

# ONE-STEP ACADEMIC PROGRAM PROPOSAL

**Institution:** Columbus State University

**Date Completed at the Institution:** March 29, 2017

**Name of Proposed Program/Inscription:** M.S. Cybersecurity Management

**Degree:** Master of Science

**Major:** Cybersecurity Management

**CIP Code:** 11.100

**Anticipated Implementation Date:** Summer 2017 or Fall 2017

**Delivery Mode (check the most appropriate delivery mode in the box below):**

On-campus, face-to-face only	
Off-campus location, face-to-face only (specify the location):	
Online Only	xxx
Combination of on-campus and online (specify whether 50% or more is offered online for SACS-COC )	
Combination of off-campus and online (specify whether 50% or more is offered online for SACS-COC)	
Hybrid, combination delivery, but less than 50% of the total program is online based on SACS-COC	
Contractual Location (specify the location):	

**School/Division/College:** Turner College of Business

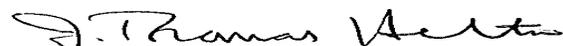
**Department:** TSYS School of Computer Science

**Departmental Contact:** Wayne Summers

**Approval by President or Vice President for Academic Affairs:**



**Approval by Vice President for Finance/Business (or designee) and contact information:**



**Approval by Vice President for Facilities (if different from VP- Finance or designee) and contact information:**

# ONE-STEP ACADEMIC PROGRAM PROPOSAL

- 1) **Rationale:** Provide the rationale for proposing the new academic program.

More than [209,000 cybersecurity jobs](#) in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics. U.S. News and World Report ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015. They state that the profession is growing at a rate of 36.5% through 2022. Faced with the growing threat of cyber-attacks, organizations are increasingly looking for qualified cybersecurity personnel to manage the protection of information and infrastructure.

Columbus Georgia is home to several multinationals (AFLAC, TSYS) and several other major financial services corporations (Synovus Banking, Regions Bank, Omega Fi), all which have a fundamental need for secure systems. All five named companies are members of our TSYS Cyber Security Center Development Team. It was discussions with the security teams and alumni from these companies and others that provided the impetus for this proposed program.

The Master of Science in Cybersecurity Management offered by the TSYS School of Computer Science provides students with the opportunity to join the cybersecurity workforce as well-qualified professionals. Students will learn how to protect critical information infrastructures by developing, implementing and maintaining appropriate cybersecurity policies and practices to help prevent, detect and eliminate security threats. Students will be able to graduate with a Master of Science degree in Cybersecurity Management at Columbus State University by completing thirty credit hours over a period of eighteen months.

- 2) **Mission Fit and Disciplinary Trends:** Description of the program's fit with the institutional mission and nationally accepted trends in the discipline (explain in narrative form). If the program is outside of the scope of the institutional mission and sector, provide the compelling rationale for submission.

Columbus State University's mission is to "...empower people to contribute to the advancement of our local and global communities through an emphasis on excellence in teaching and research, life-long learning, cultural enrichment, public-private partnerships, and service to others". This proposal is in direct response to the community's need for cybersecurity professionals as articulated by our five corporate partners on the Cybersecurity Center Development Team. Through the Cybersecurity Management Masters, our students will be empowered to help defend our cyber networks both in the local and global communities.

- 3) **Description and Objectives:** Program description and objectives (explain in narrative form).

All graduates in the MS in Cybersecurity Management program offered by the TSYS School of Computer Science will learn the essential skills necessary to join the cybersecurity workforce at mid to upper level management. Graduates will be able to:

- Identify threats to and vulnerabilities of information systems;

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

- Formulate policies for the protection of information in compliance with prevailing standards, legal frameworks and best practices;
- Manage the implementation of policies to help prevent, detect and eliminate security threats;
- Oversee the use of technologies to mitigate threats and reduce risks to information systems.

4) **Need:** Description of the justification of need for the program. (Explain in narrative form why the program is required to expand curricular academic offerings at the institution, the data to provide graduates for the workforce, and/or the data in response to specific agency and/or corporation requests in the local or regional area.)

With over 200,000 cybersecurity positions available nationally including thousands in Georgia, and 50-100 locally, the demand far outstrips the limited supply of graduates with cybersecurity degrees produced by the University System of Georgia. Recent job postings on Glassdoor.com and Indeed.com illustrate this.

Type/Title of Position	Number of Anticipated Position Openings	Average Starting Salary	Source
Cybersecurity Analyst	27 (Columbus), 420 (GA), 6,163 (US)	\$62,641 (Columbus) \$70,000 (US)	Glassdoor.com
Cybersecurity engineers	10 (Columbus), 387 (GA), 6,163 (US)	\$83,336 (Columbus) \$85,000 (US)	Glassdoor.com
Information Security Specialist	10 (Columbus), 965 (GA), 29,527 (US)	\$69,602 (Columbus) \$89,458 (US)	Glassdoor.com
Cyber Security	32 (Columbus), 1044 (GA), 34,241(US)	\$69,602 (Columbus) \$89,458 (US)	Indeed.com

The Cybersecurity Supply/Demand Heat Map developed for the Department of Homeland Security at <http://cyberseek.org/heatmap.html> claims that the TOTAL CYBERSECURITY JOB OPENINGS at the National level are 348,975; 12,783 in Georgia, and 597 in Columbus, GA (only Atlanta Metro has a higher demand in Georgia.)

5) **Demand:** Description of how the program demonstrates demand. (Explain in narrative form the data that supports demand for the program from existing and potential students and requests from regional industries.)

As a master’s level degree, this program is within the scope of Columbus State University’s mission as a state institution.

The M.S. in Cybersecurity Management is a direct result of the growing need of local companies for trained professionals in cybersecurity. The security officers from one of these companies have expressed frustration for two years over the inability to hire adequately prepared professionals to

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

fill the more than twenty open positions in cybersecurity in his company. "Cybersecurity job postings grew 114 percent from 2011 to 2015, with 86 percent of the jobs requiring at least a bachelor's degree, according to Burning Glass Technologies, a job-market-analytics company. Colleges are meeting only about 24 percent of the entry-level demand for those with four-year degrees." [The Chronicle of Higher Education, February 26, 2017]

- 6) **Duplication:** Description of how the program does not present duplication of existing academic offerings in the geographic area and within the system as a whole. If similar programs exist, indicate why these existing programs are not sufficient to address need and demand in the state/institution's service region and how the proposed program is demonstrably different.

