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

Program Director: E. Lammert,

Associate Director: C. Uthoff

With the precipitous rise in global cybercrime, espionage and terrorism, it is no surprise that cybersecurity is now the number one national security issue we face. Yet as these agents of chaos seem to multiply by the minute, we're facing a crucial shortage of cybersecurity leaders who can take on this fight. To solve the cybersecurity problem, we must fill this critical gap.

Designed in consultation with key government, military, and law enforcement organizations, GW's master's degree program in cybersecurity strategy and information management addresses issues of law, policy, and leadership to help create the next generation of cybersecurity's strategic leaders. With a degree that can be completed in as few as 16 months, students learn from the field's top experts about the strategies and practices that protect critical information and ensure the world's digital infrastructure remains secure.

Visit the program website (https://cps.gwu.edu/masters-cybersecurity-strategy-information-management/) for additional information.

ADMISSIONS

Admission deadlines:	Fall Term:
	Campus Locations: Arlington or Online Education
	Priority Deadline: April 15
	Final Deadline: June 15 (Applications received after June 15 will be reviewed, space permitting)
	Spring Term:
	Campus location: Online Education
	Application Priority Deadline: November 1
	Application Final Deadline: November 30
Recommendations required:	Two (2) recommendations
Prior academic records:	Transcripts are required from all colleges and universities attended, whether or not credit was earned, the program was completed, or the credit appears as transfer credit on another transcript. Unofficial transcripts from all colleges and universities attended should be uploaded to your online application. Official transcripts are required only of applicants who are offered admission.
	Transcripts from institutions outside the United States must be accompanied by an official transcript evaluation from an accredited independent evaluating agency. Please be sure you request a detailed, course-by-course evaluation that includes all course titles, credit hours, grade-point average (GPA), United States degree equivalency, and date of degree conferral. Please see the list of acceptable international credential evaluation services.
Statement of purpose:	In an essay of 250-500 words, state your purpose in undertaking graduate study in this field and describe your academic objectives, research interests, and career plans. Also discuss your related qualifications, including collegiate, professional, and community activities, as well as any other substantial accomplishments not already mentioned on the application form.
Additional requirements:	A resumé
International applicants only:	Please follow this link - https://www.cps.gwu.edu/international-student-admissions (https://www.cps.gwu.edu/international-student-admissions/) - to review the International Applicant Information carefully for details on required documents, earlier deadlines for applicants requiring an I-20 or DS-2019 from GW.

Supporting documents not submitted online should be mailed to:
College of Professional Studies – Office of Admission
Alexandria Education Center
413 John Carlyle Street, Suite 250
Alexandria, VA 22314

Contact for questions:
CPS Office of Admission
applycps@gwu.edu ~ 571-553-0100 (phone) ~ 202-242-1047 (fax)
8:30 am – 5:00 pm EST, Monday through Friday

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 in a Digital World
PSCS 6256	Data Management and Security
PSCS 6257	Enterprise Cybersecurity Program Management
PSCS 6258	Information Sharing and Safeguarding
PSCS 6259	Strategic Information Technology Investment and Performance Management
PSCS 6260	Methods of Analysis in Security
PSCS 6261	Advanced Topics in Cybersecurity *
PSCS 6270	Capstone Project *

*Students can take a course offered under PSCS 6261 in place of the Capstone Project (PSCS 6270) with the program director's approval.

COURSES

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 can also 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 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 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 2304W. Incident Response. 4 Credits.
Provides fundamental skills to respond to computer security incidents in an information system. Covers three main types of incidents: data breaches, advanced malware, and targeted attacks. Learn how to plan, respond, and report such incidents. Includes a significant engagement in writing as a form of critical inquiry and scholarly expression to satisfy the WID requirement.

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 3103W. Ethics, Law, and Policy. 4 Credits.
Overview of ethical, legal, and policy issues related to the impact of modern technology on society. Includes a significant engagement in writing as a form of critical inquiry and scholarly expression to satisfy the WID requirement.

PSCS 3105. Governance, Risk Management, and Compliance. 4 Credits.
Foundations of data protection from a risk management perspective with an introduction to the governance, risk, and compliance (GRC) framework. Data protection technologies, special technology requirements for compliance, governance, data security.

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 3115. Cyber Investigations and Threat Intelligence. 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 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 in a Digital World. 3 Credits.
Application of information management techniques to justice and public safety fields including governance structure, project management, technology acquisition, and emerging technology trends affecting the industry. Restricted to students in the MPS in cybersecurity strategy and information management program or with the permission of the instructor.

PSCS 6256. Data Management and Security. 3 Credits.
Examination of data management through the lens of the data pipeline to identify critical information needs. Assessing information needs to propose new data systems with actionable intelligence for stakeholders. Restricted to students in the MPS in cybersecurity strategy and information management program.

PSCS 6257. Enterprise Cybersecurity Program Management. 3 Credits.
Fundamentals of enterprise architecture (EA). Standards that can be used to build systems, networks, and security using theory and standards to understand how EA outputs are foundational in establishing a cybersecurity program. Restricted to students in the MPS in cybersecurity strategy and information management 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 6261. Advanced Topics in Cybersecurity. 3 Credits.
Topics vary by semester. Can be repeated for credit provided the topic differs. Consult the Schedule of Classes for more details.

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.

PSCS 6291. Independent Study. 3 Credits.
Self-paced independent study related to a relevant topic or trend in the cybersecurity industry selected by the student(s).