High quality ciphers and protocols are important tools, but by themselves make poor substitutes for realistic, critical thinking about what is actually being protected and how various defenses might fail (attackers, after all, rarely restrict themselves to the clean, well-defined threat models of the academic world).
— Matt Blaze

An Introduction to Security Informatics

Security Informatics is a curriculum of instruction that is centered on the protocols and practices of security; both the technological and the social contexts. Thus Security Informatics includes the core subjects that define computer security such as access control, networking, cryptography, formal verification, auditing, forensics, and secure system administration. However, Security Informatics also includes the span of material covered by informatics. Thus Security Informatics includes the technical aspects of computer security integrated with an understanding of fields such as human computer interaction and design, social engineering, economic incentives, and organizational and societal policy and law. Modern day information security problems are solved neither by technical or social contexts independently, but typically require comprehensive approaches.

This document defines the program of study for the Masters of Security Informatics (MSSI). The program’s goal is to makes our students highly competent in the multidisciplinary world of computer security. This document presents the requirements necessary for completion of the MSSI degree; resources that are available to students; expectations of student conduct and ethics; discussions of how student progress is evaluated; security course descriptions and course registration information.

Vision

Security Informatics builds upon strong theoretical foundations to construct practical solutions for the intertwined challenges of security and privacy. Security Informatics addresses the immediate problems of today, such as phishing and ecommerce fraud, mobile device security, cloud computing, embedded systems security, corporate espionage and advanced persistent threats. It also addresses
emerging research problems, including privacy in ubiquitous computing environments (e.g., the Internet of Things), cyberwar, and the security and privacy of digital currencies, such as bitcoin.

The vision of the MSSI program is to ensure students leave with core competencies that allow them to not only understand today’s problems and challenges, and deploy and use modern technologies, but to have the foundational and broad view necessary to understand emerging problems, and technologies, so they can evolve and grow in this fast paced field. Thus we expect students to be exposed to both the theory and practice of a large number of fields. This is accomplished through combinations of classroom activities, laboratories, internships, research through independent study and extra-curricular activities.

Examples of the foundational skills our students will be exposed to include:

- Cryptography
- Networking
- Protocol Analysis
- Engineering Ethics
- Social Engineering
- Formal Methods
- Secure and Reliable Coding
- Secure Network Operation and Management
- Privacy Preserving and Enhancing Technologies
- Economics of Security
- Human Computer Interaction and Design

The Program

This program is built upon four core components.

2. Security Informatics Core.
4. Electives and/or Concentrations.

The first component ensures that students have a fundamental and deep understanding of the computing systems and networks upon which modern information technology is built. Without understanding of these systems, it is hard, if not impossible, to comprehend the security problems and solutions.

The second component introduces students to a variety of theories and skills of modern security and privacy in different domains of information technology. These courses cover both technical and social approaches.

The third element ensures students gain hands-on practical knowledge, in applying security skills. This is typically done through student internships, but may also be accomplished by faculty mentored independent study, or courses that are deemed to have a sufficient applied component.

Finally, the students have a certain number of electives. Students with weak technical backgrounds may need to use electives to take courses mastering basic programming and mathematical skills. However, students with strong backgrounds will often use their electives to pursue a collection of electives that concentrate in a specific area to which they can apply their security informatics skills.
Program Goals

Some of the core goals for the Security Informatics master's degree program include:

- Develop the mathematical foundation required for security informatics.
- Become well-versed in the recognition and understanding of seminal work – research, innovation and literature – that constitutes the core of security engineering.
- Acquire the technical skills to make effective use of current and emerging design applications.
- Understand the socioeconomic ramifications of security and privacy-enhancing technologies.
- Become proficient with practical skills that will be necessary in the daily business of security engineering.
- Cultivate an understanding of security in practice and how it functions in organizations, as well as in systems and network administration.
- Develop an interdisciplinary understanding that enables design and implementation that can address social engineering and economics of security.

A Comparison to Computer Science

The MSSI is simultaneously more tightly focused and more interdisciplinary than comparable computer science programs. The program is more focused on security. For example it requires the study cryptography and protocol analysis, as opposed to a larger focus that includes other areas of computer science. As is appropriate, the programs are strongly woven together: MSSI students need to take at least three courses in computing and networking foundations from Computer Science, and conversely Informatics security courses are often heavily populated with students majoring in computer science. The MSSI is more interdisciplinary in that includes social and organizational contexts for security problem, and considers information security problems in the social domain, as well as technical.

