Analyst**– These opportunities require an undergraduate technology degree and may require professional certifications. These jobs are often categorized into three sub areas that are technical in nature.
  - Risk Assessment – identifying the problems an organization might face
  - Vulnerability Assessment – determining an organizations weaknesses
  - Defense Planning – Installing protections, firewalls & data encryption

- **Information Security Officer** – Many of these opportunities require CISSP certification as well as a technology degree. Some of the key responsibilities of these opportunities are:
  - Implement and monitor security policies and guidelines – Continuous Monitoring Plan and strategic planning – Implement and maintain incident response and audit programs for events – develop and review test plans and outcomes for user acceptance testing for all applications.

- **Computer Security Forensic Investigator** – Often require a CEH and/or CFHI certification. Responsibilities and duties include:
• **Cyber Security Systems Engineer** – Require a CISSP certification. Furthermore, such opportunities require relevant education and experience in:
  - network security – distributed systems – information security and assurance – cryptography – reverse engineering – digital forensics – enterprise network design – secure operating systems and risk analysis, among other things

• **IT Network Security Penetration Testing** – Opportunities in this job category require a CEH Certification and often a CISSP certification. Some of the key responsibilities of these opportunities are:
  - Technical knowledge of application security – network segregation – access controls – cryptography – physical security – and information security risk management. Skills and knowledge in networking protocols – TCP/IP stack – systems architecture and operating systems. Knowledge of common programming languages and scripting languages is also important.

All of the potential employment opportunities identified above require many of the same soft skills which this PSM program will address within the course content and capstone experience, which are as follows:

• **Strong verbal and written communication skills** – students need to be able to participate in high level organizational meetings, develop and deliver corporate policies, articulate organizational policies to a variety of different users, communicate with vendors and present findings and recommendations both verbally and in writing.

• **Broad Understanding of the Field** – students should have a clear understanding of fundamentals of computer and network security including – the security triad Confidentiality-Integrity-Availability; identify specific core security requirement(s) that a security policy specifies; and implement appropriate security mechanism to achieve the security goal.

• **Awareness of the State-of-the-Art** – students will also develop a clear understanding of the overarching importance of policies and procedures, knowledge of relevant and important cyberspace and information security laws and regulations, and the critical need for cyberspace governance ensuring compliance with secure cyberspace operations. Students will also develop the skill of vulnerability research to locate the latest vulnerabilities and the associated threats.

• **Complex Problem Solving** – ability to identify complex problems and review related information to develop and evaluate options and implement solutions. Students will demonstrate the ability to develop solutions for networking and security problems, balancing business concerns, technical issues and security.

• **Critical Thinking** – students will gain a deep understanding and develop skill sets necessary to identify the appropriate security approach that is needed to protect specific assets from cyber attacks; ability to understand and use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions and approaches to problems.

• **Teamwork** – ability to work collaboratively with many different stakeholders, both internal and external to the organization, to identify the key issues and come to resolution. Students
7.1 Employment Opportunities in the Region for PSM Students

Temple’s CIS department has developed strong relations with many of the major technology employers in the region. These employers are in a diverse set of industries all of which have an increasing need for the positions outlined above. We have communicated our preliminary thoughts with a number of these employers including Protiviti – an IT security consulting firm, and JPMorgan Chase – both of which have hired a number of Temple’s CIS undergraduate students. Upon initial discussions with both of these organizations they see a strong need for the program and would be excited to hire students who complete the program. We anticipate that this would hold true for many of our other employers such as Vanguard, Cigna Insurance, PriceWaterhouseCooper, Deloitte Consulting and Philadelphia Gas Works.

An internet search of job opportunities with the job titles discussed above for the local region provided the following results, we feel confident that they believe are representative of the current need for these types of professionals both today in our region as well as a sample of what the future continuous growth will support – for students willing to relocate, the number of opportunities grows exponentially.

Below are some of the current and frequently interviewed job positions within the information security workforce. This is only a short list for illustration of the demand, and by no means the only positions available.
Figure 2: Frost & Sullivan’s 2015 Global Information Security Workforce Study identifying skill sets contributing to a successful infosec profession in decreasing order of priority.

