PROFESSIONAL STUDIES CYBERSECURITY STRATEGY AND INFORMATION MANAGEMENT (PSCS)

Explanation of Course Numbers

- Courses in the 1000s are primarily introductory undergraduate courses
- Those in the 2000s to 4000s are upper-level undergraduate courses that also may be taken for graduate credit with permission and additional work assigned
- Those in the 6000s and 8000s are for master's, doctoral, and professional-level students
- The 6000s are open to advanced undergraduate students with approval of the instructor and the dean or advising office

PSCS 2301. Cyber Investigation. 4 Credits.
The investigative framework and tools needed for the investigation of cyber crime. Crimes that involve computer technology; procedural and tactical issues associated with the prosecution of cyber crime.

PSCS 2302. Digital Forensics. 4 Credits.
An introduction to digital forensic science and the systematic process of acquiring, authenticating, and analyzing digital evidence. Forensic methods and laboratories; tools, techniques, and methods used to perform computer forensics and investigation; and emerging technologies. Theoretical and practical experience using forensic equipment and software.

PSCS 2303. Compliance and Risk Management. 4 Credits.
Data protection from a risk management perspective. Data retention; security and protection technologies; technology requirements for compliance, governance, and data security; the importance of e-discovery for civil litigation; the impact of third-party services in conjunction with data protection; and data processing facets, such as the role of tiering and server and storage virtualization.

PSCS 2304. Incident Response. 4 Credits.
Principles and techniques for detecting and responding to current and emerging computer security threats. Data breaches, advanced malware, and targeted attacks. Law and policy related to incident response.

PSCS 3100. Principles of Cybersecurity. 4 Credits.
Basic principles and concepts in information security and information assurance; technical, operational, and organizational issues of securing information systems.

PSCS 3103. Ethics, Law, and Policy. 4 Credits.
Overview of ethical, legal and policy issues related to the impact of modern technology on society; ethical theories and decision making, professional responsibility and codes of ethics, copyright and intellectual property, information accountability, freedom of information and privacy, the Internet and considerations associated with information sharing and social networking.

PSCS 3107. IP Security and VPN Technology. 4 Credits.
Risks associated with an organization's network being connected to the public Internet; defensive technologies, types of encryption, enterprise firewalls, intrusion detection/prevention, and access control technologies; active threat agents and exploitation techniques used to compromise the digital infrastructure.

PSCS 3109. Network Security. 4 Credits.
Security aspects of networks and network technology; intrusion detection, virtual private networks (VPN), and firewalls; types of security threats, security policy design and management; and security technologies, products, and solutions.

PSCS 3110. Cloud Security. 4 Credits.
Explores the architecture, security design principles, design patterns, industry standards, applied technologies, and regulatory compliance requirements critical to the delivery and management of secure cloud-based services. Restricted to students in the BPS in cybersecurity program. Prerequisites: PSCS 3100.

PSCS 3111. Information Technology Security System Audits. 4 Credits.
Theory, methodology, and procedures related to IT system audits; proper audit procedures for discovering system vulnerabilities; documenting findings according to the standards of compliance based auditing.

PSCS 3113. Topics in IT Security Defense Countermeasures. 4 Credits.
Theory, methodology, and practical experience relating to IT defense countermeasures; system vulnerabilities and how adversaries can exploit them.

PSCS 3117. Project Management in Information Technology. 4 Credits.
Concepts and basic functions of the project management body of knowledge, including scope, quality, time, cost, risk, procurement, human resource, and communication management and integration of these functions into a project management system; roles and responsibilities of various project staff.

PSCS 4102. Intrusion Detection and Vulnerability Management. 4 Credits.
The use of intrusion detection systems (IDS) as part of an organization's overall security mechanisms; implementation and testing of IDS security plans, security monitoring, intrusion detection, alarm management, analysis of events and trends, and vulnerability management.