There currently exist four cybersecurity programs at the post-baccalaureate level in the USG:

Georgia Tech offers a M.S. in Information Security. This a highly technical degree. "Admission to the MS InfoSec degree program is highly selective. ... A strong background in computer science, including C programming and discrete math, is highly recommended for all applicants." Twelve students graduated in FY16.

Georgia State offers a Master of Science in Information Systems with a Cybersecurity Concentration. Enrollment has increased from six in FY13 to 34 in FY16. Since this is a concentration, students are required to take only a few security courses.

Kennesaw State and Columbus State both offer graduate certificates in cybersecurity (in FY16, Kennesaw awarded three and Columbus State awarded nine certificates to six students.) Columbus State offers a Master of Science in Applied Computer Science with an Information Assurance / Cybersecurity Concentration. With certificates and concentrations, students are required to take only a few security courses.

The proposed Masters in Cybersecurity Management is unique. It is a complete 30-credit (ten course) Masters that blends the technical expertise gained from the CPSC Computer Science courses with the newly designed CSMT Cybersecurity Management courses. The curriculum is designed to provide opportunities for IT professionals who want to change careers into cybersecurity management, but lack the background in business. Similarly, the curriculum provides opportunities for business professionals who lack the technical expertise. Graduates from the Masters in Cybersecurity Management will be able to fill a wide variety of high demand job openings in cybersecurity.

- 7) **Collaboration:** Is the program in collaboration with another USG Institution, TCSG institution, private college or university, or other entity?  
Yes \_\_\_ or No xxx (place an X beside one)

Columbus State University is part of the Cybersecurity Initiative created by the USG to focus on all of the cyber education and training resources across the USG in order to meet the needs of the United States Army Cyber Command, the National Security Agency, the financial transaction

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

processing industry, and the health informatics/electronic medical records industry. The initiative aims to create a cyber security workforce of sufficient scale, quality, and capability to meet the needs of Georgia companies, military installations, government agencies, and other institutions."

If yes, list the institution below and include a letter of support from the collaborating institution's leadership (i.e., President or Vice President for Academic Affairs) for the proposed academic program in the appendix.

- 8) **Forecast:** If this program was not listed on your academic forecast for the 2016 - 2017 academic year, provide an explanation concerning why it was not forecasted, but is submitted at this time.

This program was listed in the Turner College of Business strategic plan and the CSU academic forecast submitted to the Board of Regents for 2016-2017.

- 9) **Admission Criteria:** List the admission criteria for the academic program.
- a) Include all required minima scores on standardized tests.
  - b) Include the required grade point average requirement.

### Admission Requirements

Requirements for admission into the program for the Master of Science in Cybersecurity Management include the following:

A four-year undergraduate degree from an accredited institution with a minimum 3.0 cumulative GPA,

AND

A minimum combined score of 290 on the verbal and quantitative sections of the GRE, OR a minimum score of 410 of GMAT.

[The GRE/GMAT requirement **may be waived** for applicants with a graduate degree or four years of approved industrial work experience.]

# ONE-STEP ACADEMIC PROGRAM PROPOSAL

## 10) Curriculum (See the form below this series of questions and please complete.)

- a) List the entire course of study required to complete the academic program. Include the course prefixes, course numbers, course titles, and credit hour requirement for each course. Indicate the word “new” beside new courses.

### Cybersecurity Management Program

#### REQUIRED COURSES (18 CREDITS)

- CPSC6126 Introduction to Cybersecurity (3 credits)
- **(new)** CSMT6222 Foundation of Cybersecurity Policy and Management (3 credits)
- CPSC6136 Human Aspects of Cybersecurity [Pre-req.=CPSC6126] (3 credits)
- CPSC 6157 Computer Network and Management (3 credits)
- CPSC6159 Cybersecurity Investigations and Crisis Management [Pre-req.=CPSC6126] (3 credits)
- CPSC6167 Cybersecurity Risk Management [Pre-req.=CPSC6126] (3 credits)

#### PROGRAM ELECTIVES (choose two) (6 CREDITS)

##### TECHNICAL ELECTIVES *(Recommended for students with non-technical background)*

- **(new)** CSMT6223 Enterprise Information Security [Pre-req.=CPSC6126] (3 credits)
- **(new)** CSMT6226 Cloud Computing Security [Pre-req.=CPSC6126] (3 credits)
- **(new)** CSMT6228 Global Cybersecurity [Pre-req.=CPSC6126] (3 credits)

##### NON-TECHNICAL ELECTIVES *(Recommended for students with technical background)*

- MSOL 6115. Organizational Behavior and Leadership (3 credits)
- MSOL 6155. Strategic Leadership and Change Management (3 credits)

#### PROGRAM CAPSTONE (Choose thesis or project; repeat to total 6 credits) (6 Crs)

- **(new)** CSMT6299 Capstone in Cybersecurity Policy and Management [Pre-req. =CPSC6136] (3 credits)
- CPSC6985. Research and Thesis (3 credits)

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

- b) Provide a sample program of study that includes the course prefixes, course numbers, and course titles and credit hour requirement for each course. Indicate the word “new” beside new courses.