The Security Informatics Master's Program

The Masters of Science Degree in Security Informatics is structured as follows. A student must complete 36 credit hours of courses with the requirement that the following number of credit hours be achieved in each of the four areas as described below:

1. Computing and Networking Foundations........ 9 Credit Hours
2. Security Informatics Core.............................12 Credit Hours
3. Applied Security & Professional Practice.........6 Credit Hours
4. Electives and/or Concentrations....................9 Credit Hours

The following subsections describe exactly which courses can be used to attain credit for each of the areas mentioned. Course name and credit hours are listed in

Security Handbook: '14 Class
Informatics School of Informatics & Computing
the appropriate section. Course descriptions can be found later in this document, and on the School’s of Informatics and Computing web page. Note that any course that shows up in multiple categories can be used to fulfill at most one of those categories credit requirements. That is, courses may not be double-counted across categories.

Computing and Network Foundations

These courses are intended to ensure that students have a firm grasp of information systems. Students need to take 9 credit hours from the following list of courses. Note that not all courses are offered every semester, or even every year. Students must satisfy a networking and operating system requirement, either by taking one of (CSCI P436/CSCI P536) for operating systems and one of (CSCI P438/CSCI P538) for networking. Students who have previously taken such courses in prior studies can ask to be exempted from taking these specific courses, but must still take 9 credit hours in the area.

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCI P436 Introduction to Operating Systems</td>
<td>4</td>
</tr>
<tr>
<td>CSCI P438 Computer Networks</td>
<td>4</td>
</tr>
<tr>
<td>CSCI B534 Distributed Systems</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P538 Computer Networks</td>
<td>4</td>
</tr>
<tr>
<td>CSCI P535 Pervasive Computing</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P536 Advanced Operating Systems</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B541 Hardware System Design I</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P542 Hardware System Design II</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B543 Computer Architecture</td>
<td>3</td>
</tr>
<tr>
<td>CSCI P535 Embedded and Real-Time Systems</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B561 Advanced Database Concepts</td>
<td>3</td>
</tr>
<tr>
<td>CSCI B649 Internet Services and Protocols</td>
<td>3</td>
</tr>
</tbody>
</table>

Security Informatics Core

These courses are intended to ensure that students have a firm grasp of the fundamental ideas, skills, models and tools of information security. Students need to take 12 credit hours from the following list of courses. Students must take I520 and I533 for 6 of these core credits. This ensures that students get a well-rounded background in Security Informatics. Note that not all courses are offered every semester, or even every year (with the exception of I520 and I533, which are offered every year).

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO I520 Security and Software Assurance</td>
<td>3</td>
</tr>
<tr>
<td>INFO I521 Malware: Threat &amp; Defense</td>
<td>3</td>
</tr>
<tr>
<td>INFO I525 Organizational Informatics and Econ, Of Security</td>
<td>3</td>
</tr>
<tr>
<td>INFO I533 Systems and Protocol Security and Info. Assurance</td>
<td>3</td>
</tr>
<tr>
<td>INFO I536 Mathematical Foundations (Cryptography)</td>
<td>3</td>
</tr>
<tr>
<td>INFO I537 Legal and Social Informatics of Security</td>
<td>3</td>
</tr>
<tr>
<td>INFO I538 Introduction to Cryptography</td>
<td>3</td>
</tr>
<tr>
<td>INFO I539 Cryptographic Protocols</td>
<td>3</td>
</tr>
</tbody>
</table>
INFO I590 Topics in Informatics (See important note below) ........3
CSCI B649 Trusted Computing ................................................... 3

Note that I590 is a “Topics” course, which means many different courses are offered under this course listing. This course may be taken multiple times to satisfy credit hours in this area so long as the courses are taught by core program faculty, as listed at the top of this document, or 2) You have the approval of the MSSI program director. If you have any concerns, please check with the graduate office.

Applied Security & Professional Practice

The goal of these credits is to ensure that you have the opportunity to practice skills in an applied and preferably professional setting. Our goal is for most students to be able to have internships in organizations where they will be exposed to some practical aspect of information security in a day-to-day manner. The School’s Career Services group is an excellent resource that is useful in helping students find internships. We recommend that you start early. You need to start thinking about this in your first weeks! Please see the section on Career Services later in this document for contact and other useful information. Each 20-hour per week internship over a semester provides 3 credit hours. MSSI students are highly sought as paid interns; and it is not unusual for summer internship courses to provide both income and six hours of degree credit.

Beyond an internship, students may also satisfy their Applied Security & Professional Practice credit requirements through specific course (listed below). Finally, if a student is working with a particular faculty on a research project, then an independent study may also be possible. Please note that faculty are not obligated to supervise independent studies.

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO I591 Graduate Internship</td>
<td>........3</td>
</tr>
<tr>
<td>CSCI-Y790 Independent Study</td>
<td>........3</td>
</tr>
<tr>
<td>CSCI-A538 Network Tech &amp; Administration</td>
<td>........3</td>
</tr>
<tr>
<td>CSCI-A548 Mastering The World Wide Web</td>
<td>........3</td>
</tr>
</tbody>
</table>

Electives and/or Concentrations

The remaining credits are electives. There are three ways these credits are typically used to take courses that: 1) buttress weaknesses in your incoming education, 2) are in an area related to information security that are (frequently) outside of the school which we think of as concentrations, and 3) are traditional electives; courses which are simply of general interest to the student. It is important to note that unless you have the program director’s permission for a specific course beforehand, all electives credit must be at the 500 level or higher.

