Model Curriculum for Security Studies - Certificate Program Proposal

<u>Program Description</u>: Security Studies is a rapidly growing field that demands educated professionals schooled in a number of disciplines as it evolves into a multi-dimensioned business preservation model. The Security Studies Certificate Program provides students with courses which lead to a Certificate in Security Studies and provides a foundation for students who wish to pursue further studies in Security Studies. This will also give students the basic knowledge and skills to begin careers in the security profession.

<u>Program Courses:</u> The Certificate in Security Studies is an Interdisciplinary Program consisting of courses in Security, Criminal Justice, Business, and Computer Science. The Program consists of six required courses and one elective course chosen from a list provided.

<u>Required Courses</u>

SSxxx	Introduction to Security Studies
CSxxx	Introduction to Computer and Information Security
SSxxx	Organizational Safety & Risk Management
SS/CJxxx	Investigations
COMxxx	Interpersonal Communications
SS/CJxxx	Emergency/Crisis Management

Electives – Choose one (1)

See listing

Model Curriculum for Security Studies - Two Year Program Proposal

Program Description: Security Studies is a rapidly growing field that demands educated professionals schooled in a number of disciplines as it evolves into a multi-dimensioned business preservation model. The Security Studies major provides students with courses which lead to an Associates of Science Degree and provides a foundation for the Bachelor's in Science Degree in Security Studies as well as employment in the security profession.

This Program will emphasize both the academic and the practical as it prepares students for the challenges in protecting people and the assets of organizations from the threats, both inside and outside of the organization. Students will develop the academic skills necessary to think critically about all aspects of Security Studies as well as the practical skills required to function in the global security environment.

Program Courses:

The Associate's in Security Studies is an Interdisciplinary Program consisting of courses in Security Studies, Criminal Justice, Business, and Computer Science.

This is based on a standard two year 60 credit curriculum. Note that different institutions will have different models and required credit hours for their General Education/Liberal Arts requirements. All classes are assumed to be three credit courses.

This model assumes a 30 Credit Program with 21 required credits (7 classes) and 9 elective credits (3 classes). The remaining 30 credits would be made up of an institution’s General Education and Liberal Arts requirements, other school requirements, and free electives.

Course numbers below are suggestions; schools may use numbers as per their institutional policy. Additionally, an SS prefix may be used and cross listed with the corresponding discipline.

Required Courses – 21 Credits

SSxxx	Introduction to Security Studies
CSxxx	Introduction to Computer and Information Security
SSxxx	Organizational Safety & Risk Management
SS/CJxxx	Investigations
COMxxx	Interpersonal Communications
SS/CJxxx	Emergency/Crisis Management
CJxxx	Introduction to Criminal Justice

Electives – 9 Credits

See listing - here are the ones we have recommended, each school would use from the list or seek their own elective list.

***Ethics = core requirement or elective depending on the institution (either CJ or Business ethics)**

Model Curriculum for Security Studies - Four Year Program Proposal

Program Description: Security Studies is a rapidly growing field that demands educated professionals schooled in a number of disciplines as it evolves into a multi-dimensioned business preservation model. The Security Studies major provides students with courses which lead to a Bachelor of Science Degree and provides a foundation for employment in the security profession.

This Program will emphasize both the academic and the practical as it prepares students for the challenges in protecting people and the assets of organizations from the threats, both inside and outside of the organization. Students will develop the academic skills necessary to think critically about all aspects of Security Studies as well as the practical skills required to function in the global security environment.

Program Courses:

The Bachelor's in Security Studies is an Interdisciplinary Program consisting of courses in Security Studies, Criminal Justice, Business, and Computer Science.

This is based on a standard four year 120 credit curriculum. Note that different institutions will have different models and required credit hours for their General Education/Liberal Arts requirements. All classes are assumed to be three credit courses.

This model assumes a 54 Credit Program with 39 required credits (13 classes) and 15 elective credits (5 classes). The remaining 66 credits would be made up of an institution's General Education and Liberal Arts requirements, other school requirements, and free electives.

Course numbers below are suggestions; schools may use numbers as per their institutional policy. Additionally, an SS prefix may be used and cross listed with the corresponding discipline. (Note: the required math for the security studies program is the general education program should be the Statistics class).

