Online Master of Engineering in Cybersecurity Policy and Compliance

Onlinecybersecurity.seas.gwu.edu

School of Engineering & Applied Science
THE GEORGE WASHINGTON UNIVERSITY
The School of Engineering and Applied Sciences (SEAS) at the George Washington University has been bringing together great minds in industry and government since the 1800s. Throughout time, it has evolved to help professionals meet the technological challenges of the day. We’re excited to bring you our new, fully-online Master of Engineering in cybersecurity policy and compliance (M.Eng.[CPC]). Drawing on close connections to D.C. institutions, the program gives students the knowledge they need to lead initiatives and learn continuously as the field of information assurance changes.

The M.Eng.(CPC) is designed to teach students to innovate and to maintain tried-and-true security practices. This aligns with the School’s mission to contribute positively to the scientific sphere. More than half of the SEAS faculty received their doctoral degrees from the nation’s top engineering and computer science programs, positioning them to give students a high-level understanding of cybersecurity and the policies that propel it forward.

The curriculum focuses on the laws that shape the industry and how best to comply with them as a cybersecurity professional. In a world where the top priority of organizations is the protection of their private data, students will learn the creative, operational, and technical skills they need to advance in their current roles or transition into their desired positions.
The online M.Eng. in cybersecurity policy and compliance allows students to study cybersecurity from a variety of organizational perspectives, with a keen foothold in engineering. Students gain a comprehensive knowledge of the policies that precede actionable cyber intelligence plans, preparing them to gain entry into roles with the government, corporations, and private businesses.

While many cybersecurity programs present material that is primarily focused on technical knowledge or inform solely on policy without the latter, this program’s coursework looks at policy through the lenses of engineering and computer science. Succinctly, the M.Eng. (CPC) is centered on the broader policies and standards that enable an organization to operate efficiently without sacrificing its private information. People from diverse backgrounds may be interested in the program: IT workers, recent graduates, engineers, project management professionals and software developers, among others.

Throughout the program, students will learn critical issues and topics that relate to a career in cybersecurity, including:

- Enterprise-specific strategies and policies
- Situational awareness procedure design
- Risk management
- Mobility solution development
- Forensic analysis and predictive analytics

Upon completion of the program, students will also be prepared to take the IA Baseline certification to solidify their competency in information assurance for governmental agencies.
CURRICULUM

The online master’s degree in cybersecurity policy and compliance at GW was created to adapt to the schedules of working students.

All live lectures are recorded. While students are encouraged to attend and participate, they can be viewed at a later time if needed.

Other coursework can be completed as it suits a student’s schedule, minding required assignment deadlines. Students who work will be able to apply many of the skills and practices learned within the program immediately on the job.

Required Courses

CSCI 6012 Cybersecurity and Privacy (3 credits)
Overview of cybersecurity and privacy, including cryptography, authentication, malware, viruses, network security, anonymity, privacy and online privacy, risk management. Common cyberattacks and techniques for detection and defense. Policy and legal perspectives for managing cybersecurity missions supporting private sector and government. Cyber technologies as applied to the stability of global information and communications infrastructure; government cybersecurity policies.

CSCI 6322 Information Policy (3 credits)
Roles, issues, and impacts of computer-based information systems in national and international arenas, focusing on privacy, equity, freedom of speech, intellectual property, and access to personal and governmental information. Professional responsibilities, ethics, and common and best practices in information use.

CSCI 6532 Information Security in Government (3 credits)
Information assurance policies and standards in the federal government as mandated by legislation; security processes following NIST standards; technical tests and validation methods used in the federal government; review of federal threats and vulnerabilities; and government positions in information assurance.

ECE 6132 Secure Cloud Computing (3 credits)
Security and privacy issues in cloud computing systems. Confidentiality, integrity, and availability of data and computations. Examination of cloud computing models, threat models, outsourcing, and security issues. Practical applications of secure cloud computing.

ECE 6542 Cybersecurity Risk Management and Compliance (3 credits)
Cybersecurity threats and other risks to an organization’s core business relative to people, processes, data, facilities, technology. Risk-based planning and risk management of cybersecurity at the enterprise level. Creating risk assessment and modeling approaches to cybersecurity issues that enable an enterprise to build security structures, sustain healthy cybersecurity posture, satisfy compliance with risk frameworks such as NIST’s. Prerequisite: EMSE 6540.

