DEPARTMENT OF INFORMATION SYSTEMS AND CYBERSECURITY

Mission Statement

The Department of Information Systems and Cybersecurity empowers the next generation of technology professionals through cutting-edge undergraduate and graduate programs that blend academic rigor with real-world relevance. We prepare students to explore and excel in the fields of information systems, cybersecurity, and data analytics by fostering critical thinking, hands-on experience, and ethical leadership.

Our programs offer a strong foundation in technology while evolving continuously to reflect the pace of innovation. Our commitment to student success, employer needs, and societal impact drives our curriculum design, emphasizing the latest advancements in artificial intelligence/machine learning, behavioral security, cloud computing, data privacy, digital forensics, industrial control systems, and Internet-of-Things.

Degrees

- M.S. in Information Technology
  - Cybersecurity Concentration
  - Cyber Analytics Concentration
  - Dual M.S.I.T with a Cyber Security Concentration/Master in Cybersecurity
- Ph.D. in Information Technology

Certificates

- Graduate Certificate in Cybersecurity
- Graduate Certificate in Cloud Computing
- Graduate Certificate in Intelligence Studies

Degree-Specific Requirements

All program requirements should be unchanged from previous versions of the 2025-2027 Graduate Catalog. To confirm your degree requirements, you can visit DegreeWorks (https://dworkswebprod.sis.utsa.edu/) or consult your Graduate Advisor of Record.

- M.S. in Information Technology (p. 1)
  - Cyber Security Concentration (p. 2)
  - Cyber Analytics Concentration (p. 2)
  - Dual M.S.I.T. with a Cyber Security Concentration / Master in Cybersecurity
- Ph.D. in Information Technology (p. 3)

Master of Science Degree in Information Technology

The Master of Science degree in Information Technology (M.S.I.T.) provides information systems and computer science professionals with the opportunity to acquire technical knowledge in a variety of specialized information technology fields and the management skills to create, plan, organize, lead, and control the information technology in their organizations. The program is designed for students with a technical background and preferably an undergraduate or graduate degree in information systems or computer science.

Program Admission Requirements

For admission to the M.S.I.T. program, applicants must meet University-wide graduate admission requirements. Applicants are further considered on the basis of demonstrated potential for success in graduate study in information technology as indicated by a combination of prior academic achievement, personal statement, résumé (optional), and references (optional).

The M.S.I.T. Graduate Program Committee evaluates each applicant individually based on the complete package of submitted materials.

A complete application package will include:

- A completed application form.
- Transcripts from all universities attended.
- A personal statement.
- A current résumé with employment or other experience (optional).
- Letters of reference (optional).

Graduate admission test scores are no longer required. However, please note that competitive GMAT/GRE scores may help your chances of admission because, in addition to your GPA, the GMAT or GRE provides a quantitative metric for the M.S.I.T. Programs Committee to evaluate you as a candidate.

Degree Requirements

Candidates for the degree of Master of Science in Information Technology (M.S.I.T.) must complete the following:

Code	Title	Credit Hours
A. 9 semester credit hours of required courses:		**9**
IS 5143	Information Technology	
IS 5203	Networking and Telecommunication Systems	
IS 6813	Strategic Management of Information Technology [1]	
B. All candidates for the degree must complete an additional 24 semester credit hours of elective courses:		
1. 18 semester credit hours selected from the following:		18
CS 5103	Software Engineering	
CS 5443	Database Management Systems	
CS 6543	Networks	
IS 6083	Agile Project Management	
IS 6303	Introduction to Voice and Data Security	
IS 6323	Security Risk Analysis	
IS 6343	Secure Network Designs	
IS 6353	Security Incident Response	
IS 6363	Digital Forensics	
IS 6373	Cyber Law	
IS 6383	Policy Assurance for Infrastructure Assurance	
IS 6423	Secure Software Design	
IS 6433	Supervisory Control and Data Acquisition	
IS 6503	Principles of Database Management	

IS 6703	Introduction to Data Mining	
IS 6933	Internship in Information Technology	
2. 6 semester credit hours selected from the following:		6
MBA 5213	Management and Behavior in Organizations	
MGT 5093	Leadership	
MOT 5053	Technology Commercialization	
MOT 5163	Management of Technology	
MOT 5223	Management of Professional Personnel	
MOT 5243	Essentials of Project Management	
MOT 5253	Starting the High-Tech Firm	
MOT 5313	Emerging Technologies	
Total Credit Hours		**33**

[1] Students who earn a grade of "B" (3.0) or better in IS 6813 Strategic Management of Information Technology will satisfy the comprehensive examination requirement. A student who receives a grade of "B-," "C+," or "C" may still satisfy the requirement by successfully passing a comprehensive examination as set out in this catalog.

Master of Science Degree in Information Technology – Cybersecurity Concentration

This concentration is designed to offer the opportunity for qualified graduate students to study information technology while developing special expertise in cybersecurity. To achieve this end, students can focus their elective courses on developing the specialized knowledge requirements for the computer and information security area while at the same time completing the requirements for the Master of Science (M.S.) degree.

Candidates for the degree of Master of Science in Information Technology (M.S.I.T.) with a concentration in Cybersecurity must complete the following:

Code	Title	Credit Hours
A. 15 semester credit hours of required courses:		**15**
IS 5143	Information Technology	
IS 5203	Networking and Telecommunication Systems	
IS 6303	Introduction to Voice and Data Security	
IS 6323	Security Risk Analysis	
IS 6813	Strategic Management of Information Technology [1]	
B. All candidates for the degree must complete an additional 18 semester credit hours of elective courses:		
1. 12 semester credit hours selected from the following:		12
IS 6343	Secure Network Designs	
IS 6353	Security Incident Response	
IS 6363	Digital Forensics	
IS 6373	Cyber Law	
IS 6383	Policy Assurance for Infrastructure Assurance	
IS 6423	Secure Software Design	
IS 6433	Supervisory Control and Data Acquisition	
IS 6603	Cyber Threat Hunting	
IS 6703	Introduction to Data Mining	
IS 6943	Internship in Cyber Security	
IS 6953	Independent Study	
IS 6973	Special Problems	
NS 6503	Intelligence Reasoning Analysis	
2. 6 semester credit hours selected from the following:		6
MBA 5213	Management and Behavior in Organizations	
MGT 5093	Leadership	
MOT 5053	Technology Commercialization	
MOT 5163	Management of Technology	
MOT 5223	Management of Professional Personnel	
MOT 5243	Essentials of Project Management	
MOT 5253	Starting the High-Tech Firm	
MOT 5313	Emerging Technologies	
Total Credit Hours		**33**

[1] Students who earn a grade of "B" (3.0) or better in IS 6813 will satisfy the comprehensive examination requirement. A student who receives a grade of "B-," "C+," or "C" may still satisfy the requirement by successfully passing a comprehensive examination as set out in this catalog.

