CYBERSYSTEMS AND INFORMATION SECURITY (CSIS) CURRICULUM

The approved (by ACHE in 12/2009) and accredited (by SACS in 12/2010) Master of Science degree program in Cybersystems and Information Security will prepare students to become leaders in the field of information and network security. This program will offer instruction and research opportunities that provide graduates with the necessary knowledge and skills to effectively assess, develop, and manage secure information networks and respond to newly developed threats. The program will draw from existing faculty in these departments with expertise in the area of cybersystems and information security in addition to utilizing external experts in the field. The existing computer and information systems programs at AUM do not provide a detailed focus in the security area. The CSIS program will build on the strengths that currently exist at AUM in the Department of Mathematics (Computer Science option), and the Department of Information Systems and Decision Sciences. Thus, the accredited program will provide reciprocal support to these two departments. Additionally, the proposed program will significantly enhance educational opportunities available to graduate students in the Homeland Security option within the Master's degree program in Justice and Public Safety. Efforts are also underway and well in maturity for an ongoing partial collaboration between AU and AUM in this area. Some of the curriculum courses therefore will be taught by Auburn University professors in the Computer Science and Software Engineering (CSSE) Department.

In light of recent events, the founding of a graduate program in this field is indeed timely. In April 2009, the *Wall Street Journal* reported that in 2008 cyberspies targeting a number of companies across the U.S. "penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system." A few weeks later, the *Wall Street Journal* also reported that spies had broken into the U.S. Pentagon's $300 billion Joint Strike Fighter project. Government officials further suggested that similar incidents had led to a breach in the Air Force's air-traffic-control system in recent months.

Sources suggest that the threat of cyber-attacks is becoming increasingly more prevalent. According to a recent article, the Department of Homeland Security's US-CERT reported a grand total of 18,050 cyber-attacks in 2008 in both private and government sectors at the local and national levels. This number represents a significant increase from reported attacks in previous years. In 2007, a total of 12,986 were reported, compared to 5,144 attacks in 2006. Given the political and social significance of cybersecurity, the need for individuals with specialized training in the area of cybersystems and information security has become all the more urgent.

Evidence provided above clearly indicates the importance of cybersecurity on society and the need for greater cybersystems and information security. This not only includes leaders who can implement, monitor, and respond to security issues, but also researchers who can develop original and innovative technologies to improve cybersystems security. The approved and

accredited Cybersystems and Information Security program will provide specialized training in computer network and information security, secure software engineering, operating system security, secure network engineering, and applied cryptology. There are no existing undergraduate programs at Auburn University at Montgomery that are directly related to this accredited graduate program in Cybersystems and Information Security. However, the BS degree program in Mathematics (Computer Science Option) and the BSBA degree program in Management Information Systems are indirectly related as sources of potential students for the new CSIS graduate program.

As noted above for related graduate programs, existing computer science and management information systems courses in undergraduate programs at AUM do not provide a focus in the security area. Thus, the Cybersystems and Information Security program will provide support for these departments to enhance the security components of their undergraduate programs potentially creating interest in the proposed graduate program. Upon completion of this program, graduates will be able to:

- Demonstrate an understanding of the technical, management, and policy aspects of cybersystems and information security.
- Identify and respond to information security challenges in distributed and embedded systems.
- Recognize the impact of security issues related to software engineering on distributed information systems.
- Assess information security risks faced by an organization and develop a response plan.
- Demonstrate an understanding of technological and human engineering problems linked to security risks.
- Assess the impact of information security policies, and market developments on complex systems and organizational objectives.
- Evaluate and recommend technological tools and protocols to protect against risks.
- Mitigate system vulnerabilities and restore compromised services.
- Manage the development, acquisition and evolution of a secure information network.
- Construct secure networked and distributed computer systems.
- Troubleshoot large scale information networks and distributed systems.
- Establish requirements for complex security applications and translate these requirements into design architecture.
- Integrate the use of encryption technology in non-secure and non-private computers and systems.
- Design and conduct research in the area of cybersystems and information security.
- Critically evaluate and apply research and reports of threats to computers and cybersystems.
- Discuss the importance of life-long learning and professional development in information security disciplines.