Buttressing Weaknesses

Many students coming from less technical backgrounds need exposure to programming, so that they can succeed in our technical courses. Similarly, some students find that they need a course in probability or statistics to prepare themselves for courses related to cryptography. In contrast, many technical students need help with their writing, and look to take courses related to professional or technical writing, or writing in English as a second language. To the degree possible, the need for such courses should be identified early in your studies.
If you have concerns about your background, they should be discussed with the Program Director during your initial course planning meeting.

Concentrations
Here the goal is to use one’s electives to form an intellectually coherent concentration, that compliments the interdisciplinarity of security informatics. Note that concentrations are not recognized on transcripts nor your degree. Rather, our experience has been that students who organize their electives in this manner have the greatest satisfaction with the outcome. Such organization allows students the freedom to customize their education to meet their personal interests and needs. The goal is to use at least two electives, if not all three, to explore a view of a single method, question, point of view, discipline, or domain.

Examples of concentrations that many students have shown interest in are included later in this document.

Traditional Electives
Here the student simply takes courses at the university that are of interest to them. These courses

Example Courses of Study

Students entering the MSSI may be joining the program from a technical or social science background. The following courses of study present examples of two different paths for people entering with different strengths and interests.

Example 1: An Arriving Computer Science Student

Imagine a student arriving with a BSc in computer science. That student has previously taken a course in networking, but never in operating systems. The student’s mathematics background is weak, so she decides to take a probability course in math to help prepare for her course in cryptography. She also has an interest in Data Mining, which she has found intersects nicely with Information Security, and so she uses her last two electives on those. She found summer employment penetration testing in the security field, working full time, so she is able to finish her professional practice over the summer.
Example 2: An arriving Economics Student

<table>
<thead>
<tr>
<th></th>
<th>1st semester</th>
<th>2nd semester</th>
<th>Summer</th>
<th>3rd semester</th>
<th>4th semester</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Core</strong></td>
<td>INFO 537 Economics of Security INFO 538 Crypto</td>
<td></td>
<td></td>
<td>INFO 520 Network Security</td>
<td>INFO 533 Information Assurance</td>
</tr>
<tr>
<td><strong>Application and Professional Practice</strong></td>
<td></td>
<td>Network Admin (3) Professional Internship 1591</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Computing Foundations</strong></td>
<td></td>
<td></td>
<td></td>
<td>B534 P436</td>
<td>P438</td>
</tr>
<tr>
<td><strong>Electives</strong></td>
<td>Intro Programming</td>
<td>Business Risk</td>
<td></td>
<td></td>
<td>Business Modeling</td>
</tr>
</tbody>
</table>

The student arrives. The student has never programmed, but has a casual understanding of computers. Having taken economics, the student has a strong mathematics background. Thus the student takes an introductory course on programming and data-structures, and an applied course on systems administration in his first year to improve his computing skills, while concurrently taking mathematical and organizational security courses.

In the second year he takes the more technical and required security core courses, as well as foundational courses on computing. He uses his remaining electives to pursue some security related courses from the business school.

### Security Core Courses

The following are brief descriptions of the security core courses.

**INFO 1520 Security for Networked Systems**

This course is an extensive survey of system and network security. Course materials will cover threats to information confidentiality, integrity and availability in a computing system and network, and defense mechanisms which control these threats. The course will also provide necessary foundation on information security, such as cryptographic primitives/protocols, authentication, authorization and access control technologies, and hands-on experiences through programming assignments and course projects.

**INFO 1521 Malware Epidemic: Threat and Defense**

The objective of this course is to offer a technical review of mobile and Cloud security, particularly security weaknesses in those new computing paradigms that can be exploited by mobile or web-based malware, and also explore new technical directions to address these security challenges. Students will be trained to understand the new security threats through literature review and gain hands-on experiences through course projects.
INFO 1525 Organizational Informatics and Economics of Security
Organizational processes embed implicit and explicit decisions and information control. Security technologies and implementations make explicit organizational choices that determine individual autonomy within an organization. Security implementations allocate risk, determine authority over processes, make explicit relationships in overlapping hierarchies, and determine trust extended to organizational participants. This is a graduate case-based course that will examine implementations of security in organizations.

INFO 1533 System & Protocol Security & Information Assurance
Basic concepts of security reviewed. Threat and adversary modeling; attacked objective and currently using MS threat modeling may use Gary McGraw’s threat modeling. Do the theory in class and then the lab in practice. ACL theory and implementation, firewalls and port blocking, applied crypto, principle of least privilege, auditing, logs, data retention.

