MASTER OF PROFESSIONAL STUDIES IN THE FIELD OF CYBERSECURITY STRATEGY AND INFORMATION MANAGEMENT

The Master of Professional Studies in the field of cybersecurity strategy and information management degree program is for working professionals from the military, homeland security, and private sectors who wish to gain the expertise to address current and emerging challenges in information technology security. Students learn strategies and practices that empower them to manage critical information in the fight against hackers, terrorists, and cyber criminals. The program also enhances the skills of current homeland security and criminal justice professionals, preparing leaders to secure the country's digital infrastructure.

Specific admission requirements can be found on the Graduate Program Finder (http://www.gwu.edu/all-graduate-programs). (http://www.gwu.edu/all-graduate-programs)

Visit the program website (http://cps.gwu.edu/cybersecurity) for additional information.

REQUIREMENTS

The following requirements must be fulfilled: 36 credits in required courses.

Code	Title	Credits
Required:		
PSCS 6244	Information Systems Protection	
PSCS 6245	Cybersecurity Law and Policy	
PSCS 6246	Cyber Intelligence and Strategic Analysis	
PSCS 6247	Cyber Defense Strategy	
PSCS 6248	Introduction to Cyber Conflict	
PSCS 6255	Information Management for Justice and Public Safety Professionals	
PSCS 6256	Application of Technology to Data Analytics	
PSCS 6257	Enterprise Architecture and Standards	
PSCS 6258	Information Sharing and Safeguarding	
PSCS 6259	Strategic Information Technology Investment and Performance Management	
PSHS 6260	Methods of Analysis in Security	
PSHS 6270	Capstone Project	

FACULTY

Associate Director: *C. Utoff*

COURSES

Explanation of Course Numbers

- Courses in the 1000s are primarily introductory undergraduate courses
- Those in the 2000s to 4000s are upper-division undergraduate courses that can also be taken for graduate credit with permission and additional work
- 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 2101. Writing and Communication in a Technical Field. 4 Credits.
The fundamentals of reading and writing with a clear sense of purpose and audience. How academic writing in virtually any subject area and on virtually any topic represents a formal engagement with larger scholarly debates. The writing process, including prewriting, drafting, and revision as well as basic research methods. Making clear oral presentations. (Same as PSIS 2101).

PSCS 2102. Fundamentals of Information Technology and Computing. 4 Credits.
Basic concepts of programming including elementary data types (numeric types, strings, lists, and files), control flow, functions, objects, loops, and methods will be covered. Designing, maintaining, and implementing programs in a modern programming language. (Same as PSIS 2105).

PSCS 2103. Ethics in the Age of Technology. 4 Credits.
Ethical issues relevant to the age of technology and their role in science and technology policy making and implementation. Topics include ethical theories and decision making; professional responsibility and codes of ethics; copyright and intellectual property; information accountability, freedom of information, and privacy; information sharing and social networking; and biotechnology innovations and medical practices. (Same as PSIS 3122).

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 2305. Practicum: Incident Response Techniques. 2 Credits.
Students integrate and apply acquired knowledge and technical skills in computer laboratory settings with a focus on cyber investigation and incident response techniques.

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 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. Topics vary by semester. May be repeated for credit provided the topic differs. See department for more details.

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 4101. Introduction to Protection Technologies. 4 Credits.
The technologies most commonly used to protect an organization's information; threat agents and the exploitation techniques they use to compromise systems; and defensive technologies, including encryption, enterprise firewalls, intrusion detection/prevention, and access control technologies.

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 4103. Securing Operating Systems. 4 Credits.
The security techniques and technologies integrated into Microsoft operating systems, which are a frequent target of attacks; primary threats and protection mechanisms developed by Microsoft and others; tools used to defend against known risks and vulnerabilities; client and server operating systems, OS hardening, application security, and Active Directory.

PSCS 4104. Securing Network Devices. 4 Credits.
Key network components and devices that need to be secured in order to protect networks from attack; practical and theoretical perspectives on network protection technologies; weaknesses and vulnerabilities; mitigation strategies; viruses, worms and other threats.

PSCS 4105. Cyber Defense Techniques Practicum. 2 Credits.
Working with cybersecurity experts and other qualified computer laboratory personnel, students integrate, apply, and strengthen acquired knowledge and technical skills in laboratory settings.