Required Courses – 39 Credits

Criminal Justice

CJxxx	Introduction to Criminal Justice
CJxxx	Basic Research Methods
COMxxx	Interpersonal Communications

Business

Bus xxx	Business Ethics

Security Studies or Interdisciplinary

SSxxx or SS/CJ	Introduction to Security Studies
SS/CJxxx	Security Intelligence Analysis
SS/CJxxx	Emergency/Crisis Management

CJ/SSxxx	Security Law
CJ/SSxxx	Investigations
SS/Busxxx	Organizational Safety & Risk Management
SS/ Bus/xxx	Security Management/Administration or BUSXXX Business Management
SS/CJ/Busxxx	Capstone

Computer Science

CSxxx	Introduction to Computer and Information Security

Electives – 15 credits

See listing - here are the ones we have recommended, each school would use from the list or seek their own elective list.

END

	Credit hours	Description	Learning Outcomes	ASIS/DOL Competencies
SS /CJxxx - Introduction to Security Studies	3	The student will learn about the industry background and related law to premise, retail, business, employment, and information/computer security as well as investigation, surveillance, and even homeland security. Throughout, the emphasis is on giving students a clear sense of the numerous career opportunities available in this rapidly expanding field - including real-world insight on how to get a job in private security, concrete information on the skills needed, and succinct overviews of day-to-day job responsibilities.	1. Describe the early development of security. 2. Explain the business of security. 3. Describe the role of security within organizations. 4. Identify the theoretical foundations of security. 5. List and explain methodologies of security applied to protect organizations.	Tier 1 (Integrity, Professionalism) Tier 2 (Security Fundamentals, Critical Thinking, Reading and Writing, Communication) Tier 3 (Teamwork, Planning and Organizing, Problem Solving and Decision Making) Tier 4 (all items except Globalization and Cultural) Tier 5 (all items except Engineering and Design)
CSxxx - Introduction to Computer and Information Security	3	This course is designed to give those in the computer and security professions an understanding of the challenges of protecting information assets and the resources available to meet those challenges. An introduction to information/ computer security is followed by an examination of the need for security and the legal, ethical, and professional issues faced by professionals in this field. Students will then examine the methodologies within the five stages (Security Analysis, Logical Design, Physical Design, Implementation, and Maintenance and Change) of the development, implementation, and maintenance of a new	1. Describe the following computer crime categories: computer threats and intrusions; financial crimes and fraud: intellectual property theft; economic espionage; and cyber terrorism. 2. Explain the extent of computer crime in society and Identify traditional problems associated with the recognition and prosecution of computer crime.	Tier 1: Personal effectiveness competencies Tier 2: Academic Competencies Tier 3: Workplace Competencies Tier 4: Industry-wide technical competencies Tier 5: Industry sector technical competencies

		security system within an organization or the improvement of an existing security system.	3. Discuss the historical evolution and emerging trends in computer crime. 4. Identify various types of electronic evidence, the methods used to collect and preserve it for the introduction into a criminal prosecution. 5. Demonstrate understanding of existing technology with respect to the computer-networking environment, including hardware and software, electronic devices and media containing electronic evidence.	
CJ or BUSxxx – Organizational Safety & Risk Management	3	(with sub-sections on Bio-Security, Agricultural Security & Lab design) This course provides students with an overview of safety issues that could be experienced by security personnel as first responders in various work environment emergencies. It includes a review of OSHA, EPA, and National Fire Code safety regulations and provides methods for identifying and correcting environmental risk factors related to hazardous materials, fire, and other potential safety hazards. The course is also intended to provide the student with knowledge that will assist with the initial response to an investigation of work-related accidents.	1. Trace the early development of safety and risk management. 2. Explain the management of safety and risk management in organizations. 3. List and describe methodologies of safety management. 4. Describe how risk management relates to safety. 5. List and describe methodologies of risk management.	Tier 1: Personal effectiveness competencies Tier 2: Academic Competencies Tier 3: Workplace Competencies Tier 4: Industry-wide technical competencies Tier 5: Industry sector technical competencies
SS/CJxxx - Security Intelligence	3	This course provides the student with a	1. Understand and describe	Tier 1-Personal Effectiveness