Master of Science Degree in Information Technology – Cyber Analytics Concentration

This concentration is designed to offer the opportunity for qualified graduate students to study information technology while developing special expertise in cyber analytics. To achieve this end, students can focus their elective courses on developing the specialized knowledge requirements for the cybersecurity and analytics areas while at the same time completing the requirements for the Master of Science (M.S.) degree.

Candidates for the degree of Master of Science in Information Technology (M.S.I.T.) with a concentration in Cyber Analytics must complete the following:

Code	Title	Credit Hours
A. 18 semester credit hours of required courses:		**18**
IS 5143	Information Technology	
IS 5203	Networking and Telecommunication Systems	
IS 6303	Introduction to Voice and Data Security	
IS 6323	Security Risk Analysis	
IS 6713	Data Foundations	
IS 6813	Strategic Management of Information Technology	
B. All candidates for the degree must complete an additional 15 semester credit hours of elective courses:		
1. 6 semester credit hours selected from the following:		6
IS 6223	Intrusion Detection and Incident Response Essentials	
IS 6343	Secure Network Designs	
IS 6353	Security Incident Response	
IS 6423	Secure Software Design	

IS 6433	Supervisory Control and Data Acquisition	
IS 6603	Cyber Threat Hunting	
IS 6943	Internship in Cyber Security	
IS 6953	Independent Study	
IS 6973	Special Problems	
NS 6503	Intelligence Reasoning Analysis	
2. 9 semester credit hours selected from the following:		9
IS 6733	Deep Learning on Cloud Platforms	
DA 6213	Data-Driven Decision Making and Design	
DA 6223	Data Analytics Tools and Techniques	
DA 6813	Data Analytics Applications	
IS 6953	Independent Study	
Total Credit Hours		**33**

[1] Students who earn a grade of "B" (3.0) or better in IS 6813 (https://catalog.utsa.edu/search/?P=IS%206813) will satisfy the comprehensive examination requirement. A student who receives a grade of "B-," "C+," or "C" may still satisfy the requirement by successfully passing a comprehensive examination as set out in this catalog.

Dual Degree M.S.I.T. with a Cyber Security Concentration / Master in Cybersecurity

This dual degree program is offered through the UT San Antonio College of AI, Cyber and Computing (CAICC), M.S.I.T. Cybersecurity concentration program, and the Instituto Tecnologico de Monterrey (ITESM), Master in Cybersecurity program.

It is designed to offer the opportunity for qualified graduate students to take coursework in information technology while developing special expertise in cybersecurity at both institutions on a coordinated basis.

Applicants will be admitted to the M.S.I.T. Cybersecurity concentration program and the Master's in Cybersecurity independently, according to the admission schedule and policies of each institution. Applicants must submit all admission materials to each admission office independently and by the institution's deadline. Admission to the dual degree program may occur after a student has already matriculated in the M.S.I.T. Cybersecurity or in the Master's in Cybersecurity, or both degree programs, as approved by each institution's program director.

Upon completion, CAICC will award the M.S.I.T. Cybersecurity Concentration and ITESM will award the Master in Cybersecurity for each student who successfully completes the program.

Program Admission Requirements

For admission to the M.S.I.T. program with a Cybersecurity concentration, applicants must meet University-wide graduate admission requirements. Applicants are further considered on the basis of demonstrated potential for success in graduate study in information technology as indicated by a combination of prior academic achievement, personal statement, résumé (optional), and references (optional).

The M.S.I.T. Graduate Program Committee evaluates each applicant individually based on the complete package of submitted materials.

A complete application package will include:

- A completed application form.
- Transcripts from all universities attended.
- A personal statement.
- English proficiency test scores (If applicable)
- Foreign credential evaluation (If applicable)

Current résumé with employment or other experience and letters of reference are optional for this program.

Degree Requirements

For UT San Antonio students:

Program participants from UT San Antonio will enroll in UT San Antonio's M.S.I.T. Cybersecurity Concentration program and successfully complete the program's core requirements.

Students in the dual program who begin their education at UT San Antonio will take six (6) of 11 courses to fulfill the UT San Antonio M.S.I.T. Cybersecurity program requirement at UT San Antonio and the remaining five (5) courses at ITESM.

To earn the ITESM Master in Cybersecurity degree, UT San Antonio students must also complete a research essay jointly supervised by faculty members from both UT San Antonio and ITESM.

Additional information about the ITESM component for this dual program is available at https://maestriasydiplomados.tec.mx/posgrados/maestria-en-ciberseguridad-en-linea.

For ITESM students:

Program participants from ITESM will enroll in ITESM Master in Cybersecurity program the first semester and successfully complete their core requirements.

Students in the Dual Program will take 18 credit hours (six courses) at UT San Antonio, as well as completing a research essay jointly supervised by faculty members from both UT San Antonio and ITESM.

The requirements listed here may change as determined by UT San Antonio and ITESM. Students are required to contact their respective institution program director to review and confirm eligibility and detailed degree requirements.

Doctor of Philosophy Degree in Information Technology

The College of AI, Cyber and Computing offers opportunities for advanced study and research leading to the Doctor of Philosophy degree in Information Technology. The Ph.D. in Information Technology is awarded to candidates who have displayed an in-depth understanding of the subject matter and demonstrated the ability to make an original contribution to knowledge in their field of specialty (e.g., Information Systems, Cybersecurity and Analytics/AI).

The regulations for this degree comply with the general University regulations (refer to Student Policies, General Academic Regulations, and the Graduate Catalog, Doctoral Degree Regulations).

Admission Requirements

Applicants must have a bachelor's degree from an accredited university. The Ph.D. Program Committee in the major areas will evaluate applicants to the Ph.D. program based on several factors, including academic achievement, standardized test scores, employment history, a personal

statement, letters of recommendation, and possibly an interview. All applicants must submit the following material for evaluation:

- Official transcripts of all undergraduate and graduate coursework completed
- Graduate Management Admission Test (GMAT) scores or Graduate Record Examination (GRE) scores from a recent (no more than five years old) administration of the examination
- Three letters of recommendation from academic or professional sources familiar with the applicant's background
- A résumé or curriculum vitae and a statement of academic interests and goals
- International students must also submit a score of at least a 79 on the Test of English as a Foreign Language (TOEFL) iBT. TOEFL scores may not be more than two years old.