### FULL-TIME (9 credits/semester; summer 3-6 credits)

Semester	Recommended Courses
FALL	<ul style="list-style-type: none"> <li>• CPSC6126 Introduction to Cybersecurity (3 credits)</li> <li>• (new) CSMT6222 Foundation of Cybersecurity Policy and Management (3 credits)</li> <li>• CPSC 6157 Computer Network and Management (3 credits)</li> </ul>
SPRING	<ul style="list-style-type: none"> <li>• CPSC6136 Human Aspects of Cybersecurity [Pre-req.=CPSC6126] (3 credits)</li> <li>• CPSC6159 Cybersecurity Investigations and Crisis Management [Pre-req.=CPSC6126] (3 credits)</li> <li>• CHOOSE ELECTIVE (3 credits)</li> </ul>
SUMMER	CHOOSE 1 FROM: <ul style="list-style-type: none"> <li>• (new) CSMT6299 Capstone in Cybersecurity Policy and Management [Pre-req. =CPSC6136] (3 credits)</li> <li>• CPSC6985. Research and Thesis (3 credits)</li> </ul>
FALL	<ul style="list-style-type: none"> <li>• CPSC6167 Cybersecurity Risk Management [Pre-req.=CPSC6126] (3 credits)</li> <li>• CHOOSE ELECTIVE (3 credits)</li> <li>• CHOOSE 1 FROM:               <ul style="list-style-type: none"> <li>○ (new) CSMT6299 Capstone in Cybersecurity Policy and Management [Pre-req. =CPSC6136] (3 credits)</li> <li>○ CPSC6985. Research and Thesis (3 credits)</li> </ul> </li> </ul>

### PART-TIME (6 credits/semester; summer 3 credits)

Semester	Recommended Courses
FALL	<ul style="list-style-type: none"> <li>• CPSC6126 Introduction to Cybersecurity (3 credits)</li> <li>• (new) CSMT6222 Foundation of Cybersecurity Policy and Management (3 credits)</li> </ul>
SPRING	<ul style="list-style-type: none"> <li>• CPSC6136 Human Aspects of Cybersecurity [Pre-req.=CPSC6126] (3 credits)</li> <li>• CPSC6159 Cybersecurity Investigations and Crisis Management [Pre-req.=CPSC6126] (3 credits)</li> </ul>
SUMMER	<ul style="list-style-type: none"> <li>• CHOOSE ELECTIVE (3 credits)</li> </ul>
FALL	<ul style="list-style-type: none"> <li>• CPSC 6157 Computer Network and Management (3 credits)</li> <li>• CPSC6167 Cybersecurity Risk Management [Pre-req.=CPSC6126] (3 credits)</li> </ul>
SPRING	<ul style="list-style-type: none"> <li>• CHOOSE ELECTIVE (3 credits)</li> <li>• CHOOSE 1 FROM:               <ul style="list-style-type: none"> <li>○ (new) CSMT6299 Capstone in Cybersecurity Policy and Management [Pre-req. =CPSC6136] (3 credits)</li> <li>○ CPSC6985. Research and Thesis (3 credits)</li> </ul> </li> </ul>
SUMMER	CHOOSE 1 FROM: <ul style="list-style-type: none"> <li>• (new) CSMT6299 Capstone in Cybersecurity Policy and Management [Pre-req. =CPSC6136] (3 credits)</li> <li>• CPSC6985. Research and Thesis (3 credits)</li> </ul>

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

- c) List and reference all course prerequisites for required and elective courses within the program. Include the course prefixes, numbers, titles, and credit hour requirements.

NO ADDITIONAL PREREQUISITES

- d) State the total number of credit hours required to complete the program, but do not include orientation, freshman year experience, physical education, or health and wellness courses per the Academic and Student Affairs Handbook, Section 2.3.1.

30 CREDIT HOURS

### Program of Study Form

Courses <i>(list acronym, number, and title)</i>	Semester	Hours
<p><b>Area 1: Program Core</b></p> <p>CPSC6126 Introduction to Cybersecurity</p> <p>CSMT6222 Foundation of Cybersecurity Policy and Management</p> <p>CPSC6136 Human Aspects of Cybersecurity</p> <p>CPSC 6157 Computer Network and Management</p> <p>CPSC6159 Cybersecurity Investigations and Crisis Management</p> <p>CPSC6167 Cybersecurity Risk Management</p>		18 credits
<p><b>Area 2: Program Elective (choose two)</b></p> <p><b>TECHNICAL ELECTIVES</b> <i>(Recommended for students with non-technical background)</i></p> <p>CSMT6223 Enterprise Information Security</p> <p>CSMT6226 Cloud Computing Security</p> <p>CSMT6228 Global Cybersecurity</p> <p><b>NON-TECHNICAL ELECTIVES</b> <i>(Recommended for students with technical background)</i></p> <p>MSOL 6115. Organizational Behavior and Leadership</p> <p>MSOL 6155. Strategic Leadership and Change Management</p>		6 CREDITS
<p><b>Area 3: Capstone (Choose thesis or project; repeat to total 6 credits (take one choice twice)</b></p> <p>CSMT6299 Capstone in Cybersecurity Policy and Management</p> <p>OR</p> <p>CPSC6985. Research and Thesis</p>		6 CREDITS
<b>Total Semester Credit Hours</b>		30

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

- e) If this is a doctoral program, provide the names of four external reviewers of aspirational or comparative peer programs complete with name, title, institution, e-mail address, and telephone number. External reviewers must hold the rank of associate professor or higher in addition to other administrative titles.

N/A

- f) If internships, assistantships, or field experiences are required to complete the academic program, provide information documenting internship or field experience availability and how students will be assigned, supervised, and evaluated.

N/A

- g) Within the appendix, append the course catalog descriptions for new courses. Include the course prefixes, course numbers, course titles, and credit hour requirements.

- 11) **Waiver to Degree-Credit Hour** (if applicable): State whether semester credit-hours exceed maximum limits for the academic program and provide a rationale.

N/A

- 12) **Student Learning Outcomes:** Student Learning outcomes and other associated outcomes of the proposed program (provide a narrative explanation).

All graduates in the MS in in Cybersecurity Management program offered by the TSYS School of Computer Science will learn the essential skills necessary to join the cybersecurity workforce at mid to upper level management. Graduates will be able to:

- Identify threats to and vulnerabilities of information systems;
- Formulate policies for the protection of information in compliance with prevailing standards, legal frameworks and best practices;
- Manage the implementation of policies to help prevent, detect and eliminate security threats;
- Oversee the use of technologies to mitigate threats and reduce risks to information systems.