- **Organizations seeking Security Analyst**
  Lincoln Financial, Deloitte\(^5\), Einstein Health Network, eBay Enterprise, Thomas Jefferson Hospital, Sungard, General Dynamics

- **Organizations seeking Computer Security and Forensic Analysts**
  AmeriHealth, Universal Health Systems\(^5\), Hewlett Packard, UHS of Delaware\(^5\)

- **Organizations seeking Cyber Security Systems Engineer**
  Westinghouse Rail Systems, Lockheed Martin\(^5\), Northrop Grumman

- **Organizations seeking IT Network Security Penetration Testing**
  Verizon, Protiviti\(^5\), Sunoco, QVC\(^5\)

These organizations will also be a strong avenue to recruit students for the CyberDIA PSM program. Additionally, we can target existing technology professionals who want to pursue an information security career or want to enhance their existing skill sets in these areas.

\(^5\)Organizations with which we currently have a strong relationship with the hiring of Temple’s CIS students today.
8 Program Administrative Structure

The proposed PSM program will be administered as follows:

- The CIS department will be the program’s home department. The Steering Committee is responsible for oversight of the program and for communicating and coordinating with both departments to implement the curriculum.

- The CyberDIA PSM committee will oversee the admissions process as well as the monitoring and reporting of student progress. The steering committee will consult with the CIS graduate admissions committee on a need basis.

- The Program Director will be appointed from the ranks of the CIS department, and will be an active researcher, and instructor with CyberIA interests.

- As required for a PSM degree program, a Scientific Advisory Board will be formed that will include appropriate individuals from local industries including hospitals and banks, law enforcement agencies, and research centers.

8.1 Steering Committee

The program Steering Committee includes faculty from the departments of CIS and ECE. The Steering Committee members are responsible for developing and administering the program, in consultation with the home department, the CST, and the Graduate School.

8.2 External Advisory Committee

The Steering Committee will form a Scientific Advisory Committee comprising of experts from Government agencies and corporations representing a broad spectrum of industry verticals including hospitals, banks, law enforcement agencies – federal, state, and local, and research centers including the FBI/Regional Computer Forensics Lab (RCFL) and FBI Philadelphia Cyber Squad’s Incident Response division. While the committee has currently identified potential members, the finalization of the board and its members will be done after final approval of the proposed PSM program in Cyber Defense and Information Assurance.

9 Program Resources, Estimated Costs, and Revenue Stream

9.1 Available Program Resources

Faculty. Course instructors will include faculty from the Departments of Computer and Information Sciences and Electrical and Computer Engineering. Arrangements will be made with each department to determine appropriate teaching load and credits for teaching effort. Faculty research mentors are expected to have active, funded research programs that are relevant to the program. Wherever possible, grant funds will be used to support the capstone research projects.

Instructional and Research Space. The new SERC building has multiple smart instructional classrooms that would be adequate for the program. SERC also has computer labs which could be used for those PSM CyberIA courses which require access to specialized hardware or software that
is used as part of the instructional program. The Tech Center also holds multiple rooms ideal for this program, and in particular, student-led group assignments.

9.2 Estimated Costs (Preliminary estimates).

The program is anticipated to be self-sufficient once a minimum of ten students are enrolled, and a self-sustaining admission rate of at least 5 students per year is attained. The program will require an initial, one-time outlay of resources and there will be recurrent costs. The recurring costs will be paid for by tuition revenue.

One time (initial) Costs:

1. Web page development and maintenance $ 6,000
2. New course development $ 40,000
3. Administrative staff support (1/3 time including fringe) $ 18,000
4. IT staff support $ 10,000
5. Computer hardware and software licenses for computer labs $ 25,000

Estimated total initial costs: $ 99,000

Recurring Costs:

1. Administrative staff support (1/3 time including fringe) $ 18,000
2. Instructional costs (for lecture courses and computer labs) $ 15,000
3. Consumables (office supplies, equipment repair, website maintenance, and license renewal) $ 15,000
4. Faculty Professional Development $ 5,000

Estimated recurring costs: $ 53,000

Program Revenue Stream.

