CYBERSECURITY AND INFORMATION ASSURANCE

In the last ten years, there has been much data demonstrating that there is a rapid rise in the incidence of cyber-attacks targeting individuals, organizations, and even countries. Consequently, cybersecurity and information assurance are the US government's top priorities, as seen in various Presidential Directives and the US Justice Department document High Priority Criminal Justice Technology Needs. The US has identified cybersecurity as one of the rising workforce areas, from both public and private sectors. The Bachelor of Science in Cybersecurity and Information Assurance (CIA) program at the Department of Computer and Information Science aims to educate and train an elite, diverse cadre of students, who are ready to address real-world computer security and criminal justice challenges. It will also benefit any individual who is interested in advancing their knowledge of computer security and privacy.

Cybersecurity and Privacy Concentration

The Cybersecurity and Privacy (CP) concentration educates students in the fundamentals and principles of cybersecurity and privacy and provides students with labs and experiences that encourage creative thinking. It is built upon a rigorous undergraduate background in computer and information science. Students in this concentration study fundamental security and privacy concepts such as confidentiality, integrity, access control, security architecture and systems, attack/defense. This concentration also provides a sequence of courses that cover unique security and privacy issues in various application areas, ranging from computer security to network security, from wired security to wireless security, from data security to application security, from every day security to enterprise security.

Digital Forensics Concentration

Digital Forensics (DF) is the area of computer science concerned with the examination and analysis of computer hard drives, storage devices, cell phones, tablets, or any electronic device that may hold evidence which could be used in a court of law. The device could be as simple as a cell phone or as complex as a main server for a large corporation. The digital forensics analyst uncovers and preserves data for later use as legal evidence, and analyzes the data in light of a particular crime or criminal or civil investigation. This may involve determining how hackers or unauthorized persons gained access to information or computer systems as well as where and how they navigated within the system.

Digital forensics specialists recover files and emails or other electronic correspondence that have been deleted or erased. They also recover data after hardware or software failure, and develop means to harden computer, cyber, and data security against loss, corruption, sabotage, or external attack.

Program Educational Objectives:

1. Our graduates will be successfully employed in Cybersecurity and Information Assurance related fields or other career paths, including industrial, academic, governmental, and non-governmental organizations, or will be successful graduate students in a program preparing them for such employment.
2. Our graduates will lead and participate in culturally diverse and inclusive teams, becoming global and ethical collaborators.
3. Our graduates will continue their professional development through, for example, obtaining continuing education credits, professional registration or certifications, or post-graduate study credits or degrees.

Student Outcomes:

To achieve the educational objectives of the program, graduates of the BS in CIA program will have an ability to:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
6. Apply security principles and practices to maintain operations in the presence of risks and threats.

Dearborn Discovery Core

Please see the Dearborn Discovery Core (General Education) (https://umdearborn.edu/dearborn-discovery-core/) webpage or additional information.

Foundational Studies

Writing and Communication (GEWO) – 6 Credits

Upper-Level Writing Intensive (GEWI) – 3 Credits

Quantitative Thinking and Problem Solving (GEQT) – 3 Credits

Critical and Creative Thinking (GECC) – 3 Credits

Areas of Inquiry

Natural Science (GENS) – 7 Credits

- Lecture/Lab Science Course
- Additional Science Course

Social and Behavioral Analysis (GESB) – 9 Credits

Humanities and the Arts (GEHA) – 6 Credits

Intersections (GEIN) – 6 Credits

Capstone

Capstone (GECE) – 3 Credits

In addition to completion of the Dearborn Discovery Core, the following courses are required to earn a B.S. degree in Cybersecurity and Information Assurance from UM-Dearborn.

Major Requirements

Code	Title	Credit Hours
Prerequisite Courses		
COMP 105	Writing & Rhetoric I	3
COMP 270	Tech Writing for Engineers (Also fulfills 3 credits of DDC Written and Oral Communication)	3