List new courses that will be added to AUM curriculum specifically for this program. Indicate number, title and credit hour value for each course:

CSIS 6003 – Introduction to Computer Security – 3 credits
CSIS 6010 – Data Communications and Computer Networks – 3 credits
CSIS 6013 – Network Security and Reliability-Quantitative Metrics – 3 credits
CSIS 6020 – Distributed Systems – 3 credits
CSIS 6033 – Secure Software Systems – 3 credits
CSIS 6040 – Applied Cryptology – 3 credits
CSIS 6053 – Information Security Management – 3 credits
CSIS 6403 – Computer Systems Modeling and Simulation – 3 credits
CSIS 6912 – Supervised Practicum with Cyber-Industry Experience – 3 credits
CSIS 6952 – Security Policy Seminar: Healthcare, Finance, or Government – 3 credits
CSIS 6992 – MS Research Thesis – 9 credits

All courses have been approved by the Auburn University at Montgomery Graduate Council.

The curriculum consists of 36 semester hours that will be delivered in a two-year format. The proposed curriculum includes the following new courses:

CSIS 6003: Introduction to Computer Security (3 s.h. credit)

This course provides an introduction to techniques for defending against hostile adversaries in modern computer systems and computer networks, operating system security; network security, cryptography and firewalls, and network denial-of-service attacks and defenses; user authentication technologies with fundamental issues and first principles of security and information assurance. A laboratory component is incorporated into this course.

CSIS 6010: Data Communications and Computer Networks (3 s.h. credit)

Topics in the course include: computer networks overview, OSI layers, transport, network and link layers of the protocol stack, including network management, traffic engineering, router internals, queuing theory, data link protocol, flow control, congestion control, routing, local area networks, transport layer, fundamental principles underlying computer and telecommunication networks.

CSIS 6013: Network Security and Reliability - Quantitative Metrics (3 s.h. credit)

This course involves the exploitation of network infrastructure, either as the target of attack or as a vehicle to advance attacks on end systems. This course provides an in-depth study of network attack techniques and methods to defend against them by way of assessing and managing to mitigate. Network reliability with chance failures will be analyzed with metrics to assess security and reliability. A laboratory component is incorporated into this course.

CSIS 6020: Distributed Systems (3 s.h. credit)

Topics in this course include: models of distributed systems, distributed transactions, distributed file systems, infrastructures, distributed algorithms, cryptography and distributed security, overview of distributed multimedia applications, systems and

networking support for distributed multimedia systems, distributed real-time systems, load shedding, storage systems, security, and fault tolerance.

CSIS 6033: Secure Software Systems (3 s.h. credit)

This course takes a close look at software as a mechanism for attack, as a tool for protecting resources, and as a resource to be defended; the software design process; choices of programming languages, operating systems, and distributed object platforms for building secure systems; common software vulnerabilities, such as buffer overflows and race conditions; auditing software; proving properties of software; software and data watermarking; code obfuscation; tamper resistant software; and the benefits of open and closed source development. A laboratory component is incorporated into this course.

CSIS 6053: Information Security Management (3 s.h. credit)

This course covers administration and management of security of enterprise information systems and networks. Topics include intrusion detection systems, vulnerability analysis, anomaly detection, computer forensics, application logging, risk management, contingency planning and incident handling, digital immune systems, alarms and responses, security standards, evaluation and certification process, security planning, ethical and legal issues in information, privacy, traceability and cyber-evidence. A laboratory component is incorporated into this course.

ACCT 6180: Financial Accounting/Integrated Business Concepts (3 s.h. credit)

This is a capstone course for graduate students utilizing the applied research process in the performance of a comprehensive business analysis, including the unique accounting and auditing issues of specific industry assignments.

CSIS 6040: Applied Cryptology (3 s.h. credit)

This course is designed to provide the students with an understanding and a functional view of how to manage the activities involved in the process of converting or transforming resources into products or services. It emphasizes planning and decision-making activities associated with managing operations, with focus on manufacturing and service operations. Current best practices in managing business processes used by organizations and quantitative techniques used for decision-making and basic concepts governing risk management.

CSIS 6403: Computer Systems Modeling and Simulation (3 s.h. credit)

This course provides a simulation overview and studies types of simulation, complex system modeling, statistical simulation, selecting input probability distributions, generating random deviates, Monte Carlo simulation, discrete event simulation, modeling of computer hardware/software domain, modeling of integrated computer systems, simulation of software quality, simulation of queuing (banking etc.) systems, applications to cyber industry/security/reliability (project drafts), software application. A term project is required. A laboratory component is incorporated into this course.