- 13) **Assessment and Quality:** Describe institutional assessments throughout the program to ensure academic quality, viability, and productivity as this relates to post-approval enrollment monitoring, degree productivity, and comprehensive program review.

All academic programs are reviewed annually to assess the program outcomes and student learning outcomes. Students completing the Masters in Cybersecurity Management are required to complete either a thesis or a capstone project, which require multiple reviewers. In both cases, the course objectives will encompass the student learning outcomes for the program. In addition, the M.S. in Cybersecurity Management will be assessed as part of the Comprehensive Program Review.

- 14) **Accreditation:** Describe disciplinary accreditation requirements associated with the program (if applicable, otherwise indicate NA).

N/A

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

- 15) **Enrollment Projections:** Provide projected enrollments for the program specifically during the initial years of implementation.
- a) Will enrollments be cohort-based? Yes \_\_\_ or NoXXX\_(place an X beside one)
  - b) Explain the rationale used to determine enrollment projections.

Our Master of Science in Applied Computer Science (MSACS) receives over 250 applications each year with about 50% of the applicants accepted; about 2/3 of the accepted applicants register for classes. About 50% of those accepted and registered are required to take one or two foundation courses in computer science. Only about 2/3 of the students who take these foundation classes earn at least a grade of 'B'.

We anticipate about 40-70 applicants the first year. With higher GPA and GRE requirements, we hope to select 20-35 applicants, 10-20 who will start classes in Fall 2017. In addition, we expect at least 3-5 of the MS-ACS students to switch for a total of 13-25 students the first year. We anticipate the numbers to double to 20-40 new students the second year and stabilize at 50 new students in subsequent years. From our experience with the MS programs, we assume that 40-50% of the graduate students will complete their degree requirements within two years.

	First FY2018	Second FY2019	Third FY20 20	Fourth FY202 1
<b>I. ENROLLMENT PROJECTIONS</b>				
<b>Student Majors</b>				
Shifted from other programs	3-5	5		
New to the institution	10-20	20-40	20-40	50
<b>Total Majors</b>	13-25	35-65	50-75	75-100
<b>Course Sections Satisfying Program Requirements</b>				
Previously existing	4-6	5-9	9-15	9-15
New	1-3	1-5	2-8	2-8
<b>Total Program Course Sections</b>	5-7	6-12	11-17	11--17
<b>Credit Hours Generated by Those Courses</b>				
Existing enrollments				
New enrollments	150	320	370	600
<b>Total Credit Hours</b>	450	960	1110	1800

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

### 16) Faculty

- a) Provide the total number of faculty members that will support this program: 8
- b) Provide an inventory of faculty members directly involved with the administration and instruction of the program. Annotate in parentheses the person who holds the role of department chair. For each faculty member listed, provide the information below in tabular form. Indicate whether any positions listed are projected new hires and currently vacant. (Multiple rows can be added to the table.) *Note: The table below is similar to the SACS-COC faculty roster form.*

Faculty Name	Rank	Courses Taught (including term, course number & title, credit hours (C, UN, UT, G))	Academic Degrees & Coursework (relevant to courses taught, including institution & major; list specific graduate coursework, if needed)	Current Workload	Other Qualifications & Comments (related to courses taught)
Radhouane Chouchane	Associate Professor	<p><b>Summer 2016</b>                      CPSC 1302, Computer Science II, 3.0 (UT)                      CPSC 6000, Graduate Exit Exam (G)                      CPSC 6899, Independent Study, 3.0 (G)</p> <p><b>Fall 2016</b>                      CPSC 1302, Computer Science II, 3.0 (UT)                      CPSC 6125, Advanced Operating Systems, 3.0 (G)  <b>CPSC 6126, Info Systems Assurance, 3.0 (G)</b></p> <p><b>Spring 2017</b>  <b>CPSC 3106, Info Security Risk Assessment, 3.0 (UT)</b>                      CPSC 3125, Operating Systems, 3.0 (UT)</p>	<p>Ph.D. Computer Science, University of Louisiana at Lafayette</p> <p>M.S. Applied Computer Science, Columbus State University</p> <p>B.S. Mathematics, Faculte des Sciences deTunis</p>	9 credit hours per semester	
Shamim Khan	Professor	<p><b>Summer 2016</b>                      CPSC 2555, Selected Topics in Comp Sci, 3.0 (UT)                      CPSC 5555U, Selected Topics in Comp Sci, 3.0 (UT)                      CPSC 6985, Research and Thesis, 3.0 (G)</p> <p><b>Fall 2016</b>                      CPSC 1301L, Computer Science I, 1.0 (UT)                      CPSC 3125, Operating Systems, 3.0 (UT)                      CPSC 4505, Undergraduate Research, 3.0 (UT)</p>	<p>Ph.D. Computer Science, University of Manchester, UK</p> <p>M.S. Applied Physics &amp; Electronics, Rajshahi University</p> <p>B.S. Applied Physics &amp; Electronics; Rajshahi University</p>	9 credit hours per semester	<p>Quality Matters Applying the QM Rubric (APP) Certificate, Quality Matters Program (<a href="http://www.qmprogram.org">http://www.qmprogram.org</a>)</p> <p>Certified Tester Foundation Level, American Software Testing Qualifications Board, ASTQB</p>

