Bachelor of Science in Information Systems Security

The Bachelor of Science in Information Systems Security combines educational theory with the technical skills required to meet information security needs across the enterprise. This online bachelor’s degree brings you coursework in information assurance, information security, network design and engineering, business continuity, and more. Learning the technological skills required to protect organizational assets from unscrupulous business competitors or unfriendly combatants is paramount to the credibility and survival of businesses, government agencies, and military operations. This online degree program helps to prepare you for careers such as information security manager, analyst, auditor, consultant, or risk assessor.

Degree Program Objectives

In addition to the institutional and general education level learning objectives, this degree also seeks the following specific learning outcomes of its graduates:

- Use analytical, logical, and critical thinking to analyze user requirements and to design, develop, and deploy effective Information Systems Security solutions.
- Analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management for wired, wireless, and web-based networks.
- Prescribe Information Assurance initiatives to protect an organization’s information assets by ensuring availability, confidentiality, integrity, authenticity, and non-repudiation.
- Develop a security architecture consisting of tools, techniques, and technologies to prevent the penetration of networks, to detect attacks, and to design effective countermeasures.
- Generate a risk assessment and risk mitigation methodology to analyze and manage risks in the context of Network Security.
- Apply the discipline of network attack and defense to develop effective countermeasures to keeping hackers outside the perimeter of the network.
- Develop Network Security audit practices, processes, and plans, and specify the roles and responsibilities of the staff on the audit team.
- Develop actionable and maintainable network and information security plans and policies that address physical security, authentication, network security, encryption, software development, email, internet, acceptable use, acceptable speech, and viruses/worms.

Degree at a Glance

General Education Requirements 30
Major Required 42
Select one of the following concentrations: 15
    General Concentration (p. 3)
    Cloud Computing (p. 3)
    Cyber Intelligence (p. 3)
    Cybercrime Investigations (p. 4)
    Cybersecurity (p. 4)
    Digital Forensics (p. 4)
    Homeland Security (p. 5)
    Wireless and Mobile Security (p. 5)
Final Program Requirements 3
Electives 30
Total Semester Hours 120

Degree Program Requirements

General Education Requirements (30 semester hours)

Arts and Humanities (6 semester hours) 1
Select 2 courses from the following: 6
    ARTH200 Art Appreciation
    ARTH241 Film and Literature
    DSIN141 Image Enhancement using Adobe Photoshop
    LITR201 World Literature through the Renaissance
    LITR202 World Literature since the Renaissance
    LITR210 English Literature: Beowulf to 18th Century
    LITR211 English Literature: 18th Century to Present
    LITR220 American Literature before The Civil War
    LITR221 American Literature from The Civil War to Present
    ARAB100 Arabic I
    ARAB101 Arabic II
    FREN100 French I
    FREN101 French II
    GERM100 German I
    GERM101 German II
    JAPN100 Introduction to Japanese
    MUSI200 Music Appreciation
    PHIL101 Introduction to Philosophy
    PHIL110 Critical Thinking
    PHIL200 Introduction to Ethics
    PHIL202 Philosophy of Science
Bachelor of Science in Information Systems Security

PORT100  Introduction to Brazilian Portuguese
RELS201  Introduction to World Religions
RUSS100  Russian I
SPAN100  Spanish I
SPAN101  Spanish II

Civics, Political and Social Sciences (6 semester hours)
Select 2 courses from the following:
- ANTH100  Introduction to Anthropology
- ANTH202  Introduction to Cultural Anthropology
- CHFD220  Human Sexuality
- COMM211  Social Media and Society
- COMM240  Intercultural Communication
- ECON101  Microeconomics
- ECON102  Macroeconomics
- EDUC200  Humane Education: A Global Interdisciplinary Perspective
- GEOG101  Introduction to Geography
- HOSP110  Practical Food Safety and Awareness
- IRLS210  International Relations I
- LITR204  Contemporary World Culture Through Literature
- LITR205  Cultural Diversity in Contemporary American Literature
- POLS210  American Government I
- PSYC101  Introduction to Psychology
- SOCI111  Introduction to Sociology
- SOCI212  Social Problems
- SOCI220  American Popular Culture

Communication: Writing, Oral, and Multimedia (8 semester hours)
- COMM110  Information & Digital Literacy
- ENGL110  Making Writing Relevant
Select 1 course from the following:
- COMM200  Public Speaking
- ENGL102  Effectiveness in Writing
- ENGL200  Composition and Literature
- ENGL220  Technical Writing
- ENGL221  Scientific Writing
- ENGL225  Business Writing
- HRMT101  Human Relations Communication
- IRLS200  Information Literacy and Global Citizenship
- ITCC231  Introduction to Information Technology Writing
- MGMT100  Human Relations