Candidates who do not possess a master's degree in a related discipline (e.g. Information Systems, Computer Science, Cybersecurity and Analytics/AI), with sufficient quantitative rigor are required to complete a program consisting of a minimum of 75 semester credit hours. The Ph.D. Program Committee for the major area discipline will determine a degree program for each candidate based upon that candidate's particular background. Candidates whose backgrounds are determined to be insufficient may be directed to take additional background or leveling courses (see sections A, B, and C of the Program of Study below) before proceeding to the program's required courses. Candidates who enter the program with the appropriate prior graduate coursework may be waived from some or all of the background requirements (sections A, B, and C).

Admission may include an appointment to a teaching assistantship, research assistantship, or research fellowship. The Ph.D. Program Committee, comprised of members selected from the graduate faculty, is responsible for advising students.

All Ph.D. IT students must teach at least one course during their Ph.D. program, unless given a waiver for prior relevant experience.

Optional Concentrations

- Cybersecurity Concentration
- Artificial Intelligence and Machine Learning Concentration

Students may graduate without a concentration, in which case their course of study is considered traditional information systems. Students who wish to focus the Ph.D. in IT on **Cybersecurity** or **Artificial Intelligence and Machine Learning** should elect a concentration.

Degree Requirements for Students who have Obtained a Bachelor's Degree

The degree requires a minimum of 75 semester credit hours beyond the bachelor's degree.

No course for which a grade of less than "C" was earned can be applied to the doctoral degree program, and no more than two courses with a grade of "C" may be applied to the program.

Program of Study

Code	Title	Credit Hours
A. Discipline Background Courses		**9**
Students are required to complete at least 9 semester credit hours of 5000-level courses or higher in the major field or in a field directly related or relevant to the major field in consultation with their Graduate Advisor of Record to fulfill the Discipline Background Courses requirement. *		
B. Required Course		**3**
GBA 7103	Doctoral Teaching Seminar	
C. Statistics and Research Methodology		**12**
12 semester credit hours of 6000- or 7000-level courses in Statistics, Analytics/AI, Research Methods, Management Science, or related courses as approved by the Ph.D. Program Committee.		
D. Major Area Coursework		**27**
1. Ph.D. Level Courses: A total of 12 credit hours of Ph.D. level courses on different topics, as required and approved by the Ph.D. Program Committee, but not limited to the following:		
Cybersecurity concentration and non-concentration students are required to take IS 7013 and IS 7023. IS 7013 should be taken in the first semester.		
IS 7013	Foundations of Information Systems Research	
IS 7023	Behavioral and Organizational Information Systems and Cyber Security Research	
IS 7033	Topics in Information Systems and Information Technology Research	
IS 7053	Topics in AI/ML Research	
IS 7063	Topics in Cybersecurity Research	
Artificial Intelligence and Machine Learning concentration students must take either IS 7013 or IS 7023. Students should take this course in their second year.		
IS 7013	Foundations of Information Systems Research	
or IS 7023	Behavioral and Organizational Information Systems and Cyber Security Research	
IS 7033	Topics in Information Systems and Information Technology Research	
IS 7053	Topics in AI/ML Research	
IS 7063	Topics in Cybersecurity Research	
2. Directed Electives (15 semester credit hours).		
Prior to completion, directed electives must be approved in the student's Program of Study.		
E. Free elective		**3**
One course to be approved by the Ph.D. Program Committee. The course may be from within or outside the college and must be at the graduate level.		
F. Doctoral Research (9 semester credit hours)		**9**
This requirement is met by doctoral research coursework.		
G. Doctoral Dissertation (minimum of 12 semester credit hours)		**12**

Programs of study must be approved annually by the ACOB Ph.D. coordinator or delegate, Information Systems & Cybersecurity Ph.D. program coordinator, and the student's subject matter advisor (concentration coordinator if the student has not identified a dissertation chair; else, the dissertation chair).	
Total Credit Hours	**75**

* This requirement may be met by prior completion of a master's degree in business or business-related discipline, or at least 9 credit hours of other prior relevant graduate coursework. If a student does not have the appropriate graduate degree or prior relevant graduate coursework, a minimum of 9 semester credit hours are required. The Graduate Advisor of Record, in consultation with the Ph.D. Program Committee will select these courses based on the student's prior academic and professional experience, strengths, and research interests to best prepare the student for Ph.D.-level coursework and research. The Graduate Advisor of Record, in consultation with the Ph.D. Program Committee may require additional courses to meet this requirement if they deem it necessary.

Degree Requirements for Students who have Obtained a Master's Degree

The degree requires a minimum of 57 semester credit hours beyond the master's degree.

No course for which a grade of less than "C" was earned can be applied to the doctoral degree program, and no more than two courses with a grade of "C" may be applied to the program.

Program of Study

Code	Title	Credit Hours
A. Required Course		**3**
GBA 7103	Doctoral Teaching Seminar	
B. Statistics and Research Methodology		**12**
12 semester credit hours of 6000- or 7000-level courses in Statistics, Analytics/AI, Research Methods, Management Science, or related courses as approved by the Ph.D. Program Committee.		
C. Major Area Coursework		**18**
1. Ph.D. Level Courses: A total of 12 credit hours of Ph.D. level courses on different topics, as required and approved by the Ph.D. Program Committee, but not limited to the following:		
Cybersecurity concentration and non-concentration students are required to take IS 7013 and IS 7023. IS 7013 should be taken in the first semester.		
IS 7013	Foundations of Information Systems Research	
IS 7023	Behavioral and Organizational Information Systems and Cyber Security Research	
IS 7033	Topics in Information Systems and Information Technology Research (e.g. Blockchain in Cyber Security)	
IS 7033	Topics in Information Systems and Information Technology Research (Machine Learning)	
IS 7053	Topics in AI/ML Research	
IS 7063	Topics in Cybersecurity Research	
Artificial Intelligence and Machine Learning concentration students must take either IS 7013 or IS 7023. Students should take this course in their second year.		
IS 7013	Foundations of Information Systems Research	
or IS 7023	Behavioral and Organizational Information Systems and Cyber Security Research	
IS 7033	Topics in Information Systems and Information Technology Research	
IS 7053	Topics in AI/ML Research	
IS 7063	Topics in Cybersecurity Research	
2. Directed Electives (6 semester credit hours).		
Prior to completion, directed electives must be approved in the student's Program of Study.		
D. Free elective		**3**
One course to be approved by the Ph.D. Program Committee. The course may be from within or outside the college and must be at the graduate level.		
E. Doctoral Research (9 semester credit hours)		**9**
This requirement is met by doctoral research coursework.		
F. Doctoral Dissertation (minimum of 12 semester credit hours)		**12**
Programs of study must be approved annually by the ACOB Ph.D. coordinator or delegate, Information Systems & Cybersecurity Ph.D. program coordinator, and the student's subject matter advisor (concentration coordinator if the student has not identified a dissertation chair; else, the dissertation chair).		
Total Credit Hours		**57**