INFO 536 Foundational Mathematics of Cybersecurity
Students will learn mathematical tools necessary to understand modern cyber security. The course will cover introductory mathematical material from a number of disparate fields including probability theory, computational theory, complexity theory, group theory, and information theory.

INFO 1537 Legal and Social Informatics of Security
Security technologies make explicit organizational choices that allocate power. Security implementations allocate risk, determine authority, reify or alter relationships, and determine trust extended to organizational participants. The course begins with an introduction to relevant definitions (security, privacy, trust) and then moves to a series of timely case studies of security technologies. This course may be taken as an alternative I525. The course also requires a project, including a work plan, a timeline, peer evaluations, and professional presentations.

INFO 1538 Introduction to Cryptography
This class considers issues of network security, treating in depth the topics covered in INFO 1536. In particular, the class involves adversarial modeling, a detailed treatment of security primitives, and methods for analysis of security. It spans the ethics and technology of security, with examples drawn both from deployed and proposed protocols. Topics to be covered include studies of rational and malicious cheating, symmetric and asymmetric cryptography, security reductions and heuristics.

INFO 1539 Cryptographic Protocols
This class will cover current and timely topics in the field of Security Informatics. Topics will vary from year to year. Examples of topics that could have been covered in recent years include phishing and cyberfraud, trusted computing basis, electronic voting, and digital rights management systems.

INFO 1590 Topics in Informatics-- Today's Privacy Challenges: Technology and Policy
In this class students will learn about how privacy-infringing technologies work and how to design solutions that empower people to manage their privacy. In our interconnected world people are continuously leaking data to anyone who knows
how to listen for it. Malls now track the movement of patrons through the WIFI signals on their phones. Online advertisers track people's movements across the web to provide more meaningful advertisements.

In this class students will gain an understanding of how privacy-infringing technologies work, what they can do, and cannot do. Students will spend part of the course doing hands-on experimentation with privacy infringing technologies to better understand how they work. We will then shift to discussing how to design solutions that address these types of issues through technological, policy, and educational means.

INFO I590 Topics in Informatics—Advanced Topics in Privacy
This seminar is driven by student-led roundtable discussions of seminal and influential research papers, and short lectures on improving research skills. Building on knowledge gained in class, students will work on research projects in groups targeting either a potential academic publication or a prototype for a potential industrial startup. This seminar most recently focused on wearable and sensor-based computing and social networks.

CSCI B649 Trusted Computing
We will explore current methods for characterizing, establishing and attesting trust of a system. We will cover a variety of topics including hardware-based trusted components, trusted identities and identity management, reputation systems, trust negotiation, etc.

Seminar Series
Master’s degree students have the opportunity to attend seminars by distinguished faculty and insightful practitioners with the purpose to broaden and stimulate your intellectual development. The School organizes regular Colloquia with invited speakers. There is an Honors Seminar Series that will be open for all students, and there is also the Center's For Applied Cybersecurity (CACR) Security Seminar. It is assumed that students will regularly attend most of these seminars. It is a crucial part of learning the current and future trends in security informatics. These speakers are typically world experts in their respective fields.

Need to Know
As you tailor your electives for your program, consider what a highly effective security practitioner needs to know:

Technical Skills
• Ability to read and understand a cryptographic, security or privacy protocol, and corresponding security definitions and models.
• Appreciation of types and categories of bugs, attacks, and patches.
• Understanding basic computer science concepts and how engineers solve problems.
• Mathematics and research methods

Foundational Security Literature
• Familiarity with the foundational literature of cryptography, security and privacy systems
• Understanding of the core concepts of frequently deployed security protocols.

Current Security Literature
• Ability to read articles and protocols critically.
• Ability to read research papers, including statistical analyses.
• Reading journals on a regular basis, tracking developments.
• Ability to track and research attacks and defenses.

System Administration
• Ability to install, upgrade, manage and secure web servers and other applications.
• Ability to examine a log and explain its implications.
• Minimum level of expertise in configuration of popular operating systems and servers (e.g., linux, os x, windows)
• Familiarity with fundamental concepts of networks, interactions, etc.

Team Collaboration
• Functioning effectively as a team member and a team leader.
• Consulting skills.
• Professional skills.

Presentation Skills
• Preparation of supporting documentation.
• Speaking.
• Functioning effectively in a professional environment.

Resources

Travel Funding
All MSSI students can apply for one-time travel funds to cover some of the costs of attending a conference related to Security Informatics. Funding is awarded to students upon admission. Applications for travel funds are reviewed and approved by the grad directors. These funds must be used for travel, hotel, food, and/or registration fees. Each MSSI student will be provided up to $800 during his/her entire program. Items such as alcohol, entertainment, etc. are not allowed. All expenses must be approve prior to the event. All receipts are required for reimbursement.”