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

		<p>CPSC 6000, Graduate Exit Exam (G)  <b>CPSC 6178, Sftware Test &amp; Quality Assuran, 3.0 (G)</b></p> <p><b>Spring 2017</b>  CPSC 1301L, Computer Science I, 1.0 (UT)  CPSC 5135G, Programming Languages, 3.0 (G)  CPSC 5185U, Artificial Intelligence, 3.0 (UT)</p>			Software Testing Certification
Yesem Kurt-Peker	Assistant Professor	<p><b>Summer 2016</b>  <b>CPSC 2106, Information Security, 3.0 (UT)</b></p> <p><b>Fall 2016</b>  CPSC 1301, Computer Science I, 3.0 (UT)  <b>CPSC 2106, Information Security, 3.0 (UT)</b>  <b>CPSC 3108, Defensive Programming, 3.0 (UT)</b>  <b>CPSC 6899, Independent Study, 3.0 (G)</b>  <b>CPSC 6985, Research and Thesis, 3.0 (G)</b></p> <p><b>Spring 2017</b>  <b>CPSC 2106, Information Security, 3.0 (UT)</b>  <b>CPSC 4160, Applied Cryptography, 3.0 (UT)</b>  <b>CPSC 6899, Independent Study, 3.0 (G)</b>  <b>CPSC 6985, Research and Thesis, 3.0 (G)</b></p>	<p>Ph.D. Mathematics, Cryptography, Indiana University - Bloomington</p> <p>M.S. Mathematics, Middle East Technical University</p> <p>B.S. Computer Engineering, Middle East Technical University</p> <p>B.S. Mathematics, Middle East Technical University</p> <p><b>Relevant Coursework:</b> MATH-M 553 Cryptography, 3  CSCI-A 592 Intro to Software Systems, 3  CSCI-A 593 Computer Structures, 3  CSCI-P 573 Scientific Computing, 3  CSCI-A 547 Network Tech and Admin, 3  CSCI-B 673 Adv Scientific Computing, 3  CSCI-A 548 Mastering the World-Wide Web, 3</p>	9 credit hours per semester	GIAC Certified Incident Handler (GCIH) from SANS Institute(2016)
Lydia Ray	Associate Professor	<p><b>Summer 2016</b>  <b>CPSC 6159, Computer Forensics, 3.0 (G)</b>  <b>CPSC 6985, Research and Thesis, 3.0 (G)</b></p> <p><b>Fall 2016</b>  CPSC 1302, Computer Science II, 3.0 (UT)  <b>CPSC 2106, Information Security, 3.0 (UT)</b>  <b>CPSC 6136, Advanced System Security, 3.0 (G)</b></p>	<p>Ph.D. Computer Science, Louisiana State University</p> <p>M.S. Statistics, Indian Statistical Institute</p> <p>B.S. Statistics, University of Calcutta</p>	9 credit hours per semester	<p>Computer Forensic Boot Camp (2007)</p> <p>EnCase ® V6 Computer Forensics II (2010)</p> <p>SANS Institute certification in Penetration testing(2016)</p>

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

		<p><b>CPSC 6985, Research and Thesis, 3.0 (G)</b></p> <p><b>Spring 2017</b>            CPSC 1302, Computer Science II, 3.0 (UT)            CPSC 4899, Independent Study, 3.0 (UT)            CPSC 6167, Network Risk Assessment, 3.0 (G)</p>			
Wayne Summers	Professor (Chairperson )	<p><b>Summer 2016</b>            CPSC 3165, Professionalism in Computing, 3.0 (UT)            CPSC 4205, Senior Project &amp; Portfolio, 3.0 (UT)            CPSC 4698, Internship in Computer Science, 3.0 (UT)</p> <p><b>Fall 2016</b>            CPSC 1301, Computer Science I, 3.0 (UT)            CPSC 4000, Baccalaureate Survey (UT)</p> <p><b>Spring 2017</b>            CPSC 1302, Computer Science II, 3.0 (UT)            CPSC 469823305, Internship in Computer Science, 3.0 (UN)</p>	<p>Ph.D. Math (Dissertation CS), St. Louis U.</p> <p>M.S. Math St. Louis U.            B.S. Math Ohio State U</p> <p><b>Relevant Coursework (27 hrs)</b>            MT 478 Data Analysis, 3            MT 468 Sel. Topics/Computer Math, 3            MT 699 Dissertation Research, 13            COMSC 5964 Structured COBOL, 4            COMSC 5964 Database Processing, 4</p>	3-6 credits/sem	<p>Conducted computer security workshops internationally;</p> <p>taught faculty workshops for NSF and NSA</p>
Lixin Wang	Associate Professor	<p><b>Fall 2016</b>            CPSC 1301, Computer Science I, 3.0 (UT)            CPSC 3165, Professionalism in Computing, 3.0 (UT)            CPSC 6119, Obj-Orient Dev w/Components, 3.0 (G)</p> <p><b>Spring 2017</b>            CPSC 5127U 22210, Comp &amp; Network Sec, 3.0 (UT)            CPSC 6109, Advanced Algorithms, 3.0 (UT)            CPSC 611920293, Obj-Orient Dev w/Components, 3.0 (G)</p>	<p>Ph.D. Computer Science, Wireless Networking; Algorithm Design and Analysis, Illinois Institute of Technology</p> <p>M.S. Computer Science, Applied Computer Science, University of Houston - Clear Lake</p> <p>M.S. Applied Math, University of Houston - Main Campus</p> <p>M.S. Math, Fudan University</p> <p>B.S. Math, Hunan Normal University</p>	9 credit hours per semester	

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

Paul Wang	Professor	<p><b>Fall 2016</b>            CPSC 6107, Modeling and Simulation, 3.0 (G)            CPSC 6126, Information Systems Assurance, 3.0 (G)            WBIT 3500, Operating Systems, 3.0 (U)</p> <p><b>Spring 2017</b>            CPSC 1302, Object Oriented Programming, 3.0 (G)            CPSC 4899, Independent Study - cybersecurity, 3.0 (G)            CPSC 6126, Information Systems Assurance, 3.0 (G)            CPSC 6157, Network Management and Operation, 3.0 (G)</p>	<p>Ph.D. IT/CS, 3D Imaging, George Mason University</p> <p>M.S. CS, Southwestern Jiaotong University</p>	9 credit hours per semester	<p>Information Security for Executives Certification, National Institute of Health (NIH).</p> <p>Certified Information Systems Security Professional (CISSP) Training Certification.</p> <p>CIO/CTO at National BioMedical Research Foundation</p>
Jianhua Yang	Professor	<p><b>Summer 2016</b>            CPSC 5157G, Computer Networks, 3.0 (G)</p> <p><b>Fall 2016</b>            CPSC 5157U, Computer Networks , 3.0 (U)            CPSC 6105, Fundamental Principles of Computer Science, 3.0 (G)</p> <p><b>Spring 2017</b>            CPSC 6105, Fund Principles of Comp Sci, 3.0 (G)            CPSC 6128, Network Security, 3.0 (G)            CPSC 6175, Web Engineering/Technology, 3.0 (G)</p>	<p>Ph.D. Computer Science, Information Assurance, University of Houston</p> <p>M.S., Computer Engineering, Computer signal processing, Shandong University</p> <p>B.S. Electronic Engineering, Signal Processing, Shandong University</p>	9 credit hours per semester	