History (3 semester hours)
Select 1 course from the following:
- HIST101  American History to 1877
- HIST102  American History since 1877
- HIST111  World Civilization before 1650
- HIST112  World Civilization since 1650
- HIST121  Western Civilization before The Thirty Years War
- HIST122  Western Civilization since The Thirty Years War
- HIST221  African-American History before 1877
- HIST222  African-American History since 1877
- HIST223  History of the American Indian
- HIST270  History of Science

Mathematics and Applied Reasoning (3 semester hours)
Select 1 course from the following:
- ACCT105  Accounting for Non Accounting Majors
- ENTD200  Fundamentals of Programming
- MATH110  College Algebra
- MATH111  College Trigonometry
- MATH120  Introduction to Statistics
- MATH125  Math for Liberal Arts Majors
- MATH225  Calculus

Natural Sciences with Lab (4 semester hours)
Select 1 course from the following:
- SCIN121  Habitable Worlds Are We Alone with Lab
- SCIN130  Introduction to Biology with Lab
- SCIN131  Introduction to Chemistry with Lab
- SCIN132  Introduction to Human Anatomy & Physiology with Lab
- SCIN133  Introduction to Physics with Lab
- SCIN134  Introduction to Astronomy with Lab
- SCIN137  Introduction to Meteorology with Lab
- SCIN140  Introduction to Environmental Science with Lab

Total Semester Hours 30

1. All literature courses require successful completion of ENGL101 - Proficiency in Writing or ENGL110 - Making Writing Relevant.

Major Required (42 semester hours)

- ENTD261  Scripting Languages for the Administrator
- ISSC422  Information Security
- ISSC421  Computer and Network Security
- INTL440  Cyber Warfare
- ISSC342  Operating Systems: Hardening and Security
- ISSC351  Computer Forensics
- ISSC361  Information Assurance
- ISSC362  IT Security: Attack & Defense
- ISSC363  IT Security: Risk Management
- ISSC471  IT Security: Auditing
- ISSC481  IT Security: Planning and Policy
Bachelor of Science in Information Systems Security

ITMG381  Cyberlaw and Privacy in a Digital Age  3
ISSC451  Cybercrime  3
ISSC431  Database Systems Security  3
Total Semester Hours  42

Students must choose a concentration for this degree program and may select from a General Concentration, Concentration in Cloud Computing, Concentration in Cyber Intelligence, Concentration in Cybercrime Investigations, Concentration in Cybersecurity, Concentration in Digital Forensics, Concentration in Homeland Security, or a Concentration in Wireless and Mobile Security.

General Concentration Requirements (15 semester hours)

A general concentration allows you to take courses across a number of areas of study within your program based on your own interests.

Concentration Requirements (15 semester hours)

Select 5 courses from the following:

Select 5 courses from the following: 15

ENTD381  Object Oriented Programming With Java
ISSC331  Legal Issues in Information Security
ISSC344  Open Source System Security
ISSC364  IT Security: Access Control and Authentication
ISSC411  Application Security
MATH302  Statistics
ISSC325  Biometrics
ISSC341  Introduction to Networking
ISSC343  Wireless Networks
ISSC366  IT Security: Cryptography
ISSC424  Virtualization Security
ISSC426  Cloud Security and Privacy
ISSC452  Cybersecurity
ISSC455  Digital Forensics: Investigation Procedures and Response
ISSC456  Digital Forensics: Investigating Wireless Networks and Devices
ISSC457  Digital Forensics: Investigating Network Intrusions and Cybercrime Security
ISSC458  Digital Forensics: Investigating Data and Image Files
ISSC459  Digital Forensics: Hard Disc and Operating Systems
ISSC461  IT Security: Countermeasures
ISSC490  IT Security: Business Continuity
Total Semester Hours  15

Concentration in Cloud Computing (15 semester hours)

Explores cloud computing’s key principles, security, and privacy. Examines how to use resources for service specifications and contracts for proper management of cloud services, decision making and management techniques for best practices and organizational growth, and green IT.