Advancement to Candidacy

Advancement to candidacy requires a student to complete University and program requirements and to pass a written qualifying examination following completion of course requirements in the candidate's major field of study. The examination is administered by the Ph.D. Program Committee. No more than two attempts to pass qualifying examinations are allowed. Results of the written examinations must be reported to the Ph.D. Program Committee, the Dean of the College, and the Dean of the Graduate School. Admission into the doctoral program does not guarantee advancement to candidacy.

Dissertation

Candidates must demonstrate the ability to conduct independent research by completing and defending an original dissertation. The research topic is determined by the student in consultation with his or her supervising professor. A Dissertation Committee, selected by the student and supervising professor, guides and critiques the candidate's research. The completed dissertation must be formally presented to and approved by the Dissertation Committee.

Following an open presentation of the dissertation findings, the Dissertation Committee conducts a closed meeting to determine the adequacy of the research and any further requirements for completion of the dissertation. Results of the meeting must be reported to the Dean of the College and to the Dean of the Graduate School.

Awarding of the degree is based on the approval of the Dissertation Committee, approved by the Dean. The UT San Antonio Dean of the Graduate School certifies the completion of all University-wide requirements.

- Graduate Certificate in Cloud Computing (p. 6)
- Graduate Certificate in Cybersecurity (p. 6)
- Graduate Certificate in Intelligence Studies (p. 6)

Graduate Certificate in Cloud Computing

The Graduate Certificate in Cloud Computing is a 12-semester-credit-hour program designed to equip technical professionals with the knowledge and technical skills necessary for a career in an organization that leverages cloud computing. The wide range of use of cloud computing in today's business, government, and academic environments requires a broad range of competencies and understanding of how cloud computing influences a particular area. This certificate is designed to give a common framework of understanding cloud computing, as well as allow for specialization in specific areas, such as cyber-security, cloud-infrastructure, and applications in cloud. Students may take elective courses not listed with program approval.

The certificate is administered by the Klesse College of Engineering and Integrated Design in conjunction with the College of AI, Cyber and Computing. The course requirements for each program focus may be found under the Department of Electrical Engineering (https://catalog.utsa.edu/graduate/engineeringintegrateddesign/electricalengineering/), the Department of Computer Science, (https://catalog.utsa.edu/graduate/aicybercomputing/computerscience/) and the Department of Information Systems and Cybersecurity (p. 1).

Certificate Program Requirements

To satisfy the requirements for the Graduate Certificate in Cloud Computing, students must complete 12 semester credit hours as follows:

Code	Title	Credit Hours
A. Required Course		**3**
Select one entry course:		
IS 6973	Special Problems (Topic: Cloud Computing for Business)	
Or a cross-listed course in CS and EE. The entry course is taught through team teaching in which an instructor from each college contributes to the subjects outlined in the course syllabus.		
B. Track Electives		**6**
Select two courses from one of the following tracks: [1]		
Applications Track		
CS 5233	Artificial Intelligence	
CS 5493	Large-Scale Data Management	
CS 5573	Cloud Computing	
CS 6243	Machine Learning	
EE 5243	Special Topics in Control (Topic: Data Analytics with Cloud Computing)	
EE 5243	Special Topics in Control (Topic: Programming Techniques for the Cloud)	
IS 6703	Introduction to Data Mining	
Security Track		
IS 5513	Fundamentals of Information Assurance	
IS 6363	Digital Forensics	
Infrastructure Track		
CS 5103	Software Engineering	
CS 5123	Software Testing and Quality Assurance	
CS 6543	Networks	
CS 6553	Performance Evaluation	
C. Capstone Project		**3**
IS 6953	Independent Study (topic should be in the field of Cloud Computing)	
IS 6983	Master's Thesis	
IS 7313	Doctoral Dissertation	
Total Credit Hours		**12**

[1] Students may take elective courses not listed with program approval

Graduate Certificate in Cybersecurity

The graduate certificate in Cybersecurity is a 12-semester-credit-hour program designed for students *not* studying cybersecurity as their major field of study. It is designed to give non-cyber professionals the knowledge and technical skills needed to deal with cybersecurity issues that impact a wide variety of fields. This certificate is designed to give a common framework of understanding cybersecurity, as well as allow for specialization in specific areas, such as law, policy, analysis, response, etc.

The certificate is administered by the College of AI, Cyber and Computing. The courses are offered by the Department of Information Systems and Cybersecurity. The certificate program is open to students in any major field of study except the UT San Antonio M.S.I.T. in Cybersecurity and UT San Antonio B.B.A. in Cybersecurity graduates. The certificate program is also open to non-degree seeking students. The certificate is valuable to current UT San Antonio students, alumni, and business professionals.

Certificate Program Requirements

To satisfy the requirements for the Graduate Certificate in Cybersecurity, students must complete 12 semester credit hours as follows:

Code	Title	Credit Hours
A. Required Course		3
IS 6113	Telecommunications Essentials	
B. Electives		9
Select three courses from the following list:		
IS 6213	Information Assurance and Security Essentials	
IS 6223	Intrusion Detection and Incident Response Essentials	
IS 6463	Web Application Security Essentials	
IS 6473	Information Assurance Policy Essentials	
IS 6483	Digital Forensic Analysis Essentials	
IS 6513	Industrial Control System Security Essentials	
IS 6763	Cyber Law Essentials	
Total Credit Hours		**12**

Graduate Certificate in Intelligence Studies

The Graduate Certificate in Intelligence Studies is a 12-semester-credit-hour program designed to prepare individuals from a broad range of academic disciplines for a career in the Intelligence Community (https://

www.intelligence.gov/). Individuals with business, foreign language, social science, computer science, criminal science, engineering, or statistics backgrounds will benefit from this professional certificate. Individuals completing this certificate will gain a practical and hands-on knowledge of methods in intelligence collection, intelligence analysis, and reporting and briefing for the intelligence community. See the College of Business Critical Technology Studies Program (http://www.business.utsa.edu/ctsp/) website for more information.