*F, P: Full-time or Part-time; D, UN, UT, G: Developmental, Undergraduate Non-transferable, Undergraduate Transferable, Graduate*

- c) Explain how faculty workloads will be impacted by the proposed new program. The impact on faculty workload will be minimal the first year. Five of the six classes offered the first year are cross-listed with graduate-level CPSC Cybersecurity classes. If the combined enrollments exceed the class size maximum, the class will be split into multiple sections with experienced graduate faculty teaching the extra sections. Eight of the sixteen Computer Science faculty have taught cybersecurity courses, most at the graduate level. Those undergraduate sections being vacated will be taught by lecturers and/or adjunct faculty.

It is anticipated that the new Director of the Cybersecurity Center will teach the new course - CSMT6222 Foundation of Cybersecurity Policy and Management during the first year.

In subsequent years, new faculty positions will be justified by increased enrollments.

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

- d) Explain whether additional faculty will be needed to establish and implement the program. Describe the institutional plan for recruiting additional faculty members in terms of required qualifications, financial preparations, timetable for adding faculty, and whether resources were shifted from other academic units, programs, or derived from other sources.

The School of Computer Science hired two top quality replacement faculty in 2016; one experienced in cybersecurity. The School used the state allocation requested for the Endowed Professor position to hire Dr. Paul Wang as a professor of cybersecurity. Four additional faculty positions, one each year (FY2018, FY2019, FY2020, and FY2021), need to be funded to keep pace with the increased enrollments. At least one of the new faculty hired in FY2018 or FY2019 should have a background in cybersecurity and management. We plan to recruit nationally for all positions through traditional channels and through the cybersecurity academic channels. Additionally, three of our alumni are working on PhDs in cybersecurity and have expressed interest in returning to teach at Columbus State University.

Fiscal Year	Position needed	Financial Need (cumulative)	Source
2018	<ul style="list-style-type: none"> <li>• One FTE <b>non-tenure track</b> to teach 3 new CSMT courses each semester</li> <li>• Part-time instructor to teach lower-level classes in order to release a cybersecurity faculty to teach a graduate course</li> </ul>	\$109K	tuition
2019	<ul style="list-style-type: none"> <li>• One FTE <b>tenure-track</b> to teach 3 new CSMT courses each semester</li> <li>• Part-time instructor to teach lower-level classes in order to release a cybersecurity faculty to teach a graduate course</li> </ul>	\$243K	New faculty (state / endowment / tuition)
2020	<ul style="list-style-type: none"> <li>• One FTE <b>non-tenure track</b> to teach 3 new CSMT courses each semester</li> <li>• Part-time instructor to teach lower-level classes in order to release a cybersecurity faculty to teach a graduate course</li> </ul>	\$342K	New faculty (state / endowment / tuition)
2021	<ul style="list-style-type: none"> <li>• One FTE <b>tenure-track</b> to teach 3 new CSMT courses each semester</li> <li>• Part-time instructor to teach lower-level classes in order to release a cybersecurity faculty to teach a graduate course</li> </ul>	\$466K	New faculty (state / endowment / tuition)

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

### (17) Fiscal and Estimated Budget

- e) Describe the resources that will be used specifically for the program.

The initial set-up costs for this new program and the enhancement of existing cybersecurity programs are funded by \$700+K gifts from TSYS and \$14K from the NSA. The maintenance of the cybersecurity programs will be from a \$2M endowment from TSYS.

Budget Instructions: Complete the form further below and **provide a narrative to address each of the following:**

- f) For Expenditures:

- i. Provide a description of institutional resources that will be required for the program (e.g., personnel, library, equipment, laboratories, supplies, and capital expenditures at program start-up and recurring).

Since this program will be delivered online, no physical classroom or lab space is required. The School of Computer Science has used \$14K from the NSA and \$62K from the TSYS gift to purchase the full-version of Netlab+ and equipment to host the software.

The new Cybersecurity classroom and lab on the 1<sup>st</sup> floor of the CCT Building will be available for collaboration between on campus and online students. The Center is being built with funds from the TSYS gift.

A small fixed cost of \$5,000 is requested for supplies and expenses. \$2000 and \$8000 are requested for each faculty member's conference attendance and professional certification.

- ii. If the program involves reassigning existing faculty and/or staff, include the specific costs/expenses associated with reassigning faculty and staff to support the program (e.g., cost of part-time faculty to cover courses currently being taught by faculty being reassigned to the new program, or portion of full-time faculty workload and salary allocated to the program).

It is anticipated that there will be a need to reassign a faculty for 1-3 classes in Fall 2017, 2-3 classes in Spring 2018 and later. The cost of part-time faculty is \$3000/course.

- g) For Revenue:

- i. If using existing funds, provide a specific and detailed plan indicating the following three items: source of existing funds being reallocated; how the existing resources will be reallocated to specific costs for the new program; and the impact the redirection will have on units that lose funding.

Start-up funding from TSYS has been received and spent.

- ii. Explain how the new tuition amounts are calculated.

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

\$329 per semester hour is the recommended tuition for this online CSU graduate professional degree program. (Students will also pay the technology, institution, and student activity fees.)

### Justification

\$329 is the tuition rate charged for CSU's online M.S. in Applied Computer Science. The program in Cybersecurity Management will have some courses in common with the Applied Computer Science program. It seems rational to charge students in the two programs the same tuition rate for the courses.

The increased tuition is necessary in order to hire high quality faculty with specialized expertise. This is a professional masters degree that is priced below all online cybersecurity master's degree programs in Georgia. Two faculty interviewed for a cybersecurity position at CSU turned down the position because the salary offered was too low.