Application forms for travel funds may be found at http://www.soic.indiana.edu/graduate/formsI/other-forms.shtml

Career Services
The School of Informatics and Computing has a dedicated Career Services staff to help students find and secure internship and job opportunities or meet their other career goals. The SoIC hosts two major career fairs each year where students can meet with more than 80 companies in the fall semester and more than 60 during the spring semester. In 2013-2014, 127 companies recruited on-campus and
conducted more than 1000 interviews in the School. Career Services staff are there to help students with every step in the process including figuring out what they want to do, getting their materials prepared, connecting with employers, practicing interviewing skills, and negotiating salary. The Fall 2014 Career Fair is scheduled for Thursday, September 11 and employers will be participating in other recruiting activities beginning even earlier in the week so students should not wait to get the help they need. Students can log in to SoIC Careers using their CAS login to schedule career advising appointments, search employers, apply for job/internship opportunities, see who will be attending the Fair, find the Job Search Guide and list of upcoming workshops, and more! For more information on how Career Services can help, see the Career Services website (www.soic.indiana.edu/career/).

Diversity Office

For a community to be truly special, everyone needs to feel welcome there. This is precisely the type of community we’re fostering at the School of Informatics and Computing—a place where students, faculty, and staff of both genders and all races, backgrounds and orientations are accepted and supported.

• In 2008, Dean Schnabel created a dedicated administrative position to focus on diversity in the School and Dr. Maureen Biggers is our dedicated Assistant Dean for Diversity and Education, working with students and faculty in this arena. (Since 2008 we have tripled the number of undergraduate women in our program at a time while the number of men has doubled.)

• SOIC is named a Pacesetter (PDF) by the National Center for Women & Information Technology (NCWIT), which our dean, Bobby Schnabel, co-founded.

• Assistant Dean for Diversity and Education Maureen Biggers serves as Director of the new IU Center of Excellence for Women in Technology.

In the Student Community

Our students come from all over the world, and we want all of them to succeed as students and professionals. Women at SoIC offers mentoring and leadership opportunities, and sponsors events which promote community and professional development. SOIC recently launched a chapter of NSBE: National Society of Black Engineers, advised by Dr. Lamara Warren, Director of Diversity, Inclusion and Education for SOIC.

The PIT Crew: Promoting Inclusivity in Technology (http://pit.soic.indiana.edu/about.html)
is a group of graduate students engaged in building community and a network of Champions of Inclusion within our community. Each year a small number of paid positions are available to graduate students to get involved with this diverse group for the year. If you are interested in learning more about this paid opportunity please contact either Maureen Biggers (biggersm@indiana.edu) or Lamara Warren (ldwarren@indiana.edu).
In the Classroom

Our focus on diversity in the classroom has two main components: creating classroom environments that promote the success of all students, and recruiting and retaining diverse faculty and instructors.

We emphasize research-based best practices in the classroom, holding professional development colloquia on research about recruiting and retaining diverse students. We also host weekly seminars for faculty and instructors who teach first- and second-year students, as well as hold AI workshops that promote inclusivity in the classroom and lab environments.

Student Conduct & Evaluation

Standards & Reviews

Each first year student may receive a review from the faculty in the spring semester of the first year. The purpose of this review letter is to provide guidance and feedback. For example, every admitted student receives some funding to travel to an event. If you have not taken advantage of this opportunity you will be reminded of the purpose of the funds and the need to network while enrolled in studies. These letters also serve to identify any difficulties (should these exist). Students who are doing well and need no guidance are unlikely to receive a review, as it would be unneeded.

The standards of these reviews and our expectation of students follow. The graduate student evaluation has three components: classroom performance, practice, and professional advancement.

After the first year, you will be expected to complete a summary report. Ideally, if a review is needed, a summary report will be completed by January 31 of each year. After the first year, the report will inform the evaluation of your performance.

Classroom performance: The minimal standard is that you must maintain an average of 3.0 or above. You are expected to never receive a grade of C+ or below. If you do achieve such a score, the course will not be counted for credit towards your degree, nor towards your credit areas.

Practice performance: The standard requires that the student illustrate progress towards independent applied security skills through projects, laboratory experience and internships. As there is great variance between practice areas, this component is evaluated and documented by the faculty with which you take courses, perform independent study, and the Program Director.

Professional performance: The standard requires that the student interact with the broader security community as a whole as the student progresses in the program. Initial professional evaluations may be a result of teaching assistantships, seminar attendance, or presentations in the classroom. Later evaluation will be a function of workshop attendance, internship performance, publication of event notes, presentation at events including rump sessions, and overall integration into the community of security professionals. This component of the evaluation is
determined by the security faculty as a whole. Note that this element includes speaking, presentation and writing skills.