Concentration Requirements (15 semester hours)

ISSC326  Cloud Computing  3
ISSC345  Service Oriented Architecture  3
ISSC386  Green Computing: Foundations and Strategies  3
ISSC424  Virtualization Security  3
ISSC426  Cloud Security and Privacy  3
Total Semester Hours  15

Concentration in Cyber Intelligence (15 semester hours)

Infiltration in an organization’s systems may have already been targeted covertly and waiting for an appropriate moment for a beneficial attack by the adversary. Through information collection, social engineering, and reverse engineering of applications, cyber intelligence gives the tools necessary not only for an organization to protect its systems but also for the adversary to attack them with the same means. A complete vulnerability and threat analysis of all systems, cyber operational processes and policies in place, and revamping to build more resilient systems is key to stopping the adversary her path to approaching, attacking, or damaging the organization’s systems. This concentration prepares the student to protecting systems targeted at multiple levels based on various laws, regulations, and Presidential directives. Possible target careers include: Cyber Intelligence Analyst, Cyber Threat Intelligence Analyst, Cyber Threat Analyst, and Cybersecurity Intelligence Analyst.

Objectives

Upon completion of this concentration, students will be able to:

- Examine the homeland security threat landscape through risks, threats, and consequences facing critical homeland security infrastructure.
- Demonstrate comprehensive knowledge of counterintelligence through its role of supporting the United States counterterrorism and cyberspace activities, functions, and cyberspace operations for guarding and protecting the nation.
• Examine the history, collections platforms, doctrinal employment, and the application of Signals Intelligence against current and future threats and challenges to national security.
• Demonstrate a solid understanding of assessment of threats to states through vulnerabilities of non-state actors.
• Through the use of various tools identify problems with confidentiality, integrity, and availability arising from the increased use of cyber technology and its devices.

Concentration Requirements (15 semester hours)

HLSS320  Intelligence and Homeland Security  3
INTL410  Counterintelligence  3
INTL421  Signals Intelligence and Security  3
INTL434  Threat Analysis  3
ISSC452  Cybersecurity  3
Total Semester Hours  15

Concentration in Cybercrime Investigations (15 semester hours)

Cybercrime is on the rise resulting in billions of dollars in loss annually. The Federal Bureau of Investigation, the lead federal agency for investigating cyberattacks is working around the clock, on finding the targeting adversaries. Understanding how the adversary designs, plans, and attacks is a skill highly sought after in multiple sectors across the job market. Possible target careers include: Cyber Investigator, Cyber Action Team, Investigative Specialist, and Evidence Response Team.

Objectives

Upon completion of this concentration, students will be able to:

• Demonstrate the role of the courts in the reformation of the U.S. criminal justice system and its relationship between the law and theories of crime to the justice policies and processes.
• Analyze the procedures for conducting a criminal investigation, interview and interrogation, and the process of preserving the integrity and chain of custody for a crime scene.
• Examine the current use of intelligence in law enforcement and its applications in support of investigations and operational planning.
• Utilize various crime analysis tools to effectively reduce crime and improve policy efficiency in preventing criminal activity relative to societal interdependencies.
• Through the use of various tools identify problems with confidentiality, integrity, and availability arising from the increased use of cyber technology and its devices.

Concentration Requirements (15 semester hours)

CMRJ303  Criminology  3
CMRJ306  Criminal Investigation  3
CMRJ320  Law Enforcement Intelligence Applications  3
CMRJ335  Crime Analysis  3
ISSC452  Cybersecurity  3
Total Semester Hours  15

Concentration in Cybersecurity (15 semester hours)

Covers the processes and goals of cyber forensics investigations, and explores federal and state laws and legal concepts affecting how governments and organizations think about information security. Teaches the importance of search warrants and chain of custody in forensic investigations. Examines cybersecurity regulatory standards and compliance requirements, and explores technologies needed to detect, investigate, and prevent computer-related crimes.

Concentration Requirements (15 semester hours)

ISSC331  Legal Issues in Information Security  3
ISSC325  Biometrics  3
ISSC343  Wireless Networks  3
ISSC452  Cybersecurity  3
ISSC457  Digital Forensics: Investigating Network Intrusions and Cybercrime Security  3
Total Semester Hours  15

Concentration in Digital Forensics (15 semester hours)

Explores common incident response procedures and the forensics of wireless network attacks caused by mobile and wireless peripheral devices. Examines security and access procedures and how search warrants, chains of custody, and investigation logs impact digital investigations. Topics include basic tracking techniques and computer-related crimes, image file analysis, crime prevention techniques, and password cracking on various operating systems.

