CRIMINAL JUSTICE AND CYBERSECURITY (CJC)

CJC-506: Theories of Justice (3 Credits)
This course examines the nature of justice through careful reading of selected texts in the classical and modern traditions. The importance of justice to the administration of law is emphasized by thoughtful analysis of criminological theory.

CJC-514: Psychological Concepts for Justice Professionals (3 Credits)
This course explores the application of psychological research findings and methods to criminal justice-related issues. It examines what psychology has discovered about how people think and behave and how these discoveries can be useful when making decisions about how criminal justice should be shaped, administered, evaluated, and improved. Students will examine the psychological factors influencing criminal behavior including cyber criminal behavior, psychological health concepts relevant to those who serve in the criminal justice field including resilience and wellness, the role of psychology in law enforcement and legal proceedings, and the application of psychological principles in correctional settings.

CJC-518: Domestic & Global Challenges Shaping Public Policy (3 Credits)
Using case analysis and personal experimentation, students explore domestic and international factors that influence government national security strategy, as well as how these decisions impact the justice system and homeland security in a multicultural society.

CJC-519: U.S. Intelligence Community (3 Credits)
The U.S. Intelligence Community course provides a foundational and broad overview of the field of intelligence collection and how information gathered is analyzed and used by Policymakers, Combatant Commanders, US Embassy Country Teams, and Foreign Partners to make the most informed decisions effecting our national and global security strategy. The course discusses the fundamental components of strategic intelligence collection, critical thinking, collection capabilities, counterintelligence, influences and implications of cyber and AI/ML, and provides an understanding of the Agencies that perform these duties. This course uses a variety of approaches to explore pertinent issues including interactive lectures, guest speakers from US and NATO intelligence Agencies, student-led discussions, and exercises.

CJC-520: Effective Communication and Perspective Taking (3 Credits)
We've heard a lot in recent years about emotional intelligence and the difference it can make in how we are perceived by those around us in the wor1<.place, in our communities, and in our homes. Emotionally intelligent communications can deepen our connections with others, improving relationships and building trust. In this course, you will develop fundamental strategies to improve your emotional intelligence. With self awareness and empathy as the foundation, we will learn communication strategies for verbal interactions, written communications and presentations that will help us achieve our goals as we focus on the needs of those receiving our message (servant leadership). Communication is not just about sending messages, so we will also focus on neutral listening as a tool to improve relationships and build trust. This course will also cover social media considerations and the opportunities and challenges for organizations these channels present. You will learn theory, practical tools, and get some practice opportunities to help you improve your work experience and your leadership.

CJC-521: Critical Leadership Opportunities (3 Credits)
Students examine issues facing justice practitioners today from a leadership perspective. They will gain a deep understanding of those issues, applicable theories, and approaches that can help improve outcomes in the identified areas. Leaders at all levels have a role in approaching these challenges, and students will gain understanding about the differences in that role based on their position and assignment in an organization.

CJC-524: Emergency Management & Critical Incident Response (3 Credits)
This course will provide current and future leaders with the knowledge and skills needed to respond well to critical incidents. Students will learn a standards-based language, including the use of the Incident Command System (ICS), to coordinate their response as they undertake their role in a complex multi-jurisdictional response to an all-hazard event. Students will learn that all hazards are 1ocal," but can escalate into an event of global significance and consequence. In addition to NIMS and ICS, this class will cover crisis leadership, critical decision-making and crisis communications, preparing leaders for their role in helping their community and organization through crises and emergencies.

CJC-526: Principles of Digital Forensics (3 Credits)
This course will introduce students to the principles of digital forensics. The essentials covered in this class will include computer system storage fundamentals, operating systems and data transmission, computer network architecture, best practices when conducting digital forensic investigations, proper evidence collection and storage, and federal rules and criminal codes when conducting digital investigations. Students will participate in weekly discussions and practice what they have learned via virtual labs.

CJC-528: Cultivating Organizational Culture (3 Credits)
Pre-requisite(s): CJC-520 is required.
Every organization has a culture. Many have pointed at an organization's culture when looking to lay blame for egregious actions by its members. Many have also looked at the opposite side, organizations with strong and positive cultures leading to strong employee satisfaction and engagement and support from the customers or communities they serve. This course will be a study of organizational culture and the application of these concepts and theories in justice related settings. Once this foundation is laid, students will explore how they, whatever their position in their organization, can positively influence the climate and culture in their work area using values-based leadership, procedural justice, coproduction of leadership, and other techniques.