Tuition represents the main revenue stream, and is estimated as follows: 5 students will be admitted each year, and tuition is assumed to be entirely at the in-state rate: at the rate of $646 per credit (out-of-state rate is $933). The tuition revenue reflects a 3% yearly increase in tuition rate per credit. Program year 1 includes 18 credits (cohort-1), and year 2 includes 30 credits (cohort-1 12 credits; cohort-2 18 credits).

In the first year of the program, with 5 students, the program will break even with recurring expenses and will have a modest surplus of $5,000.00. At steady-state, with new students entering the program with each new cohort, tuition revenue will exceed the recurring expenses. In figure 3, we have presented two cases. In the first case, we expect each new cohort starting with the second cohort, will have 7 new students. In the second case, we assume 10 new students in each cohort starting with the second cohort. The year-by-year revenue details can been seen in the figure.
Figure 3: Revenue generated by the proposed CyberDIA PSM program from student tuition revenue. Two scenarios are compared reflecting the impact of even small increase in enrollment reflecting in substantial tuition revenue.
10 Program Course Requirements

Students are required to meet the following credit requirements for successful completion of the PSM program.

<table>
<thead>
<tr>
<th>Required Credits</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elective Credits</td>
<td>12</td>
</tr>
<tr>
<td>Capstone Credits</td>
<td>3</td>
</tr>
<tr>
<td>Total Credits</td>
<td>30</td>
</tr>
</tbody>
</table>

10.1 Required Courses

For this PSM, students are required to take a total of 5 required courses – a total of 15 credits. The required courses are as follows:

1. **CIS 5003. Networking and Operating Systems**  
   
   **Course Catalog Description.** This course covers the essentials of operating systems and computer networks. Topics include: the processor, data and program representation, computer memory systems, software system support for I/O including support for networking, and a thorough introduction to the TCP/IP protocol suite.

2. **CIS 5107. Computer Systems Security & Privacy**  
   
   **Course Catalog Description.** Computer systems security and information privacy has become a critical area of computer science development and research. This course involves an analysis of the technical difficulties of producing secure computer information systems that provide guaranteed controlled sharing and privacy. Emphasis is on software modeling and design to better ensure the protection of resources (including data and programs) from accidental or malicious modification, destruction, or disclosure. Current systems and methods will be examined and critiqued. The possible certification of such systems will also be investigated.

3. **CIS 5405. Introduction to Digital Forensics**  
   
   **Course Catalog Description.** This course is a broad introduction to the field of Digital Forensics. It covers various fundamental topics necessary for digital forensics investigation. The course begins with foundations of electronic evidence including cyber crime laws, the 4th Amendment, compliance and requirements, collection and handling, analysis, and reporting. The course also covers fundamentals of file systems with specific details pertaining to Microsoft FAT file systems. Students will learn two important forensics techniques-file recovery and file carving-among other things. Finally, forensics artifacts relevant to Windows Systems and Networks are discussed with relevant lab activities and students are also introduced to Antiforensics. Hands-on lab activities familiarize students with several relevant investigation techniques and the use of open source forensics tools.
4. **CIS 5415. Ethical Hacking & Intrusion Forensics**  

**Course Catalog Description.** This class teaches students how to use hacking techniques to perform a hack within legal confines. Such hacking is more commonly referred to as a white-hat or an ethical hack. The course will focus on both technical and social aspects of security, ranging from cryptography and biometrics to risk mitigation and disaster recovery aspects of security. Based on the ethical concepts built during the first half of the semester, students will learn the process involved with intrusion attack detection and forensics investigation. Finally, the course will significantly emphasize the key factors that differentiate a hacker (adversary/black-hat) from an ethical hacker, stressing the importance of being within legal confines, an important prerequisite for a successful ethical hacking career.