Possible ratings in each category are excellent, exceeds expectations, satisfactory, or unsatisfactory. Receiving satisfactory on all three is acceptable, by definition. A single mark of unsatisfactory identifies a need for significant immediate improvement. Two ratings of unsatisfactory indicate that completion of the MSSI program in two years is unlikely (given past performance) and the student will not complete the program at the current level of achievement. Three unsatisfactory ratings indicate a failure to make satisfactory progress in any dimension. A student who receives three ratings of unsatisfactory requires major, immediate change if there is hope of completing the program.

If students are making unsatisfactory progress, the faculty will usually engage with the student to identify goals and avenues of improvement. This may include proposing goals for the next semester. The faculty may also set specific near-term or long-term requirements.

The faculty may also make recommendations to the School to terminate support or to terminate the student from the program. Before this time it is likely that the student will have been in discussions with the Program Director, and possibly with the Associate Dean of Graduate Studies. Should the student feel that he or she is struggling, that student should alert the Program Director immediately. Therefore, if a student is making unsatisfactory progress, unsatisfactory ratings should not be unexpected. The student should not wait for a formal indication that the problem may have become insurmountable to seek support from the administration.

**Academic Misconduct**

Academic misconduct represents a broad range of academic offenses, examples of which include cheating, fabrications, interference, violation of course rules, facilitating academic dishonest, and plagiarism. It is essential that you properly cite a source, and only include others’ works when that work is properly delineated and credited. As an IU student you are expected to uphold Student Code of Conduct, as described here: [http://www.iu.edu/~code/code/index.shtml](http://www.iu.edu/~code/code/index.shtml)

Given that Security Informatics students are often dealing in areas where trust is paramount, there will be no warnings given for academic misconduct! Rather, the faculty and program director will push for the strongest penalties possible.

**Academic Probation**

An MSSI student may be placed on academic probation for the following reasons:

- The GPA falls below 3.0.
- Satisfactory progress is not being made towards the degree as determined by MSSI faculty or Program Director in the evaluation of the student’s work.
- Failure to fulfill requirements which were stipulated at the time of admission, including English exams or required language training for international students.

When a student is put on academic probation, recommendation will be given to the student to improve his/her academic standing with deadlines set. The student’s
performance is evaluated again at those deadlines to determine if improvements have been made and goals have been met. If performance does not improve, the student will not ordinarily be allowed to continue in the graduate program.

Course Registration, Transfer and Validation

Course Registration Guidelines

Full-time Status
To be considered full-time student, the student must register for 8 credit hours, according to IU policy. The student should choose three courses (typically 3 credit hours each) that count towards the intended degree. Students must enroll in three courses even if they are making up incompletes from a previous semester. Students are expected to maintain a normal load as they make up incompletes.

Tip: "Add and drop" instead of "drop and add": When replacing courses, be sure to add the new course first and then drop the old, in order to always be above the minimum number of credits for status.

Waitlist
If a course which you desire is shown as full, be sure to add yourself to the waitlist, which serves as a place holder for you in line. When students who enrolled in the course drop, or when the enrollment cap is expanded, students on the waitlist will be admitted into the course in order.

Drop and refunds
Be sure to finalize your schedule promptly. For course drops in the first week, IU refunds the full tuition for the course. In the second, third, and fourth weeks, refunds are 75%, 50%, and 25%. Later drops receive no refunds. We strongly encourage you to become familiar with the Office of the Bursar’s (http://bursar.indiana.edu/home/) policies and fee payment information.

Withdrawals from courses
During the automatic withdrawal period, students who withdraw will be assigned an automatic grade of W (see the Registrar’s official calendar for exact dates). After that period, withdrawals are only possible with approval from the Dean, which is normally given only for urgent reasons such as illness. Note that CS students must successfully complete at least 9 credits of courses towards their degrees each semester to be considered making satisfactory progress. The amount of tuition refund (if any) for a dropped course depends on when the course is dropped.

Applicability of fee remissions
Fee remissions normally are not applicable to outside courses not counting towards MSSI degree.

*AI and RA
Students offered a student academic appointment (SAA), as a Research Assistant (RA) or Associate Instructor (AI), have a workload that is a 50% FTE appointment (20 hours per week). Students with a SAA, are required to register for at least 6 credit hours to maintain full-time status.

Students with research assistantships must secure their RA supervisors' advance written permission to take any outside courses in addition to the required 9 credits.
of MSSI courses contributing towards their degrees. This approval must be provided to the Graduate Student Services Specialist prior to registration.

* Non-native speakers of English are required to pass an English exam. For more information see link: TEPAIC(http://www.indiana.edu/~dsls/publications/TEPAICCandidateRequirements.htm)

**Independent Study**

The MSSI Program offers one independent study course

1. **CSCI Y790.**

**How to sign up:** For independent study or research courses, the Independent Research Permission Form must be signed by the research supervisor and submit to the CS Graduate Studies Office, to obtain class permission to register. Please be sure to allow enough time to get the instructor's signature before the deadline to avoid late registration fees.

