MASTER OF PROFESSIONAL STUDIES IN THE FIELD OF TRANSFORMATIONAL LEADERSHIP IN CYBERSECURITY

OVERVIEW

The executive master of professional studies (MPS) in transformational leadership in cybersecurity is designed in response to the evolving reality that cybersecurity is no longer a purely technical or compliance function, but a core enterprise, governance, and public accountability challenge. While many graduate programs remain tool-focused or compliance-driven, this program addresses a critical gap in preparing leaders to operate at the intersection of technology, risk, policy, and institutional power.

The executive MPS is a leadership-first, experiential degree that prepares current and aspiring CISOs and senior technology executives to govern, influence, and transform organizations in complex, high-stakes environments. Grounded in executive competencies such as board-ready communication, political and fiscal risk strategy, regulatory navigation, crisis leadership, emerging technology governance, and cross-functional influence, the curriculum integrates applied coursework, simulations, executive residencies, and institutional projects.

Throughout the program, students develop the ability to translate technical risk into fiduciary and operational impact, quantify and prioritize enterprise risk, navigate regulatory and geopolitical complexity, and lead coordinated responses under public and institutional scrutiny. Through a practicum and capstone grounded in their own organizations, graduates produce and defend executive-level cybersecurity strategies that demonstrate coalition-building, ethical judgment, and the capacity to influence decision making at the highest levels

ADMISSIONS

The following requirements ensure that participants are prepared to engage with board-level strategy, organizational influence, and complex national and global cyber challenges:

- Recommended minimum GPA: 3.0
- Bachelor's degree in cybersecurity, IT, or a closely related field
- At least 10 years of professional experience, including at least 5 years in senior/management roles in cybersecurity or IT risk management; privacy; compliance; or adjacent leadership; or closely related field(s)

If any of the above minimum requirements are not met or are unclear on the application, the admissions committee may request an interview with the candidate.

Admission Deadlines

Fall: Priority – April 15; Final – June 15

Spring: Priority – November 1; Final – November 30

Required Application Materials

Candidates must complete an online application by the deadline that includes the following materials:

- Recommendations required: One (1) recommendation (ideally from a supervisor or executive sponsor)
- 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 750-1000 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 or CV
- Optional materials: Optional portfolio/work samples (de-identified)

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.

Advanced standing/waivers: Up to 3–6 credits may be waived for prior executive experience, per CPS policy and faculty review.

REQUIREMENTS

The following requirements must be fulfilled: 30 credits in required courses.

Code	Title	Credits
Required:		
PSCS 6501	Cyberlaw & Ethical AI for Technology Leaders	
PSCS 6502	Enterprise Risk and Political Dynamics in Executive Decision Making	
PSCS 6503	Executive Risk & Investment	
PSCS 6504	Cyber Intelligence for Geopolitical & Institutional Risk	
PSCS 6505	Emerging Technology and Cyber Frontiers	
PSCS 6506	Executive Strategies for Enterprise Architecture	
PSCS 6507	Political Influence and Organizational Power in Executive Leadership	
PSCS 6508	Leading through Institutional Uncertainty	
PSCS 6509	Boardroom Cyber Governance	
PSCS 6510	Executive Crisis Governance	
PSCS 6511	Communication and Media Strategy for Cyber Executives	
PSCS 6598	Cybersecurity Leadership Practicum	
PSCS 6599	Executive Cybersecurity Capstone	