PRACTICAL CYBER IMPLEMENTATION

RESIDENT: P170042   **MOBILE: P309370**   **CERTIFICATION: PME, RDFP**

This course explores policies and practices necessary to protect and defend data, networks, systems, and platforms essential for military and security organizations and that underpin economic, social, governmental, and political activity in society. Instructors highlight the importance of civilian control throughout the cyber and Ministry of Defense (MoD) staff directorates, effective cybersecurity as a national security imperative, and introduce participants to cyber mission assurance, explore barriers to effective policy and practical implementation, and consider the latest practices and innovations for building cyber resilience. Military Articles and Services List (MASL) P170370 is used when this resident course is scheduled in Monterey.

OBJECTIVES

Upon conclusion of this course, participants will be able to:

♦ Develop the policy and best practices plans and frameworks necessary to turn approved cyber strategies and national law into accountable capabilities.
♦ Use frameworks/best practices, develop processes for cyber planning lines of effort for national security missions.
♦ Identify international, national, contractual, statutory, and regulatory influencers in MoD/Armed Forces Cyber.
♦ Develop guidance including metrics, procedures and guidelines for operations, international/interagency efforts for stakeholders.
♦ Create implementation plans/supporting guidance addressing MoD/Armed Forces requirements.
♦ Understand the impacts of systems design and equipment on the practices and policies/regulations/legislation used for the cyber defense enterprise.

TOPICS

The educational approach of this course combines content with practical exercises/case studies to provide the skills and knowledge needed to understand the process of cyber implementation. Course topics may include:

♦ (GOVERNANCE) Identify means that turn Strategy to implemented capabilities and the governance practices necessary for accountable implementation
♦ (INPUTS) Identify decision makers, influencers, and relationships involved in shaping cyber defense planning
♦ (INTENT) Develop Cyber Defense Planning and Foundational Lines of Effort

♦ (CONTROLS & SOLUTIONS) Decide Foundational Cybersecurity for Mission Assurance Practices
♦ (IMPLEMENTATION) Establish Implementation Guidance
♦ (ACCOUNTABILITY) Establish controls, metrics, and baselines to execute cyber strategy and guidance

PARTICIPANTS

The course is designed for cyber defense implementation work by civilians, military officers (equivalents O-3 to general-level), government/civilian/private sectors, and technical/non-technical specialists. Cyberspace Policy/Practice Development staff; Intelligence Researchers/Operatives, Cyber Strategist/Practitioners, Budget, Human Resources, and other defense planning staff should attend.

INSTITUTE FOR SECURITY GOVERNANCE (ISG) EDUCATION PORTFOLIOS

ISG's tailored education and professional development courses help build a comprehensive knowledge base and strengthen partner capacities to confront complex security and defense challenges. Courses are designed to cultivate individual understanding of complex issues; foster peer-to-peer learning; and build international communities of practice.

- **SECURITY GOVERNANCE & CIVIL-MILITARY RELATIONS (SG/CMR)**
- **CYBER CAPABILITY (CYBER)**
- **EMERGENCY MANAGEMENT & RESILIENCE (EM&R)**
- **INT'L DEFENSE ACQUISITION RESOURCE MANAGEMENT (IDARM)**
- **LOGISTICS CAPABILITY BUILDING (LCB)**
- **MARITIME SECURITY (MARSEC)**
- **PEACEKEEPING, CONFLICT, & TERRORISM (PCT)**

FACULTY

ISG's faculty team is grounded in professional experience from academic, military, government, and civil sectors. The core faculty are augmented by experts drawn from other parts of government, and U.S. and international subject matter experts drawn from universities, industry, think tanks, international organizations, and non-governmental organizations.

ENROLLMENT

Courses are conducted as part of the U.S. Government's Security Cooperation efforts. Interested partner nation personnel should contact their government's international cooperation section, or the relevant U.S. Embassy's Security Cooperation organization for selection processes and enrollment. Interested U.S. citizens may contact ISG to discuss availability.

FUNDING

Educational programs are primarily implemented through Title 22 authorized programs, including International Military Education and Training (IMET), Foreign Military Sales (FMS), Peacekeeping Operations (PKO), and various Title 10 authorized programs, including the Maritime Security Initiative (MSI) and Regional Defense Fellowship Program (RDFP).

ABOUT ISG

The Defense Security Cooperation University's (DSCU) Institute for Security Governance (ISG) is the Department of Defense's leading implementer for Institutional Capacity Building (ICB) and one of its primary international schoolhouses. As a component of the Defense Security Cooperation Agency (DSCA), ISG is charged with building partner institutional capacity and capability through tailored advising, education, and professional development programs grounded in American values and approaches.