Analysis		foundation for the study of security and intelligence by identifying security concepts (securing humans, tangible assets, and information), intelligence concepts (the cycle of intelligence: collection, processing, analysis, dissemination, feedback/utilization), and the roles of security and intelligence professionals within corporate contexts. Prerequisites: None	the continuing evolution of intelligence analysis in the corporate security environment. 2. Identify and explain the integration of risk mitigation practices and data analysis. 3. Summarize and illustrate how intelligence-led practices help reduce repeat offending and repeat victimization. 4. Describe several different investigative and preventative strategies facilitated by intelligence-led practices, such as geographic profiling and risk terrain modeling. 5. Develop an understanding of the various issues with using data, including data sharing, ethical and legal issues. 6. Summarize a basic understanding of the various tools intelligence analysts use to create and present risk/security reports and security oriented material.	Tier 2- Academic Competencies Tier 3- Workplace Competencies Tier 4- Industry-Wide Technical Competencies Tier 5- Industry-Sector Technical Competencies
COM/CJxxx – Interpersonal Communications	3	An introduction to the concepts and skills in oral communication; listening, feedback, group	Develop a personal skillset that will enable students to	Tier 1-Personal

		discussions, speeches, self-disclosure and relational communication.	communicate ethically, responsibly, effectively. Discover the effects of group dynamics and learn to effectively communicate with and through that framework. Model professional and appropriate communication standards in both the spoken and written word. Discover or build upon the ability to prepare and deliver a public presentation. Construct effective written messages in various formats for differing audiences.	Effectiveness Tier 2- Academic Competencies Tier 3- Workplace Competencies
BUSxxx – Introduction to Business	3	The role, growth, structure, and functional organization of modern business in the U.S. economy is explored. Comparative economic systems, sole proprietorships, partnerships, corporations, and the management, marketing, and financing of business organizations are covered. Opportunities in the business field are examined throughout the course. Students will be expected to complete outside research as a course requirement.	1. Identify distinguishing characteristics of business formation 2. Examine the key functions of management 3. Describe the role of product, price, place and promotion in marketing 4. Demonstrate business problem-solving skills 5. Use project management techniques to reflect projected tasks, schedules and resources as well as the progress of task completion	Tier 1-Personal Effectiveness Tier 2- Academic Competencies Tier 3- Workplace Competencies Tier 4- Industry-Wide Technical Competencies
SS/BUSxxx – Security Management or Introduction	3	An introductory course covering the general topics of planning, organizing, directing and	1. Explain the variety of management theories and	Tier 1-Personal

to Management		controlling. Included are the historic developments of management as a separate discipline within organizations, the changing scope and styles of management, and the application of management principles in the business environment.	describe how those theories inform management practices. 2. Analyze managerial challenges and justify proper recommendations based on management theories. 3. Critically evaluate key management concepts across a variety of paradigms. 4. Effectively communicate informational and leadership messages via multiple modes of media. 5. Develop an appreciation for the evolution, development and application of management practices in a technological environment.	Effectiveness Tier 2- Academic Competencies Tier 3- Workplace Competencies Tier 4- Industry-Wide Technical Competencies
SS/CJxxx - Emergency Management / Crisis Management	3	All-hazards crisis planning is vital to the security of businesses and communities. Students discuss the essential focus for research and training issues surrounding crisis planning and disaster recovery. An insight into current practices, strategies, and past emergencies will be identified, analyzed, and proactive response lessons will expose the student to a variety of human and natural crises. Students will also examine local, state, federal, and international threats as well as varied agencies involved in	1. Explain the process of how a crisis begins 2. Discuss the anatomy of a crisis 3. Analyze the issue of forecasting, intervening, and developing crisis plans 4. Communicate the basic concepts of a crisis survey and identifying the crisis 5. Evaluate the approach to	Tier 1-Personal Effectiveness Tier 2- Academic Competencies Tier 3- Workplace Competencies Tier 4- Industry-Wide Technical Competencies