**Y790’s with supervision outside CS:** If the Independent Study supervisor is outside of the MSSI Faculty, you will need to find an MSSI faculty member to co-supervise the project and co-sign the form. The MSSI faculty member must assess the student’s work at the end of the semester and submit the grade for the course. Please be sure that all needed information is provided to him or her at the end of the semester, in time for the grade submission deadline.

**Transfer Credits**

Some graduate coursework completed at other universities may be transferred into degree and licensure programs. All coursework transferred must be from an accredited college or university and no transfer credit will be given for courses with a grade lower than a B. Transferred courses must be relevant to the student’s program of studies and must be approved by the MSSI Program Director and the Associate Dean for Graduate Studies.

To transfer credits, the student should identify the course at IU that may be considered equivalent to the course to be transferred, contact the instructor who teaches the course, provides documents, such as course description, course syllabus, sample homework assignments, projects and/or exams, as required by the instructor. In the case the instructor approves of the transfer, the student should prepare the Course Transfer form for the instructor to sign and submit the completed form to the CS Graduate Studies Office.

**Course Revalidation**

All graduate-level coursework over seven years old must be revalidated (counting back from the date of passing the oral qualifying examination). Normally, a course may not be counted toward degree requirements if it has been completed more than (a) five years prior to the awarding of the degree for master’s students or, (b) seven years prior to the passing of the qualifying examination for Ph.D. students. The graduate advisor, after consultation with the Advisory Committee, may, however, recommend to the dean that course work taken prior to the above deadlines be revalidated if it can be demonstrated that the knowledge...
Currency of knowledge may be demonstrated by such things as:

- passing an examination specifically on the material covered by the course;
- passing a more advanced course in the same subject area;
- passing a comprehensive examination in which the student demonstrates substantial knowledge of the content of the course;
- teaching a comparable course; or
- published scholarly research demonstrating substantial knowledge of the content and fundamental principles of the course.

Each course for which consideration for revalidation is being requested should be justified separately.

Leave of Absence

To request a leave of absence from the graduate program, a student should discuss the nature and length of the leave with the MSSI Program Director. The leave of absence form needs to be completed, and signed by the Director of the MSSI.

During Program of Studies: Students who do not enroll in classes for a period of one year must apply for re-admission to the program. They must meet current admission criteria, and if re-admitted, must fulfill current program requirements.

Notes for International Students

Language Proficiency

English Language Proficiency Test administered by the Indiana University Center for English Language Training (CELT). The exam is typically administered during the international student orientation held at the beginning of the fall and spring semesters.

English Course(s): Any International Student who received a form requiring English courses (Ling T101) must enroll in all the courses checked. These are required for graduation. Contact the CELT office or Richard Bier (855-0033) directly with any questions you may have about the exam.

Intensive English Program: The IEP is designed to support the development of English language skills. Incoming international students assigned as an Associate Instructor, and has a TOEFL score of 79 or below, or has not taken the TOEFL will be required to take the IEP exam. Students that do not pass the IEP exam will be required to take assigned English courses. For more information visit: http://www.indiana.edu/~dsh/eli/elp.html

AIship: Students whose native language is not English who would like to compete for teaching positions are required to take the “Test of English Proficiency for AI Candidates.” Students must pass this exam before they can be appointed to engage in the direct instruction of students at IU. If you have questions about the TEPAIC please check the website at http://www.indiana.edu/~deanfac/tepaic.

Maintaining Immigration Status

Course loads: International students should note that SEVIS regulations are
stringent about having a full course load, and that it's essential to check with International Services well in advance of any event that might affect visa status (e.g., dropping a course), to avoid the risk of deportation for being out of status. Check IU International Services' student page (http://ois.iu.edu/) for links to information on staying in status, to be sure that you are aware of the current policies.

**Completion dates for visa purposes:** International students are considered to have completed their degrees as soon as they have completed the degree requirements, regardless of whether they have filed for the degree. Consequently, it is essential to make sure that post-graduation visa arrangements are in place before completing the requirements. International Services is expert on these rules.

**Completion dates used for OPT applications:** For Optional Practical training, your date of graduation is normally the end of the semester in which you take the last courses needed for the degree, regardless of whether you will receive an incomplete in one of these courses. Even if you have an incomplete that prevents receiving your degree, you should expect the OPT to be processed using the normal completion date for your last courses (the last day of finals).

**Internship and Curricular Practical Training (CPT)**

International Students planning summer employment under the CPT program must enroll in I591 and complete the arrangements with International Services and the Computer Science Department outlined in the Curricular Practical Training I591 Authorization Form. All related forms (including those requiring an advisor signature) should be submitted to the Program Director. I591 is not allowed with a RAship or AIship, due to the policy that AIs and RAs are not allowed to take additional employment.