Admission Requirements

The certificate is open to all UT San Antonio graduate students, including non-degree seeking students, regardless of their college or major. Applicants who are currently enrolled in a graduate degree program at UT San Antonio have already met University requirements for admission. Current students should contact the Critical Technology Studies Program (http://www.business.utsa.edu/ctsp/) and complete a form requesting permission to pursue the Intelligence Studies certificate via email at ctsp@utsa.edu or by telephone at (210) 458-7328.

Applicants who are not currently enrolled in a graduate degree program at UT San Antonio will be required to apply for admission to UT San Antonio as a special (non-degree-seeking) graduate student and to indicate their intent to seek admission into a certificate program. Students who meet general UT San Antonio admission requirements are eligible for admission to this certificate program.

Certificate Program Requirements

To earn the Graduate Certificate in Intelligence Studies, students must complete 12 semester credit hours as follows:

Code	Title	Credit Hours
Required Courses (9 semester credit hours):		9
NS 6003	The Role of U.S. Intelligence in National Security	
NS 6223	Analytical Writing, Reporting and Briefing for the Intelligence Community	
NS 6503	Intelligence Reasoning Analysis	
Select one course from the following (3 semester credit hours):		3
GLA 5783	Global Security	
IS 6603	Cyber Threat Hunting	
NS 6523	Methods in Intelligence Collection	
POL 5093	Politics of U.S. National Security Policy Making	
Total Credit Hours		**12**

Information Systems (IS) Courses

IS 5143. Information Technology. (3-0) 3 Credit Hours.
Prerequisite: Undergraduate degree in information systems or computer science, or consent of instructor. This course includes a broad coverage of technology concepts underlying modern computing and information management. Topics include computer architecture and operating systems, information retrieval techniques, networks, cloud computing, and software development. Hands-on exposure to web site development, contemporary data search techniques, and software development tools. This course has Differential Tuition. Course Fee: ISCS $75.

IS 5203. Networking and Telecommunication Systems. (3-0) 3 Credit Hours.
Prerequisite: Undergraduate degree in information systems or computer science, or consent of instructor. This course examines current, future, and basic technical concepts and related telecommunications operations. Explores critical issues of communications and connectivity among information systems from strategic, organizational, and technical perspectives. An in-depth examination of basic telecommunication terminology and concepts. Topics include OSI models, signaling, modulation, multiplexing, software defined networking, network addressing, routing, reliable data transfer, digital coding, switching systems, and traffic analysis. This course has Differential Tuition. Course Fee: ISCS $75.

IS 5513. Fundamentals of Information Assurance. (3-0) 3 Credit Hours.
Prerequisite: Graduate standing. This course examines the principle areas of information assurance. Topics will include protecting networks, intrusion detection, digital forensics, and supervisory control and data acquisition. Application to business environments will be emphasized. Credit for this course cannot be counted toward the Master of Science degree in Information Technology. (Same as ACC 5513. Credit can only be earned for one of the following: IS 5513, ACC 5513, or IS 3053). This course has Differential Tuition.

IS 6083. Agile Project Management. (3-0) 3 Credit Hours.
This introductory course presents concepts and techniques for leading agile teams in many types of projects including software development, engineering, construction, product development, as well as science and technology focused efforts. The course will give students the opportunity to develop an agile mindset and a range of adaptive skills including agile methods, practices, and values that are associated with achieving higher levels of performance and customer satisfaction. Students who complete the course will be prepared for the MOT 5263 Project Management certification course. (Same as IS 4083. Credit cannot be earned for both IS 4083 and IS 6083.) This course has Differential Tuition.

IS 6113. Telecommunications Essentials. (3-0) 3 Credit Hours.
Includes an in-depth look at basic telecommunications terminology and concepts. Introduction to voice and data networks, signaling and multiplexing. Network topologies and protocol fundamentals and architectures are presented and compared. Ethernet, IEEE 802.11x, TCP/IP, dedicated circuit, and VPN technologies are introduced. Network security fundamentals are explored. Credit for this course cannot be counted toward the Master of Science degree in Information Technology with Cyber Security Concentration. (Same as IS 3413. Credit for this course cannot be counted if the student took IS 3413 in the UTSA BBA Cyber Security program.) This course has Differential Tuition.

IS 6213. Information Assurance and Security Essentials. (3-0) 3 Credit Hours.
Prerequisite: IS 6113. This course will provide the student the opportunity to learn about the basic elements that comprise Information Assurance Security. An in-depth presentation of information assurance topics such as fraud, eavesdropping, traffic analysis, intrusion detection and prevention, hacking, viruses, cryptography, risk management, and secure architectures will be discussed. (Same as IS 3513. Credit for this course cannot be counted if the student took IS 3513 in the UTSA BBA Cyber Security program.) This course has Differential Tuition.

IS 6223. Intrusion Detection and Incident Response Essentials. (3-0) 3 Credit Hours.
Prerequisite: IS 6213. This course will provide the student with the opportunity to learn about the elements that comprise intrusion detection and incident response. It provides an in-depth look at intrusion detection methodologies, tools, and approaches to handling intrusions when they occur. It examines the laws that address cyber crime and intellectual property issues and includes a study of proper computer and network forensics procedures to aid in the identification and tracking of intruders and in the potential prosecution of criminal activity. (Same as IS 3523. Credit for this course cannot be counted if the student took IS 3523 in the UTSA BBA Cyber Security program.) This course has Differential Tuition.