		emergency planning and disaster recovery.	isolating and managing the crisis 6. Demonstrate familiarization with different understandings of risk, particularly risk as a social construct, and the implications of that for community emergency and disaster management.	
SS/CJxxx - Principles of Security Investigations	3	Examine the tools necessary to conduct internal investigations in their business. Case studies will be examined as well as legal aspects of effective litigation avoidance strategies. Students will examine search techniques for both private and public databases and networks to flag potential security threats and root out criminal activity, even before it occurs. Learn emerging technologies such as intelligent agents, link analysis, text mining, decision trees, self-organizing maps, and more to conduct fraud prevention investigations.	1. Discuss the major components and principles of effective security investigations 2. Explain the role of the security manager in criminal investigations and how this role intersects to official public safety related investigations. 3. Evaluate methods of operation and their importance in criminal investigations 4. Apply specific terms and investigative processes and techniques to physical, personnel and information security 5. Analyze legal and privacy issues related to administrative and personnel investigations.	Tier 1: Professionalism Tier 2: Critical and Analytical Thinking Tier 3: Innovative and Strategic Thinking, Problem Solving Tier 4: Compliance and Legal Aspects

CS/CJxxx – Digital Forensics/Investigations	3	Investigation, data gathering, evidence and analysis of crime against computers, systems, networks and crime by usage of computers and other similar personal devices.	1. Ability to access and examine various computers, laptops, smartphones, or other hardware and personal devices to retrieve data and information as forensic criminal evidence. 2. Ability to identify criminal activity, data or information that may be considered evidence. 3. Ability to collect, analyze, and evaluate data and information following proper legal procedures and processes 4. Ability to protect security and integrity of the computer hardware and software as well as the digital evidence 5. Understand laws of evidence and any regulations relevant to digital crime, as well as business ethics and crime by computer 6. Understand cyberattacks against the computer, network or Internet 7. Understand use of computer or other devices to commit crimes	Tier 4 and above - as occupation-specific requirements.
SS/CJxxx – Loss Prevention & Retail Security	3	This course serves is an introduction to the loss prevention field and focuses on retail loss	1. Evaluate the various loss prevention methods and	Tier 1: Integrity and Professionalism

		prevention. Students will learn about the fundamentals of the field including asset protection, risk management, law of loss prevention, methods of and prevention of theft, both internal and external, and the development of asset protection programs.	their importance in deterring theft 2. Compare and contrast the elements of an effective loss prevention program 3. Determine loss prevention practices based on different organization needs, threats and vulnerabilities 4. Identify current critical issues related to shrinkage and loss	Tier 2: Security Fundamentals, Business Foundations (will gain some knowledge of retail management in this class) Tier 3: Primarily Business Acumen, also some Innovative and Strategic Thinking as well as Problem Solving and Decision Making Tier 4: Risk Management, Investigations, Case Management, Business Continuity Tier 5: Loss Prevention
SS/CJxxx – Physical Security & Asset Protection	3	Examines the threat capabilities, legal and others changes that have occurred since 9/11, and emerging technologies that may be useful in the future. The course will include an analysis of neutralization as a performance measure of facility responses and risk assessments. It also addresses the use of the many components that exist to support a security system, and will show how these elements are integrated to deliver an effective system.	1. Discuss the process to design and evaluate a physical protection systems 2. Explain the differences between detection, delay, and response functions 3. Apply the issue of target identification 4. Discuss the basic concepts of risk management as well as risk assessment principles 5. Evaluate the awareness of security in terms of potential loss, threats, and vulnerabilities, and how to respond to them 6. Analyze the approach to risk management that	Tier 1: Personal effectiveness competencies Tier 2: Academic Competencies Tier 3: Workplace Competencies Tier 4: Industry-wide technical competencies Tier 5: Industry sector technical competencies