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 4190. Capstone Project. 4 Credits.
Students use the knowledge and skills acquired throughout the program to conduct significant, independent research or work on a real-life project relevant to their interest in the security field. (Same as PSIS 4190).

PSCS 420. Computer Network Attack and Exploitation. 4 Credits.

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 4203. Analysis of the Intelligence Cycle. 4 Credits.
The intelligence cycle and sources. Target modeling and organizational analysis; quantitative and predictive techniques. The role of intelligence collectors, consumers, and analysts in developing a conceptual model of the intelligence target.

PSCS 4204. Computer Network Attack and Exploitation. 4 Credits.
Cyber attacks orchestrated by computer networks to distract, deny, degrade, or destroy other computer networks or information within large computer systems. Developing standardized attack scenarios to be used against specific targets and providing operational planning to conduct network attacks.

PSCS 4205. Practicum: Cyber Attack Techniques. 2 Credits.
Students integrate and apply acquired knowledge and technical skills in computer laboratory settings. Various cyber attack tools and techniques, including penetration testing and ethical hacking.

PSCS 6244. Information Systems Protection. 3 Credits.
The major areas of information security, including risk management, cybercrime, cyber conflict, and the technologies involved in both cyber attacks and information systems protection. Students develop an understanding of the root causes of insecurity in information systems and explore the processes involved in creating, implementing, and maintaining an information security program. Restricted to Open only to students in enrolled in graduate PSCS degree. Prerequisites: None.

PSCS 6245. Cybersecurity Law and Policy. 3 Credits.
Law and policy perspectives of 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. National security concerns. Restricted to Open only to students enrolled in graduate degree in PSCS. Prerequisites: None.

PSCS 6246. Cyber Intelligence and Strategic Analysis. 3 Credits.
Current issues in cyber intelligence and models for cyber intelligence collection methods and analysis. National and international cyber law and policy as they relate to cyber intelligence efforts. Current cyber threats to national security. Strategic, operational, and tactical cyber intelligence efforts and countermeasures; cyber weapons, actors, and methods of delivery; and advanced persistent threats (APTs) and the cyber threat landscape. Review of an intelligence-led policing model as it relates to cyber enforcement and investigation. Restricted to Limited to degree candidates in PSCS. Prerequisites: None.

PSCS 6247. Cyber Defense Strategy. 3 Credits.
An introduction to the fundamentals of cyber defense strategy. Focus on raising an organization's cyber security posture from low to high. 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. Establishing a management program and building a security team to implement the defense strategy. Restricted to Open only to students enrolled in degree program in PSCS. Prerequisites: None.

PSCS 6248. Introduction to Cyber Conflict. 3 Credits.
Exploration of the emerging concept of cyber conflict, its history over the last 25 years, and how this concept is being integrated into government and military strategies. Case studies are used to highlight the technical, tactical, and strategic use of information technology between state and non-state actors. The current state and the future of cyber conflict as an evolving phenomenon. Restricted to Limited to degree candidates in the PSCS program. Prerequisites: None.

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 organization, and processes that enable managers to make timely decisions. How information technology trends affect organizations; emerging technologies, standards, and government program objectives that affect IT implementation. Restricted to students in the Master of Professional Studies in Cybersecurity Strategy and Information Management program.

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. Students are exposed to software and strategies related to data analysis for the purpose of creating actionable intelligence and learn the importance of aligning the use of information technologies. Restricted to students in the Master of Professional Studies 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. Focus on 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.

PSCS 6258. Information Sharing and Safeguarding. 3 Credits.
Government collection, retention, and dissemination of information for criminal intelligence, national security, and other purposes. 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. Emerging legal, regulatory, and policy issues in information sharing, including executive branch and legislative initiatives. Restricted to students in the Master of Professional Studies in Cybersecurity Strategy and Information Management program.

PSCS 6259. Strategic Information Technology Investment and Performance Management. 3 Credits.
The effective use of information technology within organizations. Topics include the integration of IT in business processes, performance measurement, cost benefits analysis, and program evaluation. Restricted to students in the Master of Professional Studies in Cybersecurity Strategy and Information Management program.