CJC-530: Cyberthreat Analysis (3 Credits)
This course explores the relatively new discipline of cyberthreat analysis at a basic level, introducing students to the methodology of investigation, the threat environment (cyberspace), some of the online tools used by analysts, and their application in real world examples. Students will be introduced to the key concepts, tools, and terminologies used by professionals in the field, and apply what they learn in practical exercises that model real-world events.

CJC-531: Cyberthreat Management (3 Credits)
This course explores the relatively new discipline of cyberthreat management. This course will introduce students to the threat landscape and help them to understand the methodology used to mitigate threats to personnel and their agencies. Students will learn about some of the tools and resources currently used by technicians so that they will gain a better understanding of how investigations may be more successful in a constitutionally ethical process. Students will understand the necessity of cyberdisruption planning with a goal of redundancy and resiliency. Economics will inevitably force managers to regionalize services and facilitate an interoperable solution. Students will develop this knowledge from a basic understanding of risk management and control, along with a study of legal and compliance topics. The field of forensics will be explored including a demonstration of how a forensic analysis is performed, and how to manage the process of a technical investigation.

CJC-532: Cyberterrorism (3 Credits)
The field of cyberintelligence has expanded and is evolving as a critical part of situational awareness for the nearly 200 countries connected to the Internet today. In addition to these countries, criminal organizations, extremist groups and terrorists have also developed cyber intelligence capabilities to further their efforts to use the Internet for their overt and covert activities. Cyberterrorism has emerged as a growing threat to national security. This is true not only for the U.S., but also for many countries around the world. Terrorists have recognized the value of the Internet for recruiting and covert communication, as well as a weapon against their adversaries. This program will provide unique insight into how terrorists use the Internet and will give the students insights into the challenges that we face.

CJC-534: Cyber Fundamentals (3 Credits)
This course will prepare you for an exciting. career in the field of cybersecurity. As a student, you will delve into the foundational concepts that underpin digital security. You will explore critical topics such as network security, threat detection, penetration testing, incident response, and risk management. The curriculum is designed to closely align with the CompTIA Security+ certification, an ideal steppingstone towards becoming a certified cybersecurity professional. Furthermore, as a student, you will gain insights into the latest developments in cybersecurity, including the integration of artificial intelligence for threat analysis and mitigation. This course will seek to enhance your practical skills and knowledge in these areas and empower you to effectively safeguard digital environments. (If you already hold an active Security + certification, you may be able to substitute a cyber elective for this course).

CJC-537: Network Forensics and Incident Response (3 Credits)
This course will introduce students to the topic of network security and provide them with a background on networking fundamentals such as common protocols, port numbers and relevant security appliances (firewalls, web filtering, IDPS). An emphasis will be placed on covering different types of network intrusion events and proposing countermeasures that can be applied by network defenders to detect/prevent these types of attacks. Students will also be trained on how to perform live collection & analysis of network events through the examination of packet capture (PCAP) files via Wireshark in order to understand the different pieces of evidence that can be gathered from such evidence and subsequently deployed as signatures to perform attack sensing and warning (AS&W) across an enterprise network.

CJC-540: Executive Leadership Development (3 Credits)
Pre-requisite(s): CJC-520 is required.
Many employees have performed well at the line level and in first level supervisory positions and have been rewarded for their performance with a promotion, only to discover that they are ill prepared for their new role and that the techniques that drove their success earlier in their career are no longer relevant. Whatever their current position, this course equips students with the necessary skills and perspective to continue their growth and success as they move to new leadership roles. This course will address leader development, leadership perspective, adaptability, conflict resolution, problem solving, strategic planning and strategic communications for leaders.

CJC-543: Cyber Intelligence (3 Credits)
This course provides an understanding of the current and future environment surrounding cyber intelligence. The course examines the foundational terms such as cybersecurity and cyberwarfare, and explores current and emergent cyber threats, effects of AI/ML, cyber threat actors, and mechanisms for increased cyber resiliency in the public and private sectors. The students are asked to think critically as they address current cyber intelligence collection management, analytical techniques, tradecraft, security, and counterintelligence methods.

CJC-546: Insider Threat (3 Credits)
This course will challenge students to think more systemically about the current threat landscape as it relates to insider threats. This course is designed to assist management, human services, and information technology professionals with the prevention, detection, and mitigation of risks associated with Insider Threats. Instructional methods include readings, written assignments, online discussion forums, and computer lab assignments.