			links security strategies and related costs to realistic threat assessments and risk levels	
SS/CJxxx – Legal Issues in Security Management or Criminal Law	3	This course presents an up-to-date analysis of significant practices in the security industry that relate to law, regulation, licensure, and constitutional dilemmas. As well as liability problems of security operations. Students will review recent cases.	1. Explain the differences between regulation, licensing, education, training, and professionalism 2. Discuss the issue of search and seizure 3. Evaluate the basic concepts of civil liability and criminal liability 4. Communicate an awareness of security and law enforcement roles 5. Analyze the approach to selected case readings	Tier 1: Professionalism Tier 2: Critical and Analytical Thinking Tier 3: Innovative and Strategic Thinking, Problem Solving Tier 4: Compliance and Legal Aspects
SS/CJxxx – Introduction to Homeland Security	3	This course examines the historical and contemporary governmental actions designed to prevent, detect, respond to, and recover from acts of terrorism and national disasters. Focuses on efforts to align Federal, State, local, tribal, private sector, and non-governmental preparedness, incident management, and emergency response plans into the effective and efficient national structure necessary for the protection of the United States. The course relies upon theories, concepts and case studies	1. Explain the structure and authority of the Department of Homeland Security 2. Describe the manner in which threats are identified, evaluated and mitigated with the rationale behind each of these processes 3. Demonstrate an	Tier 1: Personal effectiveness competencies Tier 2: Academic Competencies Tier 3: Workplace Competencies Tier 4: Industry-wide technical competencies Tier 5: Industry sector technical competencies

		to explore the challenges facing organizations which are a part of protecting our homeland security.	understanding of the federal government structure and the separate cooperative efforts of the relevant federal state and local agencies 4. Describe the various types of threats, natural as well as terrorist, facing the United States and the means of dealing with those threats. 5. Explain the term assessment, preparedness, and mitigation and describe what is involved in each of these processes. 6. Articulate an understanding of the legal, social and policy issues that impact the way in which the Department of Homeland Security and related agencies operate. 7. Explain the Patriot Act and understand the issues regarding legality from both a supportive and non-supportive approach.	

			8. Specifically be able to identify and articulate the CBRNE hazards	
SS/CJxxx – Critical Infrastructure	3	The protection of critical infrastructure is necessary to the continuity of any organization regardless of the mission that it must carry out. In this course students will learn the identification and analysis of critical infrastructure systems including security, risk, and threat assessments. This course will also cover the mitigation of threats as well as evaluation and revision of security measures in order to protect critical infrastructures	1. Identify critical infrastructure sectors, purposes, and threats 2. Evaluate critical infrastructure both public and private sectors 3. Perform risk assessments including vulnerability assessment 4. Report methods to revise security of protection assets 5. Demonstrate mitigation of a critical infrastructure threat	Tier 1: Personal effectiveness competencies Tier 2: Academic Competencies Tier 3: Workplace Competencies Tier 4: Industry-wide technical competencies Tier 5: Industry sector technical competencies
SS/CJxxx – Introduction to Terrorism	3	This course examines all aspects of terrorism from three varied perspectives. First, it will explore the anti and counter terrorism methods in-depth. Topics will include the organization and operation of terrorists, their goals, financing, exploration and the role of the media. An examination of the most violent terrorist acts. In addition, it will explain the roles of law enforcement, the intelligence community, and the authority and mission of the Department of Homeland security. Second, it will identify the origins of Jihad and the role of the Caliphate. It will also look at where Jihad is going and its impact on the world. And third, it will explore the ideology of terrorism through the writings, manifestos, and varied manuals of terrorists from around the world and throughout the ages.	1. Define the various types of terrorism and terrorist threats. 2. Appreciate the history of terrorism and the motivating factors contributing to the perpetration of terrorism domestically and globally. 3. Compare and contrast between different ideologies associated with terrorism and how to identify groups and threats.	Tier 1: Personal effectiveness competencies Tier 2: Academic Competencies Tier 4: Industry-wide technical competencies

			4. Locate and explain the geographical regions around the world sponsoring terrorism or sympathetic to terroristic goals. 5. Define and explain activities of the counterterrorism effort 6. Summarize the benefits and advantages between using force, legislation and intelligence to combating terrorism. 7. Identify the role of the media in terrorism and counterterrorism activities 8. Examine police and governmental responses to terrorism	

CJxxx – Introduction to Basic Research	3	A basic course concentrating on the scientific research in Behavioral Science. Students will acquire information on the methods of collecting data; how to operationalize variables; how to identify types of data; and how to communicate research.	1. Describe and discuss the concepts in Behavioral Sciences research methods and design. 2. Critically analyze scientific claims made in popular and academic media. 3. Analyze and interpret quantitative and qualitative data, as well as, mixed methodology. 4. Enhance public presentation skills through communication of research findings. 5. Demonstrate an understanding of ethical requirements used in research.	Tier 1: Professionalism Tier 2: Critical and Analytical Thinking Tier 3: Innovative and Strategic Thinking, Problem Solving
CJxxx – Capstone Seminar	3	The Capstone Seminar will be conducted seminar style with the student completing a significant research project in the Security Studies field. The research will be presented both in a written paper and the findings presented orally to the class. This research will allow the student to synthesize and demonstrate the knowledge gained over the course of their college studies as well as the application of that knowledge.		
CJxxx Intro to Criminal Justice	3	Introduction to Criminal Justice: This course introduces students to the agencies, processes and theories involved in the administration of		