ECON 201	Prin: Macroeconomics	3
or ECON 202	Prin: Microeconomics	
MATH 115	Calculus I	4
MATH 116	Calculus II	4
MATH 227	Introduction to Linear Algebra	3
ACC 298	Financial Accounting	3
CIS 150	Computer Science I	4
CIS 200	Computer Science II	4
CIS 275	Discrete Structures I	4
CRJ 200	Intro to Criminal Justice (Also fulfills 3 credits of DDC Social and Behavioral Analysis)	3
IMSE 317	Eng Probability and Statistics	3
PHIL 240	Ethics (Also fulfills 3 credits of DDC Humanities and the Arts)	3
Select one laboratory science sequence from the following:		
BIOL 130 & BIOL 320	Intro Org and Environ Biology and Field Biology	
CHEM 134 & CHEM 136	General Chemistry IA and General Chemistry IIA	
GEOL 118 & GEOL 218	Physical Geology and Historical Geology	
PHYS 125 & PHYS 126	Introductory Physics I and Introductory Physics II	
PHYS 150 & PHYS 151	General Physics I and General Physics II	
CIA Major Core		
CIS 310	Computer Org and Assembly Lang	4
CIS 350	Data Struc and Algorithm Anlys	4
CIS 375	Software Engineering I	4
CIS 421	Database Mgmt Systems	4
CIS 427	Comp Networks and Dis Process	4
CIS 435	Web Technology	3
CIS 450	Operating Systems	4
CIS 4951	Design Seminar I	2
CIS 4952	Design Seminar II	2
OB 354	Behavior in Organizations (Also fulfills 3 credits of DDC Social and Behavioral Analysis)	3
Students must choose a concentration in Digital Forensics or Cybersecurity and Privacy. Concentration requirements listed below.		21-24

CIA Electives

Code	Title	Credit Hours
CIA Electives		**4-7**
Students must select electives not already used to fulfill the concentration or intersection requirements of your degree. Concentration courses and technical electives must total 28 credit hours.		
CIS 285	Software Engineering Tools	
CIS 299	Internship	
CIS 316	Prac. Comp. Sec.	
CIS 376	Software Engineering II	
CIS 381	Industrial Robots	
CIS 387	Digital Forensics I	
CIS 399	Internship	
CIS 411	Introduction to Natural Language Processing	
CIS 425	Information Systems	
CIS 436	Mobile App Des & Impl	
CIS 437	Advanced Networking	
CIS 439	Text Mining and Information Retrieval	
CIS 446	Wireless & Mobi Comp Security	
CIS 447	Intro Computr & Ntwrk Security	
CIS 449	Intro to Software Security	
CIS 467	Digital Forensics II	
CIS 476	Soft Arch & Design Patterns	
CIS 479	Intro to Artificial Intel	
CIS 483	Deep Learning	
CIS 4851	Data Security and Privacy	
CIS 487	Computer Game Design & Implem	
CIS 489	Edge Computing	
CIS 499	Internship	
CRJ 474	Cyber Crimes	
CRJ 475	Digital Evidence	
CRJ 487	Forensic Science Evidence in Criminal Cases	
CRJ 490	Topics in Criminal Jusice	
ECE 372	Intro to Microprocessors	
ECE 426	Multimedia Forensics	
ECE 427	Digi Content Protec	
ECE 428	Cloud Computing	
ECE 435	Intro to Mobil/Smrt Dev & Tech	
ECE 473	Embedded System Design	
ENGR 360	Design Thinking : Process, Method & Practice	
ENGR 399	Experiential Honors Prof. Prac	
ENGR 400	Appl Business Tech for Engr	
ENGR 492	Exper Honors Directed Research	
ENGR 493	Exper Hnrs Dir Dsgn	
ENT 400	Entrepreneurial Thinking&Behav	
IMSE 421	Eng Economy and Dec Anlys	
General Electives		**0-6**
Any 100 to 400 level course, (that is, courses not on the No Credit list, which is found at the end of the CECS Student Handbook), with no more than 6 credits, as needed to get a minimum of 120 credits for graduation.		

CIA students must choose a concentration in Cybersecurity and Privacy or Digital Forensics. Concentration requirements are listed below.

Cybersecurity and Privacy Concentration Requirements

Code	Title	Credit Hours
CIA-Cybersecurity and Privacy Required		**22**
CIS 316	Prac. Comp. Sec.	3
CIS 446	Wireless & Mobi Comp Security	3
CIS 447	Intro Computr & Ntwrk Security	3
CIS 4851	Data Security and Privacy	3
CRJ 409	Intel and Homeland Security	3

ECE 427	Digi Content Protec	4
or CIS 449	Intro to Software Security	
MATH 396	Introduction to Cryptography	3

Digital Forensics Concentration Requirements

Code	Title	Credit Hours
CIA-Digital Forensics Required		**23**
CIS 387	Digital Forensics I	4
CIS 467	Digital Forensics II	4
CIS 447	Intro Computr & Ntwrk Security	3
or ECE 426	Multimedia Forensics	
or ECE 427	Digi Content Protec	
CRJ 468	Criminology	3
CRJ 475	Digital Evidence	3
CRJ 487	Forensic Science Evidence in Criminal Cases	3
CRJ 409	Intel and Homeland Security	3
or CRJ 474	Cyber Crimes	

Learning Goals

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
6. Apply security principles and practices to maintain operations in the presence of risks and threats.