CSIS 6040: Applied Cryptology (3 s.h. credit)

Topics covered include cryptographic primitives such as symmetric encryption, public key encryption, digital signatures, and message authentication codes; cryptographic protocols, such as key exchange, remote user authentication, and interactive proofs; cryptanalysis of cryptographic primitives and protocols. The goal is to become familiar with the foundations of these techniques and the cryptographic technologies, in particular: The range of security objectives, the levels of security that can be achieved, and the basic cryptographic systems, including conventional systems, symmetric and asymmetric systems, public key cryptography, secret sharing schemes and zero-knowledge proof systems.

QMTD 6750: Operations Research (3 s.h. credit)

This course utilizes the application of operations research methods to business and economic problems. The methods include linear programming, network analysis, game theory, queing theory, simulation and Markovian processes.

CSIS 6912: Supervised Practicum with Cyber-Industry Experience (3 s.h. credit)

This supervised practicum provides internship experience with an IT organization. During this practicum, the student is to apply knowledge in a real-world setting, gain experience in a specific field on security and privacy risk concerns, and create professional contacts. The cyber-industry is not limited to information technology but also can be extended to telecommunications enterprises and wireless communications.

CSIS 6952: Security Policy Seminars: Healthcare, Finance, Business or Government (3 s.h. credit)

This course provides the opportunity to participate in seminars by healthcare, finance and government authorities associated with risk related trends and problems. Most important, this is an opportunity for the student to learn and apply advanced engineering and management skills, including the specialized knowledge, to solve real-world problems. This course will provide opportunity for the student to respond to data intensive risk trends.

CSIS 6992: MS Research Thesis (9 s.h. credit)

This course provides individualized support and direction for students completing research and writing their thesis.

Master of Cybersystems and Information Security Semester-by-Semester Curriculum Model

1st year Fall Semester (9 credits)

CSIS 6003- Introduction to Computer Security – 3 credits*
CSIS 6010- Data Communications and Computer Networks–3 credits**
CSIS 6020- Distributed Systems – 3 credits*

Spring Semester (9 credits)

CSIS 6013- Network Security and Reliability-Quantitative Metrics – 3 credits**
CSIS 6033- Secure Software Systems – 3 credits*
CSIS 6040- Applied Cryptology – 3 credits**

2nd year Fall Semester (9 credits)

CSIS 6053- Information Security Management – 3 credits**
CSIS 6403 - Computer Systems Modeling and Simulation**
ACCT 6180- Financial Accounting Integrated Business Concepts - 3 credits***

Spring Semester (9 credits)
Non-thesis option
QMTD 6750 - Operations Research – 3 credits***
CSIS 6912- Supervised Practicum with Cyber-Industry Experience – 3 credits***
CSIS 6952- Security Policy Seminar: Healthcare, Finance or Government – 3 credits***

Thesis option
CSIS 6992- MS Research Thesis – 9 credits

Program Total: 36 credit hours

*At Auburn University in Auburn, AL
**At AUM in Montgomery, AL
***At AUM with an On-line option

The program will be administered through the AUM School of Sciences. The dean of this school will be responsible for oversight of the program.

APPENDIX: FAQ (Freq. Asked Questions by Applicants):

1. *When will the program become available for students to enroll?*

Officially in Fall Semester 2011 with the formal SACS accreditation letter arriving on Dec. 14, 2010. The CSIS Graduate Degree program has been officially approved by ACHE (Alabama Commission on Higher Education) in December 2009 and accredited by SACS (Southern Association of Colleges and Schools) in December 2010. The CSIS will start its 2nd year as of Fall'12. See offered courses for Fall'12 in the Appendix.

2. *How many semester hours does the program include?*

See the summary above.

36 semester hours that will be delivered in an approx. two-year format; with or without thesis; see pp.3-6.

3. *Will the courses be offered in the evening as well as during the day?*

Depends. For example the courses offered this semester are in the evening but then those offered by the Auburn U. campus at Auburn may be during the day. However there may/will be video or on-line versions of those Auburn courses made available on course by course basis to be inquired from the proper instructor, so that he/she will not have to commute if he/she has a local job.

4. *Do you have any information that you can forward to me regarding the degree plan and qualifications? What will be the criteria or litmus test for admissiosn into the program?*

See the above Curriculum section on pages 3-6 for the degree plan.