PSCS 4110. Data Communication and Networking Technologies. 4 Credits.
Overview of the networking technologies deployed by modern enterprises. Hardware and software used to transfer information from source to destination, including switches, routers, firewalls, Ethernet, and the TCP/IP protocols suite. (Same as PSIS 4141)

PSCS 4202. Cyber Attack Tools and Techniques. 4 Credits.
Linux-based introduction to traditional and contemporary attack tools and technologies used by threat actors. Constructing an effective computer network defense.

PSCS 6244. Information Systems Protection. 3 Credits.
Major areas of information security, including risk management, cybercrime, cyber conflict, and the technologies involved in both cyber attacks and information systems protection; root causes of insecurity in information systems and the processes involved in creating, implementing, and maintaining an information security program. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6245. Cybersecurity Law and Policy. 3 Credits.
Law and policy perspectives on the federal government's response to cyber threats; legal concepts relating to investigation and enforcement activities; application of traditional laws of armed conflict in cyberspace; and national security concerns. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6246. Cyber Intelligence and Strategic Analysis. 3 Credits.
National and international cyber strategies, law, and policy as they relate to cyber intelligence efforts with a review of current cyber threats to national security; identification of strategic, operational, and tactical cyber intelligence efforts, the cyber threat landscape, and intelligence-led policing relative to cyber enforcement and investigation. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6247. Cyber Defense Strategy. 3 Credits.
The fundamentals of cyber defense strategy; understanding the organization's threatscape and building a threat matrix to prioritize and monetize cyber security defense needs; creating a sound cyber defense strategy through efficient use of known security management practices and establishing a management program to implement the defense strategy. Restricted to students in the MPS in CSIM program or with the permission of the instructor. Prerequisite: None.

PSCS 6248. Introduction to Cyber Conflict. 3 Credits.
The emerging concept of cyber conflict, its history over the last 25 years, and its integration into government and military strategies; technical, tactical, and strategic use of information technology between state and non-state actors; cyber conflict as an evolving phenomenon. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6255. Information Management for Justice and Public Safety Professionals. 3 Credits.
Application of information management techniques to justice and public safety fields; governance structure, emerging modes of communication within and outside organizations, and processes that enable managers to make timely decisions. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6256. Application of Technology to Data Analytics. 3 Credits.
Strategic application of technology to data analysis; introduction to leading edge software, including predictive and spatial analytics; principles of data visualization and application of analytics and visualization to solving justice and public safety problems; data collection, analysis, and production of usable information output. Restricted to students in the MPS in cybersecurity strategy and information management program.

PSCS 6257. Enterprise Architecture and Standards. 3 Credits.
Current and emerging trends in enterprise architecture domains; technology environments, including software, hardware, networks, applications, data, communications, and other relevant architecture disciplines; service-oriented architecture and similar innovations; conventions, principles, and practices for creating enterprise architectures; contemporary standards-based architectures for system development; industry guidelines and standards. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6258. Information Sharing and Safeguarding. 3 Credits.
Key principles of privacy and safeguarding of information; how information is shared among government agencies, outside the federal government, and between the government and the private sector. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6259. Strategic Information Technology Investment and Performance Management. 3 Credits.
The effective use of information technology within organizations; integration of IT in business processes, performance measurement, cost benefits analysis, and program evaluation; cross-disciplinary and comprehensive with examples from federal, justice and public safety, and industry organizations. Restricted to students in the MPS in CSIM program or with the permission of the instructor.

PSCS 6260. Methods of Analysis in Security. 3 Credits.
Methods and problems of data collection in security fields with a focus on cybersecurity related issues and readings; analytical design, instrument utilization, sampling, and measurement; data analysis techniques. Restricted to students in the MPS in CSIM program.

PSCS 6270. Capstone Project. 3 Credits.
Designed to help participants refine their conception of leadership in and knowledge of the cybersecurity field. Students must have completed the MPS in CSIM program curriculum before enrolling in this course. Restricted to students in the MPS in CSIM program.