Students will save money by taking a program that is 30 hours in length. A 30-hour program at \$329 will have a total tuition of \$9,870. A 36-hour program at CSU's basic graduate e-Tuition rate of \$301 would have a tuition cost of \$10,836.

- iii. Explain the nature of any student fees listed (course fees, lab fees, program fees, etc.). Exclude student mandatory fees (i.e., activity, health, athletic, etc.).  
NA
- iv. If revenues from Other Grants are included, please identify each grant and indicate if it has been awarded.  
NA
- v. If Other Revenue is included, identify the source(s) of this revenue and the amount of each source.  
NA

### h) When Grand Total Revenue is not equal to Grand Total Costs:

- i. Explain how the institution will make up the shortfall. If reallocated funds are the primary tools being used to cover deficits, what is the plan to reduce the need for the program to rely on these funds to sustain the program?

We continue to solicit private funding and grants to sustain our cybersecurity programs.

- ii. If the projected enrollment is not realized, provide an explanation for how the institution will cover the shortfall.  
Once this program is approved, we have an ambitious recruitment plan ready to roll-out.

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

<b>I. EXPENDITURES</b>	<b>FY 2018 Dollars</b>	<b>FY 2019 Dollars</b>	<b>FY 2020 Dollars</b>	<b>FY2021 Dollars</b>
<b>Personnel - reassigned or existing positions</b>				
Faculty (see 15.a.ii)				
Part-time Faculty (see 15 a.ii)				
Graduate Assistants (see 15 a.ii)				
Administrators(see 15 a.ii)				
Support Staff (see 15 a.ii)				
Fringe Benefits				
Other Personnel Costs				
<b>Total Existing Personnel Costs</b>	0	0	0	0
<b>EXPENDITURES (Continued)</b>				
<b>Personnel - new positions (see 15 a.i)</b>				
Faculty	\$80,000	\$180,000	\$260,000	\$360,000
Part-time Faculty	\$9,000	\$18,000	\$18,000	\$18,000
Graduate Assistants				
Administrators				
Support Staff				
Fringe Benefits	\$ 19,889	\$ 44,577	\$ 63,777	\$ 87,777
Other personnel costs				
<b>Total New Personnel Costs</b>	\$108,889	\$242,577	\$341,777	\$465,777
<b>Start-up Costs (one-time expenses) (see 15 a.i)</b>				
Library/learning resources				
Equipment (servers for virtual lab)				
Other (virtual lab software)				
Physical Facilities: construction or renovation (see section on Facilities)				
<b>Total One-time Costs</b>	0	0	0	0
<b>Operating Costs (recurring costs - base budget) (see 15 a.i)</b>				
Supplies/Expenses	\$5,000	\$5,000	\$5,000	\$5,000
Travel	\$2,000	\$6,000	\$8,000	\$10,000
Equipment				
Library/learning resources				
Other	\$8,000	\$16,000	\$8,000	\$8,000
<b>Total Recurring Costs</b>	\$15,000	\$27,000	\$21,000	\$23,000
<b>GRAND TOTAL COSTS</b>	\$123,889	\$269,577	\$362,777	\$488,777

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

<b>III. REVENUE SOURCES</b>				
<b>Source of Funds</b>				

Reallocation of existing funds (see 15 b.i)				
New student workload				
New Tuition (see 15 b.ii)	\$148,050	\$315,840	\$365,190	\$592,200
Federal funds				
Other grants (see 15 b.iv)				
Student fees (see 15 b.iii) Exclude mandatory fees (i.e., activity, health, athletic, etc.).				
Other (see 15 b.v)				
New state allocation requested for budget hearing				
<b>GRAND TOTAL REVENUES</b>	\$148,050	\$315,840	\$365,190	\$592,200
<b>Nature of Revenues</b>				
Recurring/Permanent Funds				
One-time funds				
<b>Projected Surplus/Deficit</b> (Grand Total Revenue - Grand Total Costs) (see 15 c.i. & c.ii).	\$24,162	\$46,263	\$2,413	\$103,423

### 17) Facilities/Space Utilization for New Academic Program Information

Facilities Information — Please Complete the table below.

		<b>Total GSF</b>
<b>a.</b>	<b>Indicate the floor area required for the program in gross square feet (gsf). When addressing space needs, please take into account the projected enrollment growth in the program over the next 10 years.</b>	NA
<b>b.</b>	<b>Indicate if the new program will require new space or use existing space. (Place an "x" beside the appropriate selection.)</b>	
	<b>Type of Space</b>	<b>Comments</b>
i.	Construction of new space is required (x). → <b>No</b>	<b>Program delivered online</b>
ii.	Existing space will require modification (x). → <b>no</b>	<b>Program delivered online</b>
iii.	If new construction or renovation of existing space is anticipated, provide the justification for the need.	NA

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

iv.	Are there any accreditation standards or guidelines that will impact facilities/space needs in the future? If so, please describe the projected impact.	NA		
v.	Will this program cause any impact on the campus infrastructure, such as parking, power, HVAC, other? If yes, indicate the nature of the impact, estimated cost, and source of funding.	NA		
vi.	Indicate whether existing space will be used.	yes		
<b>c.</b>	<b>If new space is anticipated, provide information in the spaces below for each category listed:</b>			
i.	Provide the estimated construction cost.	-		
ii.	Provide the estimated total project budget cost.	-		
iii.	Specify the proposed funding source.	-		
iv.	What is the availability of funds?	-		
v.	When will the construction be completed and ready for occupancy? (Indicate semester and year).	-		
vi.	How will the construction be funded for the new space/facility?	-		
vii.	Indicate the status of the Project Concept Proposal submitted for consideration of project authorization to the Office of Facilities at the BOR. Has the project been authorized by the BOR or appropriate approving authority?	-		

