

# CYBERSECURITY AND INFORMATION ASSURANCE

The Master of Science in Cybersecurity and Information Assurance (CIA) is a 30-credit hour graduate degree offered by the Department of Computer and Information Science (CIS). This initiative reflects the University's eagerness to address rising needs of cybersecurity professionals in both the private and public sectors. The CIA program educates and trains an elite, diverse group of students who want to pursue a career in cybersecurity, such as cybersecurity analysts/specialists, cybersecurity engineers, network engineers/architects, software developers, etc. The program will also benefit anyone on this campus who is interested in advancing their knowledge of computer security and privacy, and it will offer a great opportunity for interdisciplinary inquiry and teaching.

This program can be completed fully online, in person, or a combination of both.

## Accelerated Master's Options for Undergraduate Students (4+1 Program)

Accelerated master's (4+1) programs in the Computer and Information Science (CIS) department allow qualified undergraduate students to seamlessly transition into the department's graduate programs. These programs will enable students to earn both a bachelor's and a master's degree in a reduced timeframe, enhancing their academic experience and providing a cost-effective pathway to advanced degrees.

Students enrolled in this option can take eligible 500-level courses during their junior and senior years, with up to 9 credit hours of such coursework being double-counted toward both degrees. Additionally, another 6 credit hours earned but not applied to the bachelor degree can later be counted toward the master's degree. Depending on the number of graduate courses taken while working toward the bachelor program, students will need to complete 15-21 credit hours to finish the master's program after earning their undergraduate degree.

BS in Computer and Information Science (CIS) or Software Engineering (SWE) can advance to MS in CIS, Data Science (DATA), Artificial Intelligence (AI), Software Engineering (SWE) or Cybersecurity and Information Assurance (CIA).

A maximum of 9 credits from combined undergraduate and graduate courses can be double-counted toward both the undergraduate and graduate degrees. This will streamline the process and reduce the total credit load required to complete both degrees. Any 500-level course that is part of the respective master's program can be selected for double-counting, as shown in the following table. If there is a mismatch in credit hours between the combined course pair, only the smaller number of credits will be counted.

In addition, students may apply up to 6 additional credits of 500-level courses toward their master's degree, taken during their undergraduate study, though these credits cannot be double-counted. This allows students to make substantial progress toward their graduate degree while still completing their undergraduate requirements. However, the courses of these six additional credits should be listed in the corresponding graduate program.

Applying to the 4+1/Accelerated option is a two-stage process coordinated with both your undergraduate and graduate advising teams.

For detailed instructions and application links, please visit the central 4+1 programs webpage (<https://umdearborn.edu/academics/program/41-programs/>).

The following undergraduate programs are approved for the MS-CIA 4+1 program:

1. BS in Computer Information Science (CIS)
2. BS in Software Engineering (SWE)

## Curriculum

To satisfy the requirements for the MS degree in Cybersecurity and Information Assurance, all students admitted to the program are expected to complete a minimum of 30 credit hours of graduate coursework, with a cumulative grade point average of B or better. The program of study consists of core courses, concentration courses and electives with coursework/project/thesis options. Students are required to choose one of the following three concentration areas for the program: (1) Network & System Security, (2) Data & Application Security, and (3) Software Security.

Minimum Grade Requirement in addition to maintaining a minimum cumulative GPA of 3.0 or higher every semester:

- Courses in which grades of C- or below are earned cannot be used to fulfill degree requirements.
- A minimum of a 3.0 cumulative GPA or higher is required at the time of graduation.

**Option 1:** MS Coursework. This option requires a minimum of 30 credits be earned through coursework. The minimum requirements are as follows:

- Core courses - 9 credit hours
- Concentration courses -12 credit hours
- Elective courses - 9 credit hours

**Option 2:** MS Project. This option requires a project report describing the results of an independent study project under the supervision of the advisor. The minimum requirements are as follows:

- Core courses - 9 credit hours
- Concentration courses -12 credit hours
- Elective courses - 6 credit hours
- Master's Project - 3 credit hours

**Option 3:** MS Thesis. This option requires a research thesis prepared under the supervision of the advisor. The minimum requirements are as follows:

- Core courses - 9 credit hours
- One concentration area - 12 credit hours
- Elective courses - 3 credit hours
- Master's Thesis - 6 credit hours