EMSE 6540 Management of Information and Systems Security (3 credits)
Development and management of effective security systems. Includes information, personnel, and physical security. Emphasis on risk analysis for information protection.

EMSE 6543 Managing the Protection of Information Assets and Systems (3 credits)
Advanced topics in protection of information assets and systems, including authentication, asset control, security models and kernels, physical security, personnel security, operational security, administrative security, security configuration management, and resource control. Prerequisite: EMSE 6540.

EMSE 6544 Auditing, Monitoring, and Intrusion Detection for Information Security Managers (3 credits)
Methods for detecting problems with unauthorized activity in information systems and management challenges associated with those activities. Prerequisite: EMSE 6540.

EMSE 6545 Cybercrime for Information Security Managers (3 credits)
Legal issues regarding information security actions related to and in response to criminal activity, including industrial espionage, back-hacking, cracking, and cyberterrorism. Transnational issues, cybercrime treaties and conventions, and cyberwar issues. Prerequisite: EMSE 6545.
Ideal candidates for the programs will meet the following requirements:

- Accredited bachelor’s degree from an accredited institution
- Minimum grade point average of B (3.0 on a 4.0 scale) or higher in upper level coursework.
- Work experience in an IT field for those who do not hold a degree in a technical discipline

Note: GW considers a candidate’s entire background and all submitted materials when reaching an admission decision. Applicants who do not meet these requirements may still be eligible for admission and their records will be evaluated on a case-by-case basis. Please contact an Admissions Counselor for more information.

Admissions Materials

To apply, please submit the following materials:

- **Completed Application**

- **Official Transcripts**: Transcripts are required from all institutions whether or not a degree was earned. Official transcripts are required to complete a student file. More information on transcript requirements can be found on our website’s transcript policy page. Official transcripts can be sent directly from the institution to our office via email at applyoffcampus@gwu.edu or in a sealed envelope via mail at:

  **EMSE Online Programs**
  Attn: Michelle Harris
  1 Old Oyster Point Rd, Ste 220
  Newport News, VA 23602

- **Statement of Purpose**: In an essay of 250 words or less, describe how the Cybersecurity Policy and Compliance program fits into your professional life and career objectives.

- **Letters of Recommendation**: Three letters of recommendation are required for admission and at least one letter must come from a professional reference. Please download the letter of recommendation form, fill out the top portion, and email the form to the individual providing the recommendation. A letter of recommendation is considered official only when it is sent directly from the individual providing the recommendation to an Admissions Counselor via email at onlinecybersec@gwu.edu or via fax at 888-245-5409. Submissions sent directly from applicants are not accepted.

- **Current Resume or C.V.** This can be submitted to onlinecybersec@gwu.edu.

- **GRE and GMAT scores are not required** to complete the application packet, but can be submitted to strengthen the application.

- **International Applications**: If academic records are in a language other than English, a copy in the original language and an English language translation must be submitted. Transcript evaluations need not be sent.

Note: There is no application fee for this program.
TUITION

At GW, providing world-class programs at an affordable tuition rate is one of our fundamental goals. Required textbooks and software are included in the price of tuition, which is among the most competitively priced in the nation. This allows students to pursue a top-tier education and expand their career possibilities online, on their own schedule, confident that they are making a smart investment in their future.

Tuition per credit hour: $995
Total tuition (minimum 30 credits): $29,850
Registration fee (per semester): $35

Financial Aid

As a GW student, you have several types of financial assistance programs available to you. The Office of Student Financial Assistance administers financial aid to graduate students. They will assist in the administration/certification of education loans to help meet the program's tuition cost. The FAFSA code for GW is 001444.

Contact Information

Phone: (202) 994-6620
Fax: (202) 994-0906
Email: finaid@gwu.edu

Prospective students can also contact an Admissions Counselor at (877) 246-4824 for more information about financial aid.
The George Washington University was founded in 1821 to honor its namesake. Since then, it has become the largest university in the D.C. metropolitan area, deeply interwoven with the culture and industries of the city. GW offers its students access to opportunities in many different fields with the unquestionable confidence that comes from having graduated from a respected, reputable institution of higher learning.

We strive to offer online students direct access to the world-class faculty, pioneering research, and spirit of exploration that defines GW as a leading institution. Beyond that, we’re committed to supporting online students as they pursue their education and welcoming them to the GW academic community.

Contact an Admissions Counselor today to begin your journey to cybersecurity expertise.

Email: onlinecybersec@gwu.edu
Phone: (877) 246-4824