		criminal justice. The learning objectives include - but are not limited to - examining the major components of the criminal justice system, including the police, courts and corrections and understanding contemporary criminal justice issues and challenges.		
Elective Options	**Credit Hours**	**Description**	**Learning Outcomes**	**ASIS/DOL Competencies**
CJxxx Criminology	3	Criminology: This course introduces students to the study of crime, its causes, and definitions. Learning objectives include – but are not limited to – understanding theories of crime, and identifying correlates of criminal behaviors.		
BUSxxx Accounting I or	3	This course provides a fundamental study of the concepts and methodology of accounting. Learning objectives include gaining knowledge of assets, liabilities		
BUSxxx Business Ethics	3	This course is an introduction to ethical decision -making in business which examines individual, organizational, and macro level issues in business ethics. Students will learn to identify and analyze ethical issues in business, including specific ethical problems such as: whistle-blowing, discrimination, and truth in advertising, employee theft, product safety, and the environment.		
CJxxx Crime Prevention	3	Students will learn about topics to include reasons not to solely rely on the criminal justice system to prevent crime, crime data analysis techniques, crime problem-solving models, models of crime prevention, ingredients of successful private / public		

		partnerships in order to prevent crime and simple methods of implementing and evaluating crime prevention initiatives. Upon completion of this crime prevention course, participants will have a working knowledge of key crime prevention concepts and be familiar with strategies to effectively prevent crime. The practical nature of the training means that the skills and knowledge gained through this training will be directly transferable to the workplace.		
CJxxx White Collar/Organized Crime	3	Introduction to White-Collar Crime provides students with an understanding of what white-collar crime is, how it works, and the extent to which it exists in our society. The wide range of topics analyzes the opportunity structures for committing white-collar crime and explores new ways of thinking about how to control it. Topics include theories behind white-collar crime, including social and psychological theories, routine activity, crime pattern, and situational crime prevention theories, laws that govern the securities industries, including the Securities Exchange Act and Sarbanes–Oxley, bank fraud, money laundering, racketeering, organized crime, crimes involving public		
CJxxx Cybercrime/Cybersecurity	3	Students will learn to protect an organization's critical information and assets by ethically integrating cyber security best practices and risk management through enterprise. Students will also learn processes to integrate continuous monitoring and real-		

		time security solutions with information collection, collaboration, and analysis capabilities, improve cyber security situational awareness and deployment of countermeasures in industry and government, evaluate and assess the use of technology to support cyber security goals and objectives, participate in forensic analysis of cyber incidents and learn how to assist in recovery of operations, and formulate, update, and communicate short- and long-term organizational cyber security strategies and policies.		
CJxxx Fraud Investigation	3	In this course, learners study the principles and methodology of fraud detection and deterrence. The course includes such topics as skimming, cash larceny, check tampering, register disbursement schemes, billing schemes, payroll and expense reimbursement schemes, non-cash misappropriations, corruption, accounting principles and fraud, fraudulent financial statements and interviewing witnesses.		
MATH Statistics	3	This course will introduce students to the basic concepts, logic, and issues involved in statistical reasoning, as well as basic statistical methods used to analyze data and evaluate studies. The major topics to be covered include methods for exploratory data analysis, an introduction to sampling and experimental design, elementary probability theory and random variables, and methods for statistical inference including simple linear regression. The objectives of this course are to help students develop a critical approach to the evaluation of study designs,		

		data and results, and to develop skills in the application of basic statistical methods in empirical research.		
Internship	3	The student should be able to find a curriculum focused position (paid or unpaid) that would expose the candidate to relevant job experience and feedback. The learner should have the ability to draw lines of comparison from the intern opportunity to their coursework and emerge with action items that will help them prepare themselves for post-graduation employment.		