## Requirements

### Core Courses

Code	Title	Credit Hours
<b>Required:</b>		<b>6</b>
CIS 540	Foundation of Information Security	

CIS 564/ IMSE 570	Enterprise Information Systems	
<b>Select one of the following:</b>		<b>3</b>
ACC 601	Information Technology Auditing	
CIS 546	Security and Privacy in Wireless Networks <sup>1</sup>	
CIS 548	Security and Privacy in Cloud Computing	
<b>Total credit hours</b>		<b>9</b>

<sup>1</sup> Simultaneous credit toward eligible undergraduate majors and MS in Cybersecurity and Information Assurance for students admitted to the 4+1 option. Please see the College's website for admission requirements and program details.

### Elective Courses

The following specializations are provided for guidance only. Students are allowed to select elective courses from the same or different specializations. **An elective course should not be the same as any course taken to satisfy concentration course requirements.**

- **Option 1:** MS Coursework. Choose 9 credit hours (or 3 courses) from the following list below
- **Option 2:** MS Project. Choose 6 credit hours (or 2 courses) from the following list below and CIS 695 Master's Project for 3 credits.
- **Option 3:** MS Thesis. Choose 3 credit hours (or 1 course) from the following list below and CIS 699 Master's Thesis for 6 credits.

Code	Title	Credit Hours
Specialization 1: Security, Privacy, Forensics, and Auditing		
ACC 505	Devel & Interp Financial Info	3
CIS 544	Computer and Network Security <sup>1</sup>	3
CIS 545	Data Security and Privacy <sup>1</sup>	3
CIS 546	Security and Privacy in Wireless Networks <sup>1</sup>	3
CIS 548	Security and Privacy in Cloud Computing	3
CIS 549	Software Security <sup>1</sup>	3
CIS 584	Advanced Computer and Network Security	3
ECE 527	Multimedia Secur & Forensics	3
HHS 570	Information Science and Ethics	3
ISM 642	Cybersecurity and Networking	3
Specialization 2: Systems, Networks and Communications		
CIS 527	Computer Networks	3
CIS 537	Advanced Networking and Distributed Systems <sup>1</sup>	3
CIS 574	Compiler Design	3
CIS 578	Advanced Operating Systems	3
CIS 589	Edge Computing <sup>1</sup>	3
CIS 647	Research Advances in Networking and Distributed Systems	3
ECE 526	Multimedia Comm Sys	3
ECE 535	Mob Dev & Ubiqys Comp Sys	3
ECE 550	Communication Theory	3
ECE 5541	Embedded Networks	3
ECE 570	Computer Networks	3
ECE 5701	Intro to Wireless Comm	3
ECE 5702	High-Speed and Adv Networks	3
ECE 531	Intelligent Vehicle Systems	3

ISM 525	Fundamentals of Information Systems	3
Specialization 3: Data Management, Analytics, and Intelligent Systems		
CIS 536	Text Mining and Information Retrieval <sup>1</sup>	3
CIS 556	Database Systems <sup>1</sup>	3
CIS 5570	Introduction to Big Data	3
CIS 562	Web Information Management	3
CIS 568	Data Mining	3
CIS 5700	Advanced Data Mining	3
CIS 579	Artificial Intelligence <sup>1</sup>	3
CIS 581	Computational Learning <sup>1</sup>	3
CIS 583	Deep Learning <sup>1</sup>	3
CIS 585	Advanced Artificial Intelligence	3
CIS 586	Advanced Data Management	3
CIS 658	Research Advances in Data Management	3
ECE 531	Intelligent Vehicle Systems	3
ECE 537	Data Mining	3
ECE 552	Fuzzy Systems	3
ECE 579	Intelligent Systems	3
ECE 5831	Pat Rec & Neural Netwks	3
Specialization 4: Software Engineering		
CIS 505	Algorithm Analysis and Design <sup>1</sup>	3
CIS 525	Web Technology <sup>1</sup>	3
CIS 535	Wireless Technologies and Pervasive Computing	3
CIS 553	Software Engineering	3
CIS 565	Software Quality Assurance	3
CIS 566	Software Architecture and Design Patterns <sup>1</sup>	3
CIS 571	Web Services	3
CIS 575	Software Engineering Mgmt	3
CIS 577	S/W User Interface Dsgn&Analys	3
CIS 580	Data Analytics in Software Engineering	3
CIS 678	Research Advances in Software Engineering	3
CIS 577	S/W User Interface Dsgn&Analys	3
Specialization 5: Human Computer Interface Design		
IMSE 514	Multivariate Statistics	3
IMSE 559	System Simulation	3
IMSE 577	Human-Computer Interaction	3
IMSE 586	Big Data Aanal & Visuliztn	3
HCDE 530	Information Visualization	3
HCDE 540	Integrated Design Thinking and Implementation in Business	3
HCDE 510	Foundation of HCDE	3
HCDE 501	Human Factors and Ergonomics	3