CJC-550: Intelligence Writing and Communicating (3 Credits)
Pre-requisite(s): CJC-519 or CJC-543 is required.
This course provides students with comprehensive instruction on writing and communicating intelligence for US Government policy makers and other intelligence consumers. Students will be instructed in the application of Intelligence Community Directive 203 which prescribes the use of Estimative Language, nine analytical tradecraft standards for all intelligence production, and customized intelligence report writing. Upon successful completion of the course, students will be able to write intelligence reports to US Intelligence Community (USIC) standards.

CJC-556: Open Source Intelligence (3 Credits)
The daily threat of cybersecurity incidents has led private and public sector entities to treat intelligence gathering as a pivotal and crucial daily operation. This course will teach students the skills and techniques required to conduct open-source investigations using a wide range of publicly available resources including online databases, social media, news articles, internet archives, government website and more. Resources gathered in an open-source investigation are an essential pan of defending an organization's online infrastructure. Students will be trained to ethically verify, authenticate, and assess the credibility of the information gathered and learn to articulate their findings in a well organized and structured report.

CJC-560: Structured Analytic Techniques (3 Credits)
Pre-requisite(s): CJC-519 or CJC-543 is required.
This scenario-based course provides students with comprehensive instruction on the use of Structured Analytic Techniques (SATs) in mitigating inherent cognitive and other biases, and in analyzing incomplete information sets to determine best supported analytic solutions and outcomes. Upon successful completion of this course, students will be able to apply SATs to complex and/or incomplete sets of data to determine the best analytically supported and bias-free solutions, most likely outcomes, and best supported recommendations to policy makers.

CJC-563: Criminal Justice Research Methods (3 Credits)
This course examines a wide range of quantitative and qualitative statistical techniques, and the applied use of survey instruments, transpersonal research methods, and data visualization best practices. Upon completion, students will have the ability to both interpret data and present research findings to senior decision makers to allow them to make informed policy-level choices.

CJC-570: Cybersecurity Law (3 Credits)
It is by now cliche to observe that technology is revolutionizing the way we work, live, and govern ourselves. Never before have communications and data sharing been achievable so quickly and across the planet geographically. Unfortunately, the exponential increase in technological ability has in the same manner increased the opportunities for thieves, exploiters, and spies. In this course we will explore how our society and governments are using the law - both civil and criminal and both domestic and international to respond to these challenges. How can law keep up with technological change? How far can and should the government be allowed to go in protecting U.S. citizens? Ale the present policies adequate? What responsibilities lie in the private sector?

CJC-576: High Technology Crime (3 Credits)
This course studies the response of law enforcement and information systems scientists to the use of computers and related technologies for criminal purposes. While no prior computer knowledge is required, students will use computers as a part of this class. Major policy issues surrounding this area will also be discussed.

CJC-579: State Sponsored Advanced Persistent Threats (3 Credits)
Pre-requisite(s): ADJ-576 or CJC-576 is required except for SMEs in the field and working professionals.
This course is designed to broaden individual understanding of the ever changing threatscape posed to American infrastructure by advanced and persistent nation-state/state sponsored attacks. The class will also prepare students to begin a career in a Cyber Security Operations Center (SOC), Computer Emergency Response Team (CERT) or as a cyber intelligence analyst by fostering technical and analytical skills against known APT skill sets and tool kits.

CJC-581: Special Topics (3 Credits)
This course provides an opportunity to explore current topics not covered in regularly offered courses. Evolving technologies and contemporary trends in justice and homeland security law and practice may create opportunities to present the most timely and important topics to students. All students may individualize their program of study to access special topics classes with collaboration and permission from the program director. Recent topics have included: The Philosophy of Police, Strategic Planning for Law Enforcement Executives, Community Policing, Organized Crime, White Collar Crime, Contemporary Issues in Undercover Operations, Police Use of Force, and Advanced Community Policing.

CJC-598: Internship (3 Credits)
The internship is an individual work experience or project in an organization (normally off-campus) under the supervision of a practicing professional and structured by a Salve Regina University faculty member. Although the specific nature of the internship varies with the student's academic interest, there should be a close relationship between the program of study and the non-academic setting. The internship is a supervised learning experience for academic credit typically consisting of a minimum of 120 hours (40 hours/credit) of on-the-job experience occurring within a semester. This course may be repeated for a total of six credits.