Please refer to AUM's graduate admissions office either by e-mail or calling Ashley Warren at 244-3623 or e-mail awarren3@aum.edu

Describe briefly the criteria and screening process that will be used to select students for the program:

The proposed program will require that all students satisfy the general admission requirements of the Auburn University at Montgomery Graduate School. These admission requirements include:

- Undergraduate degree in a computer science related field from an accredited college or university. Minimum undergraduate gpa of 2.75
- Graduate Record Examination (GRE) or MAT scores to support your GPA
- Official transcript(s) of all undergraduate and any graduate credits from each school previously attended. Successful international applicants must score at least 500 on the Test of English as a Foreign Language (TOEFL) paper version, 173 on the computer version, or 61 on the Internet version. Auburn University at Montgomery will also accept a 5 on the International English Language Testing System (IELTS) exam.
- International applicants must demonstrate full financial sponsorship if accepted into the graduate program, proof of a comprehensive medical plan, and submit an official Statement of Financing for International Students Form.

5. *Are the classes based on a 8 week or 16 week schedule?*

Generally and usually 16 week semester schedule. However, certain instructors may have 8-week versions. Therefore it is best to contact them once the courses are announced.

6. *What is unique about this Program that made a difference for the River Region?*

It is the first and only in-class (only partially 30% on-line if preferred) cyber security degree -not a certification- with a rigorously creative educational program, found to be accredited, south of CMU's (Carnegie Melon's INI: Information Networking Institute) cyber-security MS program.

7. *What are the job prospects for a potential candidate when he graduates?*

Check www.indeed.com and search for information and network security.
*SEE Appendix

8. *Why should the serious career-minded student consider the CSIS Graduate Degree program?*

   This program will prepare the student for a career in the fastest growing area of Information Technology that addresses the very real challenges the United States and the State of Alabama face in the world today with respect to cybersecurity. Today, many security professionals are limiting their educational to certification programs such as Security + and CISSP. However, a master's degree is so much better than any of these types of certifications in security because the student will be exposed to a broader and deeper body of knowledge than is available in a certification program. This will provide the student with a better base of knowledge to work with and will ultimately lead to a higher skill-level. Also, a graduate degree positions the student for further advancement when competing for promotions in the security profession.

9. *What are the internship opportunities?* Plenty with the area IT companies on cyber-security doing business with USAF, also those in Huntsville with NASA and Army.

10. What are the prereqs if you do not come from Computer Science background?

    1) Calculus I, 2)Computer Concepts and Fundamentals, 3)Statistics (offered at AUM in Fall or Spring), 4) Discrete Math (offered in AUM/Math this Fall 2012), 5) JAVA I-II Programming (offered at AUM this Fall) 6) Operating Systems (Spring 2013, will be offered at AUM's CSIS)

*Appendix:

Several mechanisms were utilized to project job openings in the area of Cybersystems and Information Security. To generate the numbers for the Projected Job Openings, www.indeed.com was reviewed in detail as the most cohesive and extensive website to project job openings in Montgomery (local), State, southern region (as defined by the Southern Regional Education Board (SREB) member states from South to East Coast), and national markets. The "Information Security and Network Security" search words were sought and the results obtained for 2010 are as follows: 9 projected job openings in the local Montgomery area; 63 projected job openings in the State; 6,079 job openings projected for the SREB; and 11613 projected jobs nationwide. Additional information on this search is located in Appendix C.

The national job openings projections noted above are supported by data presented in the Occupational Handbook from the Bureau of Labor Statistics. Network and Computer Systems Administrators are expected to show a 27% increase in employment needs from 2006 to 2016. While not all new jobs in this area will require a specialty in security, the Handbook notes that "the need for computer security specialists has increased over the past few years as cyber attacks have become more common" and this trend is expected to continue.[14] This information supports the numbers reported above for the area of Cybersystems and Information Security.

A separate online survey was used as an additional gauge of employment needs in the Montgomery region. The link to the online survey was e-mailed to these potential employers. The survey required each respondent to login using their e-mail address, which ensured that the survey was only completed once by each respondent. Each potential employer was contacted twice which yielded a 32% response rate. 72% of the respondents agreed or strongly agreed to the question, "If an advanced degree in this field were available at AUM, you would support your employees enrolling in the program." Additionally, 78% of the respondents agreed or strongly agreed that, "The presence of employees with and advanced graduate degree in Cybersystems and Information Security in [their] organization would enhance efforts to promote and create a more secure computing environment." The survey and results are provided in Appendix C.