Authorization for I591 will be given for registration only when the MSS1 Professional Internship form is returned to the Computer Science program with the following information:

**BEFORE** starting internship, the student should

1. Provide for the CS Graduate Office:
   - Offer Letter: A formal letter offering the internship, which clearly identifying the company or organization, the dates of expected employment, and a description of the nature of the employment (Job title only WILL NOT be enough to be approved by OIS).
   - Completed I591 MSS1 Professional Internship form.
2. Register for Y798 – CS Professional Internship course
3. Complete information for the Office of International Services (OIS) on IStart

**AFTER** the Internship is completed, the student must provide the MSS1 program with an “Exit” letter - a formal letter from the employer stating that the term of employment or internship was satisfactorily completed. A pass/fail grade is assigned. This will turn to an "F" on the transcript one year after registration in the course unless the Exit letter is provided.
Example Elective Concentrations
These are examples of possible concentrations one might try to pursue with their electives credit. Students are welcome to make their own. These are examples of sets of courses where two or three are clearly well-matched. While every course has been offered, not every course will be offered in the forthcoming academic year.

There are others not listed here including bioinformatics, cognitive science, data mining, cyberinfrastructure, artificial intelligence, cognitive science, programming languages, databases, and logic.

Complex Systems
SLIS-S 604 INFORMATION NETWORKS
INFO-I 601 INTRODUCTION TO COMPLEX SYSTEMS
INFO-I 586 ARTIFICIAL LIFE
INFO-I 590 (TOPICS) VT: THE SIMPLICITY OF COMPLEXITY

Privacy
CSCI-B 649/INFO-I 590: ADVANCED TOPICS IN PRIVACY
INFO-I 609 ADVANCED SEMINAR: SOCIAL INFORMATICS
TEL-T 340 ELECTRONIC MEDIA ADVERTISING
TEL-T 353 ECONOMICS OF INFORMATION
TEL-T 321 TELECOMMUNICATIONS POLICYMAKING
SLIS-S 643 THE INFORMATION INDUSTRY
TEL-T 650 TELECOMM & THE CONSTITUTION

Social Informatics
INFO-I 504 SOCIAL DIMENSIONS OF SCIENCE INFORMATICS
INFO-I 506 GLOBALIZATION AND INFORMATION
INFO-I 651 ETHNOGRAPHY OF INFORMATION

Embedded Systems
CSCI-B441 DIGITAL DESIGN.
CSCI-B442 DIGITAL SYSTEMS.
CSCI-P545 EMBEDDED & REAL-TIME SYSTEMS.

Technology & Society
SLIS-S 514 COMPUTERIZATION IN SOCIETY
SLIS-S 680 THE BOOK TO 1450
SLIS-S 671 SCHOOL MEDIA

Content & Semantics
SLIS-S 636 SEMANTIC WEB
SLIS-S 532 INFO ARCHITECTURE FOR THE WEB
SLIS-S 642 CONTENT ANALYSIS FOR THE WEB

Psychology Concentration
PSY-P 647 DECISION MAKING UNDER UNCERTAINTY
PSY-P 533 INTRODUCTION TO BAYESIAN DATA ANALYSIS I
PSY-P 651 PERCEPTION/ACTION
PSY-P 654 MULTIVARIATE ANALYSIS
PSY-P 820 SOCIAL PERCEPTION

**Telecom Concentration**
TEL-T 504 INTRO TO TELECOMM POLICY STDS  
TEL-T 610 THE NETWORKED SOCIETY  
TEL-T 532 ECONOMICS OF MEDIA INDUSTRIES  
TEL-T 512 COMMUNICATION AND POLITICS  
TEL-T 650 TELECOMM & THE CONSTITUTION  
TEL-T 575 DIRECTED GRP NEW MEDIA DES PRJ

**Business Concentration**
BUS-F 421 DERIV SECURITS/CORP RISK MGMT  
BUS-F 525 CORPORATE FINANCIAL RISK MGMT (1.5 CR)  
BUS-K 490 IND STUDY IN DECISION SCIENCES (1-3 CR)  
SPEA-V 541 BENEFIT COST ANALYSIS
SPEA Concentration
SPEA-E 560 ENVIRONMENTAL RISK ANALYSIS
SPEA-V 673 PUB POL ANAL/MGMT SCI/OPR RSCH
SPEA-V 507 DATA ANALYS & MODELING-PUB AFF

Criminal Justice Concentration
CJUS-P 430 LAW AND THE LEGAL SYSTEM
FORENSICS
CJUS-P 595 DATA ANALYS IN CRIM JUSTICE I
CJUS-P 596 DATA ANALYS IN CRIM JUSTICE II