<b>d.</b>	<b>If existing space will be used, provide information in the space below.</b>			
	Provide the building name(s) and floor(s) that will house or support the program. Indicate the campus, if this is part of a multi-campus institution and not physically located on the main campus. Please do not simply list all possible space that could be used for the program. We are interested in the actual space that will be used for the program and its availability for use.			
	<p><b>This program will be collocated with the other programs in the TSYS School of Computer Science on the 4<sup>th</sup> floor of the Center for Commerce and Technology.</b></p> <p><b>Since this program will be delivered online, no physical classroom or lab space is required.</b></p> <p><b>The new Cybersecurity classroom and lab on the 1<sup>st</sup> floor of the CCT will be available for collaboration between on campus and online students.</b></p>			
<b>e.</b>	<b>List the specific type(s) and number of spaces that will be utilized (e.g. classrooms, labs, offices, etc.)</b>			
i.	<b>No. of Spaces</b>	<b>Type of Space</b>	<b>Number of Seats</b>	<b>Assignable Square Feet (ASF)</b>
		Classrooms		

## ONE-STEP ACADEMIC PROGRAM PROPOSAL

	Labs (dry)		
	Labs (wet)		
	Meeting/Seminar Rooms		
	Offices		
	Other (specify)		
<b>Total Assignable Square Feet (ASF)</b>			
ii.	If the program will be housed at a temporary location, please provide the information above for both the temporary space and the permanent space. Include a time frame for having the program in its permanent location.		
	NA		
<b>Chief Business Officer or Chief Facilities Officer Name &amp; Title</b>		<b>Phone No.</b>	<b>Email Address</b>
		<b>Signature</b>	
<b><i>Note: A Program Manager from the Office of Facilities at the System Office may contact you with further questions separate from the review of the new academic program.</i></b>			

# ONE-STEP ACADEMIC PROGRAM PROPOSAL

## APPENDIX

Use this section to include letters of support, curriculum course descriptions, and recent rulings by accrediting bodies attesting to degree level changes for specific disciplines, and other information.

### **CPSC6126 Introduction to Cybersecurity (3 credits)**

Students learn to protect computer technology assets using mechanisms to enforce confidentiality, integrity and availability of data. Topics include an overview of the information security framework, the OSI model, security attacks, services and mechanisms, firewalls, network security basics, security and cryptography, intruder detection system basics, information security policy, basic security terminology and professional terms, DoS attacks, overview of malware, rules for avoiding viruses and vulnerabilities.

### **CSMT6222 Foundation of Cybersecurity Policy and Management (3 credits)**

This course provides students with an introduction to information security policies. Students will be introduced to sociological and psychological issues in policy implementation in general and then provided a focused dialogue on information security specific policies. The class discusses the entire lifecycle of policy creation and enactment and presents the students with issue specific policies in different domains of security. The structure of the policy is also discussed to assist the students design and modify policies. Several examples from different domains are incorporated in the curriculum to assist the students to learn in the context of real life situations.

### **CSMT6223 Enterprise Information Security [Pre-req. = CPSC6126] (3 credits)**

The course provides an in-depth study of security issues in computer systems, networks, and applications for corporations. Application level security focuses on various security policies; network security; and supply chain security. Internet and intranet topics include security in firewalls, web servers, databases and mail servers, encryption, and authentication.

### **CPSC6136 Human Aspects of Cybersecurity [Pre-req. = CPSC6126] (3 credits)**

This course examines the ethical and human aspects of cybersecurity, with focus on the human element of cyber incidents. The course surveys topics such as ethics, insider threats, usable privacy and security, laws, human training, policies, standards, cybercrime and the social, psychological and cultural aspects of cybercrime.

### **CSMT6226 Cloud Computing Security [Pre-req. = CPSC6126] (3 credits)**

This course focuses on the security concerns and countermeasures in a cloud environment. Topics include an overview of cloud computing and virtualization, the critical technology underpinning cloud computing, necessary foundation for threats in cloud computing, access control, identity management, account and service hijacking, secure APIs, malware, regulatory compliance, forensics, and secure computing in the cloud, etc.

### **CSMT6228 Global Cybersecurity [Pre-req. = CPSC6126] (3 credits)**

This course provides an in-depth study of cybersecurity from a global perspective. Topics include cyber-terrorism, cybercrime, and cyber-warfare; the international legal environment; nation- and region-specific norms regarding privacy and intellectual property; international standard setting; effects on trade (including offshore outsourcing); and opportunities for international cooperation.

# ONE-STEP ACADEMIC PROGRAM PROPOSAL

## **CPSC 6157 Computer Network and Management (3 credits)**

Besides exposing graduate students to current computer networks issues and techniques, this course is specifically designed to focus on the protocols, algorithms and tools needed to support the development and delivery of advanced network services over the Internet. This graduate-level course is also focused on understanding technical details in a number of areas of advanced networking through reading and discussion of important research papers in the field. The topics covered in this course include 1) network communication; 2) network security; 3) web organization; 4) mobile and multimedia networking; 5) quality of service; 6) network management; 7) compression; 8) network performance.

## **CPSC6159 Cybersecurity Investigations and Crisis Management [Pre-req. = CPSC6126] (3 credits)**

The course will focus on the role of computer forensics and the methods used in the investigation of computer crimes. The course explains the need for proper investigation and illustrates the process of locating, handling, and processing computer evidence. A detailed explanation of how to effectively handle crisis will be covered.

## **CPSC6167 Cybersecurity Risk Management [Pre-req. = CPSC6126] (3 credits)**

This course focuses on the risk analysis component of cybersecurity management. It provides detailed coverage of contemporary frameworks and processes related to managing risk. Also, it involves enumerating organization's resources and prioritizing their protection based on probability of threat and subsequent damage. Reporting security breaches to management, and providing steps to mitigate threats and implement future controls will be an integral part of this course

## **CSMT6299 Capstone in Cybersecurity Policy and Management [Pre-req. = CPSC6136] (3 credits)**

This course will provide students with the opportunity to integrate all concepts and competencies that have been learned in this program, building on their experiences and professional goals, into a single project. The project may be part of an internship / coop. The project will be the culmination of a student's studies integrated in their area of specialization or expertise. In cooperation with a faculty advisor (and possibly a professional mentor), the student will design, research, and implement a project that is comprehensive in nature and which addresses, to the extent feasible, all core areas of knowledge around which the program has been built. The capstone is intended to be a six-credit experience spanning two semesters.