Class Schedule Listing

Fall 2012
May 29, 2012

Sections Found

Info Sec Management - 1759 - CSIS 6053 - A

Associated Term: Fall 2012
Registration Dates: Mar 30, 2012 to Aug 16, 2012
Levels: Graduate (Semesters)

AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	6:20 pm - 7:35 pm	MW	GOODWYN HALL 318GH	Aug 13, 2012 - Dec 12, 2012	Base/Lecture Course	Joel B. Junker (P)

Modeling and Simulation - 1762 - CSIS 6403 - 0

Associated Term: Fall 2012
Registration Dates: Mar 30, 2012 to Aug 16, 2012
Levels: Graduate (Semesters)

AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	5:00 pm -	MW	GOODWYN HALL 115GH	Aug 13, 2012 - Dec	Base/Lecture Course	Mehmet Sahinoglu

	6:15 pm	12, 2012	(P)

Return to Previous

powered by SUNGARD HIGHER EDUCATION

Fin.Acct.Integ.Bus.Concepts - 1763 - ACCT 6180 - O

Associated Term: Fall 2012
Registration Dates: Mar 30, 2012 to Aug 16, 2012
Levels: Graduate (Semesters)

AUM Campus Campus
Hybrid Schedule Type
3.000 Credits

View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	7:40 pm - 10:15 pm	W	BUSINESS BLDG 208B	Aug 13, 2012 - Dec 12, 2012	Hybrid	Judith A. Kamnikar (P)

Class Schedule Listing

Spring 2013
Nov 07, 2012

Sections Found

Intro to Computer Security - 2980 - CSIS 6003 - 0

Associated Term: Spring 2013
Registration Dates: Nov 02, 2012 to Jan 10, 2013
Levels: Graduate (Semesters)

AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	5:00 pm - 7:35 pm	M	GOODWYN HALL 204GH	Jan 07, 2013 - Apr 30, 2013	Base/Lecture Course	Joel B. Junker (P)

Network Security & Reliability - 2979 - CSIS 6013 - 0

Associated Term: Spring 2013
Registration Dates: Nov 02, 2012 to Jan 10, 2013
Levels: Graduate (Semesters)
AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	5:00 pm - 7:35 pm	W	GOODWYN HALL 211GH	Jan 07, 2013 - Apr 30, 2013	Base/Lecture Course	Mehmet Sahinoglu (P)

Applied Cryptography - 3136 - CSIS 6040 - 0

Associated Term: Spring 2013
Registration Dates: Nov 02, 2012 to Jan 10, 2013
Levels: Graduate (Semesters)

AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	5:00 pm - 6:15 pm	TR	GOODWYN HALL 116GH	Jan 07, 2013 - Apr 30, 2013	Base/Lecture Course	Robert G. Underwood (P)

Supervised Practicum - 2981 - CSIS 6912 - 0

Associated Term: Spring 2013
Registration Dates: Nov 02, 2012 to Jan 10, 2013
Levels: Graduate (Semesters)

AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	5:00 pm - 6:15 pm	MW	GOODWYN HALL	Jan 07, 2013 - Apr 30, 2013	Base/Lecture Course	A Staff (P)

Security Policy Seminars - 2982 - CSIS 6952 - 0

Associated Term: Spring 2013
Registration Dates: Nov 02, 2012 to Jan 10, 2013
Levels: Graduate (Semesters)

AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	7:35 pm - 8:55 pm	TR	GOODWYN HALL	Jan 07, 2013 - Apr 30, 2013	Base/Lecture Course	Mehmet Sahinoglu (P)

Operating Systems - 3216 - CSIS 6970 - 0

Associated Term: Spring 2013
Registration Dates: Nov 02, 2012 to Jan 10, 2013
Levels: Graduate (Semesters)

AUM Campus Campus
Base/Lecture Course Schedule Type
3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	6:20 pm - 7:35 pm	TR	IRMA MOORE HALL 302N	Jan 07, 2013 - Apr 30, 2013	Base/Lecture Course	Luis A. Cueva-Parra (P)

Return to Previous

Operations Research - 2417 - QMTD 6750 - 0

Associated Term: Spring 2013
Registration Dates: No dates available
Levels: Graduate (Semesters)

AUM Campus Campus
Hybrid Schedule Type

3.000 Credits
View Catalog Entry

Scheduled Meeting Times

Type	Time	Days	Where	Date Range	Schedule Type	Instructors
Class	7:40 pm - 8:55 pm	MW	BUSINESS BLDG 113B	Jan 07, 2013 - Apr 30, 2013	Hybrid	David S. Ang (P)