5. **CIS 5425. Audit & Compliance for Security & Digital Forensics**  

**Course Catalog Description.** This course will provide students with a basic understanding of IT systems and the need for audit and compliance. Students will learn about IT terminology, governance, and the IT audit practice that has matured into given sets of frameworks, methodologies, approaches, and models with certain sets of underlying assumptions such as COBIT and SOX. Students will be exposed to various governance standards and federal compliance requirements.
10.2 Elective Courses

Students are highly recommended to choose up to 12 credits in elective from the list of courses below. However, students can choose courses from other TU graduate programs and discuss the suitability of the course as an elective with the program director. Certain courses may have additional prerequisites, and those prerequisites will not count towards the PSM’s elective credits. Please check with the program director prior to registration. Below is the recommended list of courses that count towards PSM elective credits. All graduate courses can be found by visiting the following link – https://prd-wlssb.temple.edu/prod8/bwckschd.p disp_dyn_sched

1. CIS XXXX Advanced Digital Forensics TBD

**Course Description.** Introduction to the design and analysis of computer networks and communications systems, including the Physical, Data Link, Network, Transport and Application layers. The Internet (TCP/IP) model will be emphasized and compared and contrasted with other current technologies. Major themes include the distinction between service and protocol, performance metrics, analysis techniques, and fundamental performance tradeoffs.

2. CIS XXXX Ethical Hacking & Intrusion Forensics-II TBD

**Course Description.** This class teaches students how to use basic hacking techniques learned in CIS 4615 to perform advanced hacks within legal confines. This course will focus on building further on both technical and social aspects of security ranging from cryptography and biometrics to risk mitigation and disaster recovery aspects of security, that can be leveraged for hacking purposes. Students will also advance their knowledge of forensics investigation process involved with intrusion attacks, and learn to use open source as well as some proprietary tools.

OR

3. MIS 5211 Ethical Hacking Existing

This course introduces student to the hacking strategies and tactics used by ethical or ?White Hat? hackers. Methods of vulnerability exploitation to be used primarily in the process of Security Penetration will be explored in theory and in hands on exercises. The course will require simple programming using Open Source scripting languages and hacking tool kits. For that reason knowledge of and experience with computer programming is required.

3. CIS 5637. Network & Information Security Existing

**Course Catalog Description.** This course introduces fundamental knowledge of cryptography and its applications to network and information security. The topics include Symmetric Encryption and Message Confidentiality, Public Key Cryptography, Authentication, Web Security, Internet Security, Intrusion Detection, Malicious Software, and Firewalls.

**Course Description.** Cyber-Physical Systems (CPS) augment physical systems with monitoring, communication and control capabilities to enhance their efficiency, flexibility, safety, and resilience. While CPS have the potential to address difficult societal problems such as reducing healthcare costs, minimizing traffic congestion, and constructing zero-net energy buildings, they present many challenging problems and opportunities for research. The course will start with an overview of these opportunities and challenges and then gradually explore a few physical systems including their monitoring, communications, control, safety, and security requirements. Some potential systems to be covered include power grid, building management, automotive or other transportation systems, and health-care. The course would then focus on potential attack vectors from physical and cyber ends, and mechanisms to harden state CPS.

5. **CIS 5210. Seminar in Information Science and Technology**

**Course Catalog Description.** An intermediate level graduate special topics course in current and emerging developments in information systems and technology.

**Special Note:** This course can only be taken with prior approval of the PSM committee and the program director. Student has to provide in writing the need for taking this course, its relevance, and potential impact from the course on the student’s professional career, which could otherwise be not met by other suggested electives. Then the program director, in consultation with the committee, will evaluate the student’s request and make a decision. The primary reason if to avoid letting students take topics that are not relevant or less technical in place of other needed knowledge domains that help meet the program’s **Student Learning Outcome (SLO).**

6. **CIS 9182/9282. Independent Study**

**Course Catalog Description.** Independent research supervised by a Computer and Information Sciences faculty member.

**Special Note:** This course can only be taken with prior approval of the PSM committee and the program director. Student has to provide in writing the need for taking this course, its relevance, and potential impact from the course on the student’s professional career, which could otherwise be not met by other suggested electives. Then the program director, in consultation with the committee, will evaluate the student’s request and make a decision. The primary reason if to avoid letting students take topics that are not relevant or less technical in place of other needed knowledge domains that help meet the program’s **Student Learning Outcome (SLO).**
7. ECE 5528. Introduction to Cryptography and Information Security

Course Catalog Description. This course covers the theory and practice of computer communications security. Topics include symmetric encryption, public and private key cryptography, message digests, digital signatures, secure email, and various types of authentication methods. We will review various cryptographic primitives, algorithms, intrusion attacks, and security protocols.