IS 6303. Introduction to Voice and Data Security. (3-0) 3 Credit Hours.
Prerequisite: Completion of or concurrent enrollment in IS 5203. A study of security in both the voice and data networks and an examination of the security issues associated with the movement toward a convergence of the two infrastructures. Topics to be covered include voice and data network connectivity, modem security, VOIP security, wireless security, cryptography, intrusion detection systems, voice and data firewalls, malicious software, information operations and warfare, and denial of service attacks. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6323. Security Risk Analysis. (3-0) 3 Credit Hours.
Prerequisite: IS 5203 and IS 6303, or consent of instructor. Addresses the tools, techniques, and methodologies in performing computer system and network security risk analyses. Computer system and network vulnerabilities will be examined as well as tools designed to discover or exploit them. Security Best Practices and audit requirements for specific environments will be studied. Topics to be covered include internal and external penetration tests, wardialing, wireless security technology, risk analysis methodology, and security audits. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6343. Secure Network Designs. (3-0) 3 Credit Hours.
Prerequisite: IS 5203 and IS 6303, or consent of instructor. The course is intended to provide the background on issues related to secure network design and management. Subjects included in the class are network design, firewalls, security, fault management, and performance management. Current network management software, network security evaluation, and the role of the network architecture and protocols will also be discussed. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6353. Security Incident Response. (3-0) 3 Credit Hours.
Prerequisite: IS 6303. Addresses the detection and response portion of the security operational model. Takes an in-depth look at intrusion detection methodologies and tools and the approaches to handling intrusions when they occur. Examines the laws that address cybercrime and intellectual property issues. Includes a study of proper computer and network forensics procedures to aid in the identification and tracking of intruders and in the potential prosecution of criminal activity. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6363. Digital Forensics. (3-0) 3 Credit Hours.
Prerequisite: IS 6303 or consent of instructor. This class will examine the role of computer forensics in the security process. Technical issues concerning how to conduct a forensic examination as well as the legal issues associated with the process will be studied. Current forensics software will be used to illustrate the process. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6373. Cyber Law. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. Legal issues associated with cybercrimes will be studied. Laws associated with cybercrime, and rules of evidence will be the main issues discussed in this class. Intellectual property and privacy will also be included. This course has Differential Tuition.

IS 6383. Policy Assurance for Infrastructure Assurance. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. This course will examine the policies associated with infrastructure assurance. This will include the laws and regulations from a governmental body as well as policies generated by a business organization. The emphasis will be to examine the effect that policies and policy decisions have on the security function. Current case studies will be included. This course has Differential Tuition.

IS 6423. Secure Software Design. (3-0) 3 Credit Hours.
Prerequisite: IS 5143 and IS 6303, or consent of instructor. This class will present ways of designing and implementing secure software. Techniques for developing interconnected software that is secure from outside attack will be explored. Modifying legacy code will also be discussed. Case studies and class projects will be used to illustrate the design principles discussed in class. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6433. Supervisory Control and Data Acquisition. (3-0) 3 Credit Hours.
Prerequisite: IS 6303 or consent of instructor. Supervisory control and data acquisition systems are used to control many utility networks, chemical plants, pipelines and many other types of industries. This course will examine the vulnerabilities associated with these systems and discuss how they can be made secure from outside attack. Fundamentals of software-controlled processes will also be discussed. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6463. Web Application Security Essentials. (3-0) 3 Credit Hours.
Prerequisite: IS 6213. The security issues related to web applications will be discussed in this course. Topics include web application authentication, authorization, as well as browser and web database security principles. Various web application security attack types such as code injection, cross- site scripting, and cross-site request forgery will be studied. The course will also include discussions about business aspects that contribute to a secure web-based transaction environment. Research into appropriate topics will be incorporated into the course. (Same as IS 4463. Credit for this course cannot be counted if the student took IS 4463 in the UTSA BBA Cyber Security program.) This course has Differential Tuition. Course Fee: ISCS $75.

IS 6473. Information Assurance Policy Essentials. (3-0) 3 Credit Hours.
Prerequisite: IS 6113. There are many policy issues within the firm and at various levels of government that affect information assurance. This course will examine how these policies affect electronic security. Subjects will include privacy of information, intellectual property protection, globalization of information systems, and other policy matters. The protection and control of secured information will also be discussed. Research into appropriate topics will be incorporated into the course. (Same as IS 4473. Credit for this course cannot be counted if the student took IS 4473 in the UTSA BBA Cyber Security program.) This course has Differential Tuition.

IS 6483. Digital Forensic Analysis Essentials. (3-0) 3 Credit Hours.
Prerequisite: IS 6213. This is an introductory course in collecting, examining, and preserving evidence of computer crimes. This course examines the issues, tools, and control techniques needed to successfully investigate illegal activities facilitated through the use of information technology. The tools of collecting, examining, and evaluating data in an effort to establish intent, culpability, motive, means, methods, and loss resulting from e-crimes will be examined. Research into appropriate topics will be incorporated into the course. (Same as IS 4483. Credit for this course cannot be counted if the student took IS 4483 in the UTSA BBA Cyber Security program.) This course has Differential Tuition. Course Fee: ISCS $75.

IS 6503. Principles of Database Management. (3-0) 3 Credit Hours.
Prerequisite: IS 3063 or consent of instructor. Discussion and in-depth analysis of topics associated with the definition, creation, and management of databases for business-oriented applications. Topics include current developments in the field of database management systems. Design and implementation of a database system will be done as a major project in the course. This course has Differential Tuition.

IS 6513. Industrial Control System Security Essentials. (3-0) 3 Credit Hours.
Prerequisite: IS 6213. Many of the critical infrastructure systems contain a system control and data acquisition (SCADA) component. Frequently, the control systems are remotely accessed and therefore becomes the focal point for attack. This course examines the control system components from the standpoint of vulnerability and protection. Research into appropriate topics will be incorporated into the course. (Same as IS 4513. Credit for this course cannot be counted if the student took IS 4513 in the UTSA BBA Cyber Security program.) This course has Differential Tuition. Course Fee: ISCS $75.

IS 6533. Federal Research Projects. (3-0) 3 Credit Hours.
Prerequisite: Consent of the Instructor. This course is a research based course that makes real-world research problems that exist in the government domain available for students to work on. The research problems cover a wide variety of issues. The solutions may be a literature review, developing code, proposing an answer, or testing a solution. Weekly coordination with a Technical Director from a Federal Lab is part of the process. This course has Differential Tuition.

IS 6603. Cyber Threat Hunting. (3-0) 3 Credit Hours.
This course will provide the opportunity to learn how to proactively and iteratively search through networks and computer systems to detect and isolate latent intrusions. Students will also learn how to identify and anticipate cyber-related incidents using data analysis techniques on large data sets of structured and unstructured data from a variety of sources. The course will emphasize analytical methodologies needed to address Advanced Persistent Threat (APT) attacks as well as other known and unknown strategies for compromising a computer system. This course has Differential Tuition. Course fee: DL01 $75.