<sup>1</sup> Simultaneous credit toward eligible undergraduate majors and MS in Cybersecurity and Information Assurance for students admitted to the 4+1 option. Please see the College's website for admission requirements and program details.

### Concentrations

12 credit hours from one of the three concentrations listed below:

## Data and Application Security

Code	Title	Credit Hours
<b>Required:</b>		<b>3</b>
CIS 545	Data Security and Privacy <sup>1</sup>	
<b>Select three from the following:</b>		<b>9</b>
CIS 548	Security and Privacy in Cloud Computing	
CIS 556	Database Systems <sup>1</sup>	
CIS 5570	Introduction to Big Data	
CIS 568	Data Mining	
CIS 581	Computational Learning <sup>1</sup>	
CIS 582	Trustworthy Artificial Intelligence <sup>1</sup>	
ECE 527	Multimedia Secur & Forensics	
HHS 570	Information Science and Ethics	
ISM 642	Cybersecurity and Networking	
<b>Total credit hours</b>		<b>12</b>

<sup>1</sup> Students admitted to the 4+1 program may substitute CIS 545 for CIS 4851, CIS 556 for CIS 421, CIS 581 for CIS 481, and CIS 582 for CIS 482.

## Network and System Security

Code	Title	Credit Hours
<b>Required:</b>		<b>3</b>
CIS 544	Computer and Network Security <sup>1</sup>	
<b>Select three from the following:</b>		<b>9</b>
CIS 512	Introduction to Quantum Computing <sup>1</sup>	
CIS 527	Computer Networks	
CIS 535	Wireless Technologies and Pervasive Computing	
CIS 537	Advanced Networking and Distributed Systems <sup>1</sup>	
CIS 546	Security and Privacy in Wireless Networks <sup>1</sup>	
CIS 578	Advanced Operating Systems	
CIS 584	Advanced Computer and Network Security	
CIS 624	Research Advances in Computer and Network Security	
ECE 5541	Embedded Networks	
<b>Total credit hours</b>		<b>12</b>

<sup>1</sup> Students admitted to the 4+1 program may substitute CIS 512 for CIS 412, CIS 537 for CIS 437, CIS 544 for CIS 447, and CIS 546 for CIS 446.

## Software Security

Code	Title	Credit Hours
<b>Required:</b>		<b>3</b>
CIS 549	Software Security <sup>1</sup>	
<b>Select three from the following:</b>		<b>9</b>
CIS 525	Web Technology <sup>1</sup>	
CIS 553	Software Engineering	
CIS 565	Software Quality Assurance	
CIS 566	Software Architecture and Design Patterns <sup>1</sup>	
CIS 574	Compiler Design <sup>1</sup>	
CIS 578	Advanced Operating Systems	

CIS 579	Artificial Intelligence <sup>1</sup>	
CIS 580	Data Analytics in Software Engineering	
<b>Total credit hours</b>		<b>12</b>

<sup>1</sup> Students admitted to the 4+1 program may substitute CIS 549 for CIS 449, CIS 525 for CIS 435, CIS 566 for CIS 476, and CIS 574 for CIS 474. CIS 579 for CIS 479.

## Learning Goals

1. Students will be able to understand fundamentals and the state of the art of cyber technology, their security and privacy risks, and defenses.
2. Students will be able to analyze and evaluate potential security risks of computer and information systems.
3. Students will be able to design, coordinate, and deliver cybersecurity solutions in a timely and cost-effective manner.
4. Students will be able to interpret security risks and solutions and communicate the implications to stakeholder