8. LAW 0433. Cyberspace

Course Catalog Description. The goal of this course is to introduce students, by means of a series of specific case studies chosen to illustrate the clash between existing legal regimes and new technologies, to a reasonably comprehensive subset of the legal problems that are being addressed as part of the developing "online law." Topics to be covered include the law of copyright as applied to electronic information, trademark law as applied to Internet "domain names," application of the First Amendment to the regulation of Internet communications, privacy concerns on the Internet, the law of anonymous communication and the regulation of encryption technology, and the difficult international jurisdictional questions presented by Internet activity. Although it is not a prerequisite, it is strongly recommended that students have had a course on intellectual property prior to enrolling in this course.

10.3 Project

Students are required to complete a group capstone project, worth 3 credits, for successful completion of the PSM program.

1. CIS XXXX. Capstone in Cyber Defense and Information Assurance

Each student would be given a real security problem. Phase one would include identifying the compliance bit: Identifying how the security problem affects the organization and what regulations/standards are to be considered. Phase two would be the technical piece: Identify network and application vulnerabilities, performing forensics (chain of custody) and document the findings. Phase three would be to present all the findings from phases one and two to the executive body of the affected organization and the faculty mentor(s).
10.4 Plan of Study, Certificates, and Program Burden

<table>
<thead>
<tr>
<th></th>
<th>YEAR 1</th>
<th>YEAR 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fall</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 5003</td>
<td>Networking and Operating Systems</td>
<td>CIS XXXX</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Audit and Compliance for Security and Digital Forensics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>CIS XXXX</td>
<td>Introduction to Digital Forensics</td>
<td>CIS XXXX</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Elective-3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>CIS XXXX</td>
<td>Elective-1</td>
<td>CIS XXXX</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Elective-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

|                  |                                                                        |
| **Spring**       |                                                                        |
| CIS XXXX         | Ethical Hacking and Intrusion Forensics                                | CIS XXXX                                                             |
|                  | 3                                                                      | Capstone                                                             |
|                  |                                                                        | 3                                                                     |
| CIS 5107         | Introduction to Computer and Network Security.                         |                                                                        |
|                  | 3                                                                      |                                                                        |
| CIS XXXX         | Elective-2                                                             |                                                                        |
|                  | 3                                                                      |                                                                        |
| **Total**        | 9                                                                      |                                                                        |

Figure 4: Sample plan of study for the proposed CyberDIA PSM.
Figure 5: Courses that are recommended for each of the three certificates that students can potentially obtain upon successful completion of the CyberDIA PSM.

<table>
<thead>
<tr>
<th>Course</th>
<th>CEH</th>
<th>CHFI</th>
<th>CISSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS 5003 Networking and Operating Systems</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CIS 5107 Computer Systems Security and Privacy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CIS 5405 Intro to Digital Forensics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CIS 5415 Ethical Hacking &amp; Intrusion Forensics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CIS 5425 Audit &amp; Compliance for Security &amp; Digital Forensics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CIS XXXX Capstone</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Required PSM Courses**

<table>
<thead>
<tr>
<th>Course</th>
<th>CEH</th>
<th>CHFI</th>
<th>CISSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS XXXX Advanced Digital Forensics</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CIS XXXX Ethical Hacking &amp; Intrusion Forensics-II</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CIS 5637. Network &amp; Information Security</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>CIS 5435 Security in Cyber Physical Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIS 5210. Seminar in IST</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECE 5528 Intro to Cryptography and Info Security</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>LAW 0433 Cyberspace</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>LAW 0478 Cyberprivacy Law</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**Elective PSM Courses**