IS 6703. Introduction to Data Mining. (3-0) 3 Credit Hours.
This course introduces the fundamental data mining concepts and techniques that are applicable to business research. The course covers basic skills required to assemble analyses for both pattern discovery and predictive modeling. It provides extensive hands-on instruction using data mining software. This course is open to all graduate students. (Same as ACC 6703. Credit cannot be earned for both IS 6703 and ACC 6703.) (Formerly titled "Advanced Business Information Systems.") This course has Differential Tuition.

IS 6713. Data Foundations. (3-0) 3 Credit Hours.
The ability to understand, store, process, transform, cleanse, fuse, and share data is critical to data analytics; and it can often be the most challenging and/or most time consuming part of the data analytics process due to the vast variety of data sources, types, and formats. This course equips students to collect/process common types of data used in data analytics, and provides them a solid understanding of various data sources, types, and formats, and how to handle and process each. Students will learn how to wrangle and preprocess structured and unstructured data, to include multidimensional data, textual data that requires natural language processing (NLP) and web-based data. Students will also learn web scraping, web crawling, and how to collect data via web-based application programming interfaces (APis). Students will learn all of these topics using common Python data analytics and data science packages. Students will have the opportunity to learn how to store, process, transform, cleanse, fuse, and share data. Exemplar data will be used extensively in the course so that students see and experience a wide variety of data and understand how to process and handle it. Data handling exercises will be provided in the context of scenario based problems to further improve their educational knowledge, practical skill set, and contextual understanding. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6733. Deep Learning on Cloud Platforms. (3-0) 3 Credit Hours.
This course presents students with basic understanding of modern neural networks and their applications in computer vision and natural language processing (NLP). The course starts with a recap of linear models and discussion of stochastic optimization methods that are crucial for training deep neural networks. students will examine all of the popular neural network building blocks including fully connected layers, convolution, and recurrent layers. In this course, students will gain a thorough introduction to cutting-edge topics such as attention and transformer in Deep Learning for NLP using public cloud platforms. Students will also gain practical hands-on experience in the optimization, deployment, and scaling ML models of various types. The prerequisites for this course are: 1) Basic knowledge of Python. 2) Basic linear algebra and probability. This course has Differential Tuition. Course Fee: ISCS $75.

IS 6763. Cyber Law Essentials. (3-0) 3 Credit Hours.
Legal issues associated with cybercrimes will be studied. Laws associated with cybercrime, and rules of evidence will be the main issues discussed in this class. Intellectual property and privacy will also be included. (Same as IS 3533. Credit for this course cannot be counted if the student took IS 3533 in the UTSA BBA Cyber Security program.) This course has Differential Tuition.

IS 6813. Strategic Management of Information Technology. (3-0) 3 Credit Hours.
Prerequisite: Semester of graduation or consent of Graduate Advisor of Record. This course develops a conceptual framework for strategy, its definition, elements, and relationships to the basic business functions of the management of technology. Considers the impact of political, economic, social and technological forces on the strategic management of organizations. Examines the role of technology and cyber security in business process re-engineering, product life cycles, and new business models. (Same as MOT 5203 and MOT 6203. Credit can be earned for only one of the following: IS 6813, MOT 5203, or MOT 6203.) This course has Differential Tuition.

IS 6933. Internship in Information Technology. (0-0) 3 Credit Hours.
Prerequisite: Graduate standing, 15 semester credit hours of graduate work (including IS 5143), and consent of instructor. Supervised full- or part-time off-campus work experience and training in the areas of information technology. May not be done at student's current or past employer unless in a new role/function. May not be repeated for credit. (Credit cannot be earned for both IS 6933 and IS 6943.) This course has Differential Tuition.

IS 6943. Internship in Cyber Security. (0-0) 3 Credit Hours.
Prerequisite: Graduate standing, 15 semester credit hours of graduate work (including IS 6303), and consent of instructor. Supervised full- or part-time off-campus work experience and training in the areas of cyber security. May not be done at student's current or past employer unless in a new role/function. May not be repeated for credit. (Credit cannot be earned for both IS 6943 and IS 6933.) This course has Differential Tuition.

IS 6953. Independent Study. (0-0) 3 Credit Hours.
Prerequisite: Graduate standing and permission in writing (form available) from the instructor and the student's Graduate Advisor of Record. Independent reading, research, discussion, and/or writing under the direction of a faculty member. For students needing specialized work not normally or not often available as part of the regular course offerings. May be repeated for credit, but not more than 6 hours, regardless of discipline, will apply to the degree. This course has Differential Tuition.

IS 6961. Comprehensive Examination. (0-0) 1 Credit Hour.
Prerequisite: Approval of the appropriate committee on graduate studies to take the Comprehensive Examination. Independent study course for the purpose of taking the Comprehensive Examination. May be repeated as many times as approved by the Committee on Graduate Studies. Enrollment is required each term in which the Comprehensive Examination is taken if no other courses are being taken that term. The grade report for the course is either "CR" (satisfactory performance on the Comprehensive Examination) or "NC" (unsatisfactory performance on the Comprehensive Examination). This course has Differential Tuition.

IS 6973. Special Problems. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. An organized course offering the opportunity for specialized study not normally or not often available as part of the regular course offerings. Special Problems courses may be repeated for credit when topics vary, but not more than 6 hours, regardless of discipline, will apply to the degree. This course has Differential Tuition.

IS 6983. Master's Thesis. (0-0) 3 Credit Hours.
Prerequisite: Permission from the Graduate Advisor of Record and thesis director (form available). Thesis research and preparation. May be repeated for credit, but not more than 6 hours will apply to the Master's degree. Credit will be awarded upon completion of the thesis. Enrollment is required each term in which the thesis is in progress. This course has Differential Tuition.

IS 7013. Foundations of Information Systems Research. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. A survey of the foundations of information systems (IS) research. Students gain an understanding of both the foundations and the current research directions in a variety of IS topic areas. The course addresses frameworks, research concepts, and exemplary Management Information Systems (MIS) research. Students develop the ability to critically evaluate MIS journal articles and are exposed to diverse topics, research methodologies, and journals. This course has Differential Tuition.