Concentration Requirements (15 semester hours)

ISSC455  Digital Forensics: Investigation Procedures and Response  3
ISSC456  Digital Forensics: Investigating Wireless Networks and Devices  3
ISSC457  Digital Forensics: Investigating Network Intrusions and Cybercrime Security  3
### Concentration in Homeland Security (15 semester hours)

Critical infrastructures at the national level are continually targeted by the adversary through cyberattacks, cyberespionage, and cyber hacktivism. Assessing vulnerabilities and threats, increasing levels of protection and prevention against such threats, addressing cyber operational processes, and mitigating and building more resilient systems is key to the prevention of future cyberattacks of the nation’s infrastructure and systems. This concentration expands on a holistic approach to cybersecurity and cyber operations. Possible target careers include: Cyber Incident Prevention and Response Team, Cyber Risk and Strategic Analyst, Cyber Intelligence Analyst, Cyber Threat Intelligence Analyst, Cyber Threat Analyst, and Homeland Security Cyber Intelligence Analyst.

#### Objectives

Upon completion of this concentration, students will be able to:

- Examine risk management in homeland security operations, its capabilities and limitations for homeland security support through assessments of United States critical infrastructure protection programs.
- Examine the roles and responsibilities of U.S. intelligence community members at the federal, state, and local levels, which support homeland security strategic process and operations.
- Examine the homeland security threat landscape through risks, threats, and consequences facing critical homeland security infrastructure.
- Examine the history, collections platforms, doctrinal employment, and the application of Signals Intelligence against current and future threats and challenges to national security.
- Through the use of various tools identify problems with confidentiality, integrity, and availability arising from the increased use of cyber technology and its devices.

#### Concentration Requirements (15 semester hours)

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>HLSS302</td>
<td>Introduction to Homeland Security and Defense</td>
<td>3</td>
</tr>
<tr>
<td>HLSS303</td>
<td>Homeland Security Risk, Threats and Consequences</td>
<td>3</td>
</tr>
<tr>
<td>HLSS320</td>
<td>Intelligence and Homeland Security</td>
<td>3</td>
</tr>
<tr>
<td>INTL421</td>
<td>Signals Intelligence and Security</td>
<td>3</td>
</tr>
</tbody>
</table>

### Concentration in Wireless and Mobile Security (15 semester hours)

Mobile devices have become very common with everyone in everyday use – often using multiple mobile devices, cellular, Tablets, e-Readers, wearables and implantable electronics, etc., in addition to laptops and notebooks, simultaneously. These devices use wireless and mobile networks and downloadable applications and software, opening a wide array of security and privacy issues unsuspected by the user. This concentration for the Bachelors of Science in Information Systems Security will allow students to specialize in the methodologies used to secure the networks, hardware – devices, software – apps, and the laws and regulations, policies and procedures, and ethical responsibilities for privacy and security of mobile devices using mobile and wireless network infrastructures. The concentration will emphasize countermeasures taken to harden the security of various aspects of mobile technologies associated to government, military, industry, educational, and private enterprises.

#### Objectives

Upon successful completion of this concentration, students will be able to:

- Examine current mobile and wireless networks, their architecture, infrastructure, and various utilized components.
- Extrapolate threats and vulnerabilities introduced into the network infrastructures of wireless, mobile, cellular, and satellite technologies.
- Examine current mobile application models, their security framework, and methodologies on hardening the security to safeguard the devices running them.
- Appraise security hardening techniques for wireless or mobile device technologies based on wireless security principles and current industry standards.
- Compare and contrast the needs of law-enforcement versus individual right-to-privacy in wireless infrastructures.
- Prepare a group presentation or individual written assignment on a relevant wireless or mobile security topic.

#### Concentration Requirements (15 semester hours)

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISSC343</td>
<td>Wireless Networks</td>
<td>3</td>
</tr>
<tr>
<td>ISSC412</td>
<td>Mobile Application Security</td>
<td>3</td>
</tr>
<tr>
<td>ISSC415</td>
<td>Mobile Device Security</td>
<td>3</td>
</tr>
<tr>
<td>ISSC442</td>
<td>Wireless and Mobile Network Security</td>
<td>3</td>
</tr>
</tbody>
</table>
Bachelor of Science in Information Systems Security

ITMG381  Cyberlaw and Privacy in a Digital Age  3

Total Semester Hours  15

Final Program Requirements (3 semester hours)

ISSC498  IT Security: Implementation Plan: Capstone (to be taken as the last course before graduation)  3

Total Semester Hours  3

Prerequisite: ENGL101 - Proficiency in Writing or ENGL110 - Making Writing Relevant and Senior Standing and completion of all major courses prior to enrollment.

Electives (30 semester hours)

Select any courses that have not been used to fulfill major requirements. Credits applied toward a minor or certificate in an unrelated field may be used to fulfill elective credit for the major.