



CYBERSECURITY POLICY & PRACTICE

RESIDENT: P170370
MOBILE: P309370

ELIGIBLE FUNDING: IMET, FMF/FMS
CERTIFICATION: PME

This course explores policies and practices that can be adapted to maintain an advantage over actors who seek to exploit, disrupt, or damage the networks and systems our societies and militaries depend upon. Instructors highlight the importance of effective cybersecurity for economic growth and innovation, examine barriers to effective policy and practice development, and consider methods for response that represent a comprehensive approach for cybersecurity.

OBJECTIVES

As an outcome of this offering, participants will be able to:

- ◆ Effectively analyze, design, and implement policies and practices for safeguarding unfettered access to cyberspace
- ◆ Be conversant in policy aspects for a global domain, including cyber deterrence and international regimes
- ◆ Understand cyber analogies, threat intelligence, and cyber conflict considerations
- ◆ Undertake challenges related to cyber-related legal issues
- ◆ Enhance partner capabilities, such as security management plans, defensive measures, and cyber
- ◆ Employ vulnerability assessment tools security frameworks

TOPICS

The delivery format combines informational presentations on academic theory and practical frameworks with a notional cyber security posture and capability assessment of awareness and capacity to counter cyber threats in scenarios based on actual attacks.

Sample topics include:

- ◆ Cyber attack trends, vectors, vulnerabilities and risks
- ◆ Cyber conflict elements, laws, and regime
- ◆ Security plans, frameworks, and controls
- ◆ Network architectures and technical methods
- ◆ Data analytics and emerging innovations
- ◆ Commercial sector, civil agency, and military department cooperation mechanisms

PARTICIPANTS

The seminar is designed for senior international officials from ministries of defense, foreign affairs, and communications. Public and private sector representatives responsible for cybersecurity are welcome to attend.



FACULTY

ISG employs a diverse faculty with strong professional, academic, military, and government backgrounds. This faculty core is augmented by other government experts (both civilian and military) and subject matter experts (SMEs) drawn from universities, think tanks, international organizations, and industry.

ENROLLMENT

Courses are conducted for partner countries as part of the United States government's security assistance and security cooperation efforts. As such, participation in ISG courses is managed through the security cooperation office of the US Embassies in partner countries. Interested, non-US persons should contact the international cooperation section of their own government or the relevant US Embassy for selection processes and enrollment. ISG reserves limited space in courses for US citizens. Interested US citizens may contact ISG to discuss availability.

FUNDING

ISG can accept most types of US government funding. Courses are typically funded by IMET, FMF, FMS, CTIWFP, PKO, and other DoD-wide O&M funds (333, MSI, etc) on a case-by case basis. Cost estimates can be obtained by contacting ISG.

ABOUT ISG

The Institute for Security Governance (ISG) is a global security cooperation organization established to build partner capability and grow the field and practice of institutional capacity building (ICB). Located in Monterey, California, ISG serves as the Defense Security Cooperation Agency (DSCA)'s primary resource for ICB integration and implementation, project scoping and design, and education and advising expertise.

This course is a key component of ISG's 25-year-long effort to provide military and civilian officials with unique education and professional development programs. Designed to cultivate individual understanding of complex issues and foster peer-to-peer learning, this custom-tailored course offering brings theoretical and applied learning practices into a exciting and rich classroom environment.