IS 7023. Behavioral and Organizational Information Systems and Cyber Security Research. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. This course focuses on one or more areas of emerging IS behavioral research. Topics may include individual, group, or organizational decision making, issues for e-commerce, knowledge management, management of information, and human factors. May be repeated for credit when topics vary. This course has Differential Tuition.

IS 7033. Topics in Information Systems and Information Technology Research. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. This research seminar focuses on issues and methods in one or more areas having to do with the technology of information systems. Topics may include information communication technology systems, management of information systems, systems analysis and design, and data management. May be repeated for credit when topics vary. This course has Differential Tuition.

IS 7053. Topics in AI/ML Research. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. This research seminar focuses on the challenges in the design of safe and robust AI-based systems. It explores some of the major problems in this area from the viewpoint of industry and academia, as well as issues such as safety, fairness, robustness, adversarial examples, explainable AI, and real-world implications of AI. May be repeated for credit when topics vary. This course has Differential Tuition.

IS 7063. Topics in Cybersecurity Research. (3-0) 3 Credit Hours.
Prerequisite: Consent of instructor. This research seminar focuses on cybersecurity, as well as infrastructure assurance / critical technology from a security perspective. Topics may include blockchain, economics of security, cloud and big data security, threat hunting and detection, and cybersecurity metrics and analytics. May be repeated for credit when topics vary. This course has Differential Tuition.

IS 7211. Doctoral Research. (0-0) 1 Credit Hour.
May be repeated for credit, but not more than 24 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7212. Doctoral Research. (0-0) 2 Credit Hours.
May be repeated for credit, but not more than 24 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7213. Doctoral Research. (0-0) 3 Credit Hours.
May be repeated for credit, but not more than 24 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7214. Doctoral Research. (0-0) 4 Credit Hours.
May be repeated for credit, but not more than 24 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7215. Doctoral Research. (0-0) 5 Credit Hours.
May be repeated for credit, but not more than 24 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7216. Doctoral Research. (0-0) 6 Credit Hours.
May be repeated for credit, but not more than 24 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7311. Doctoral Dissertation. (0-0) 1 Credit Hour.
Prerequisite: Admission to candidacy for the Doctoral degree in Business Administration. May be repeated for credit, but not more than 12 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7312. Doctoral Dissertation. (0-0) 2 Credit Hours.
Prerequisite: Admission to candidacy for the Doctoral degree in Business Administration. May be repeated for credit, but not more than 12 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7313. Doctoral Dissertation. (0-0) 3 Credit Hours.
Prerequisite: Admission to candidacy for the Doctoral degree in Business Administration. May be repeated for credit, but not more than 12 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7314. Doctoral Dissertation. (0-0) 4 Credit Hours.
Prerequisite: Admission to candidacy for the Doctoral degree in Business Administration. May be repeated for credit, but not more than 12 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7315. Doctoral Dissertation. (0-0) 5 Credit Hours.
Prerequisite: Admission to candidacy for the Doctoral degree in Business Administration. May be repeated for credit, but not more than 12 hours may be applied to the Doctoral degree. This course has Differential Tuition.

IS 7316. Doctoral Dissertation. (0-0) 6 Credit Hours.
Prerequisite: Admission to candidacy for the Doctoral degree in Business Administration. May be repeated for credit, but not more than 12 hours may be applied to the Doctoral degree. This course has Differential Tuition.

National Security (NS) Courses

NS 6003. The Role of U.S. Intelligence in National Security. (3-0) 3 Credit Hours.
This course provides a broad overview of the role of intelligence work - and in particular U.S. intelligence efforts - in maintaining and enhancing the country's national security posture. The history of the intelligence community from the Second World War onward is examined in terms of how that community has evolved over the years. Emphasis is placed upon the interplay and challenges that the intelligence community face with policy makers. Included is an examination of case studies that illustrate intelligence successes and failures that have had a significant impact on national security. Also covered is the evolving unique nature that the cyber domain plays in cyber/national security issues. This course has Differential Tuition.

NS 6223. Analytical Writing, Reporting and Briefing for the Intelligence Community. (3-0) 3 Credit Hours.
Prerequisite: NS 6003. Fundamentals of writing and reporting for intelligence community audiences. Illustrated concepts and principles include bottom line up front, topic sentences, presentation of key judgments, the descriptive use of confidence intervals, estimative language, presentation of alternative outcomes, scenario description, appropriate reading level for reports, key challenges in one time briefings, speaking truth to power, the benefits of brevity and clarity, the issue of source disclosure, the value of context, characteristics of assessments, and avoiding policy statements. This course has Differential Tuition.

NS 6503. Intelligence Reasoning Analysis. (3-0) 3 Credit Hours.
Prerequisite: NS 6003. Analysis and analytical reasoning for intelligence analyst professionals requires adherence to analytical standards and principles that promote integrity as well as logic. The course includes, but is not limited to, topics such as transforming data to intelligence, the intelligence process, critical thinking, selected structured analytical techniques, recognizing and overcoming perceptual, cognitive and cultural biases, methods for describing the assessed validity of information or conclusions, and other components of the process, and psychology of intelligence analysis. This course provides students opportunities to apply critical thinking and analytic skills learned in class through exercises, case studies, and a capstone paper. This course has Differential Tuition.

NS 6523. Methods in Intelligence Collection. (3-0) 3 Credit Hours.
Prerequisite: NS 6003. This course covers the fundamentals of the primary methods for intelligence collection: human intelligence (HUMINT), geospatial intelligence (GEOINT), open source intelligence (OSINT), signals intelligence (SIGINT), and measurement and signal intelligence (MASINT). Topics explored include methods used, nature of the data collected, sources of error within the data collected for each method, limitations of the data, and challenges encountered when integrating and fusing data from multiple sources and methods. Use of unclassified case studies will provide additional examples of some of the concepts and principles covered. This course has Differential Tuition.

NS 6723. National Security and Human-Digital Technology Relationships. (3-0) 3 Credit Hours.
One of the recent key emerging areas of research is the role of psychological, social, and cultural processes in cyber conflict. Following the kill chain upstream you will find at the end a human with motivations and objectives, This course examines a number of critical elements involved in the relationship between humans and digital technology as it relates to cyber and national security, including the role that motivations for malicious online acts and how social dynamics affect the emergence of relationships between non-nation state actors and nation states, the evolving nature of social movements and communities online and the emergence of cyberterrorism as a new entrant into the cyber threat matrix. This course has Differential Tuition.