COURSE AND TRAINING OFFERINGS

This document provides an outline of the online courses available through the International Association of Maritime Security Professionals (IAMSP) learning platform.

2017-2019 Year

This document is published under the authority of the Executive upon the recommendation of the Chief Learning Officer as part of the Association's support towards its membership.

A McDougall PCIP CMAS CISSP CPP PSP
Chief Learning Officer IAMSP
certification@iamsponline.org

PART 1 - ADMINISTRATION

PART II - LIST OF COURSES

Part 1 - Administration

Introduction

1. The International Association of Maritime Security Professionals (IAMSP) is a volunteer-led association of professionals / non-governmental organization (NGO) seeking to advance the professionalization of maritime security. The Association web presence can be found at www.iamsponline.org and includes the Association's core documentation.

2. Part of the IAMSP core activities involves the provision of education, training and familiarization products on a wide range of subjects that directly impact maritime security.

Goal of the Online Learning Program

3. The goal of the online learning program is to provide a web-supported avenue to deliver education, training and familiarization products on an on-demand, global level.

4. The following are the core desirable characteristics of the platform:
   4.1. Available on demand to those seeking education, training and familiarization products
   4.2. Leverages network technology to provide an enhanced learning experience for those involved
   4.3. Provides low-bandwidth solutions for those operating in remote areas or in isolation
   4.4. Provides a communication channel to those participating on courses
   4.5. Maintains accurate records of training
   4.6. Accomplishes the above for reasonable cost

5. The learning program is part of the revenue generation process. The structure of any fees is to ensure that there is a clear return on investment for members.

Education, Training, and Familiarization

6. The IAMSP operates three levels of instruction:
   6.1. Educational offerings focus on developing an understanding of the concepts underlying issues;
   6.2. Training offerings focus on the specific steps to be taken in performing tasks; and
   6.3. Familiarization offerings focus on informing individuals so that they are aware of certain issues.

7. IAMSP also offers several courses that are confirmed through various kinds of testing:
   7.1. **Performance-based** testing: for situations where the candidate must demonstrate that he or she can undertake a task or activity that requires both a knowledge of the processes to be followed and an understanding of the knowledge base to be applied. This is confirmed using an assignment that mirrors a real-world application.
   7.2. **Confirmation-based** testing: for situations where the candidate must demonstrate that he or she possesses a knowledge of a certain domain or body of knowledge. In this case, the testing is conducted through questions derived from the presented information and for which the

candidate must provide a correct response. This testing is generally done through the online testing tools to support a consistent and rigorous confirmation process.

7.3. **Reinforcement-based** testing that asks questions that remind the candidate of knowledge or information presented in the material.

Management Structure

8. The IAMSP uses a management structure based on ISO 17024:2003 *General Requirements for Bodies Operating the Certification of Persons* in the development of its course material. This is described in documents available through the IAMSP website.
9. The Chief Learning Officer (CLO) acts as the focal point for the technical knowledge base for the IAMSP.
10. The President acts as the senior officer for appeals and challenges associated with any issues of fairness.
11. Changes to the knowledge base or decisions regarding the delivery of services are put forward by the CLO to the Executive for ratification.

Issuance of Certificates and Electronic Badges

12. The issuance of a credential requires a recommendation from the CLO (indicating that all requirements are met) and ratification by the executive at the monthly meeting (to ensure all quality checks are performed and in its exercising of oversight over the activity).
13. The requirement to pass each course must be clearly indicated so that an individual understands what is needed to be achieved to pass.
14. Once the Executive has ratified the checks and balances, the individual may be issued both a certificate and digital badge clearly reflecting the level and nature of achievement.
15. Certificates and badges are provided in electronic form to the candidate with a copy retained by the Association.

Course Offerings

16. The IAMSP syllabus will be updated October of the year prior to the applicable year (for example, the updated syllabus for the 2018 calendar year will be available October 2017).
17. While most courses are on demand, the IAMSP reserves the right to modify any activity within the course for efficiency and scheduling around operations.

Grading

18. The grading process ensures that no one person determines the grade of an individual without a check and balance:

18.1. For performance-based assignments, the results are reviewed by the board independently (blind review) when they meet at the monthly meeting; and

18.2. For certification-based testing, the Learning Management System (LMS) test generating capabilities are utilized to ensure that testing is fair and impartial. The IAMSP has taken steps to separate the testing questions from the review questions to ensure that each candidate has the same opportunity.

Supporting Activities

19. The structure of these courses is intended to leverage network technology to the benefit of the candidate, including (on a course-by-course basis) the use of:
    - 19.1. WebEx meetings to discuss key points
    - 19.2. Forums to post discussion information
    - 19.3. Communications channels through which updates can be communicated to candidates.
20. Candidates are enrolled for a period of one year when completing the course. This is to ensure that the candidate not only has time to process the information but also has access to a capable community and instructors during the critical period of attempting to apply the knowledge and skills in new domains. Those
    - 20.1. Non-members wishing to remain a part of the community after the course may do so for the cost of a modest maintenance fee
    - 20.2. Members of the association who are in good standing are not required to pay a renewal fee as it is included in their annual membership dues.

Continuous Improvement

21. The IAMSP places significant value on continuous improvement. Each offering is subject to its own continuous improvement cycle and encourages feedback from participants to support this.

Appeals and Appeal Process

22. The IAMSP prohibits discrimination based on the elements associated with the United Nations Universal Declaration of Human Rights and takes steps to ensure that all results are solely based upon the accomplishments against course standards and requirements.
23. Where there is a question of a technical nature, the issue is to be referred to the CLO who may, based upon accepted doctrine, assess the situation and make changes as necessary.
24. Where there is a question of fairness, the issue is referred to the President who may, based upon his or her or their own fact finding, recommend a result (supporting, modifying or overturning the original result) to the Executive for ratification.

Part II - List of Courses

Name	Certified Maritime Security Professional	Code	CMSP
Pre-requisites	Element 1: CMSP SPM 100 Element 2: CMSP PHY 100 Element 3: CMSP ITS 100 Element 4: CMSP MDA 100 Element 5: CMSP ETH 100	Testing	3 x 70% computer based 1 x assignment Values / Ethics package
Element of	Formal certification	Estimated Effort	80 hours to 100 hours (not including readings)
Subject	Certified Maritime Security Professional (CMSP)		
Description	This is the formal IAMSP certification for those seeking IAMSP endorsement of their knowledge within the Asset Protection and Security domains (maritime). The certification consists of the five following elements: • Security Management (CMSP SPM 100) • Physical Security (CMSP PHY 100) • Information Systems Security (CMSP ITS 100) • Applying Security in the Marine Domain (CMSP MDA 100) • Values and Ethics (Legal, Human Rights, Use of Force) (CMSP ETH 100) This is a significant undertaking appropriate for those that are seeking to clearly distinguish themselves as having a broad base of credible knowledge. Those undertaking this considerable effort will face intermediate to advanced level courses for the first three elements. These provide a knowledge base that has been widely accepted within the professional security community. The testing for each of these involves computer-based testing. Following those three elements, the doctrines are brought more into the maritime context. The values and ethics element provides the professional conduct element of the certification, as is consistent with most professional bodies. The confirmation process for Element 4 is performance based meaning that an individual must describe and support a course of action given specific circumstances and their own national requirements. This structure also allows those completing it to realize efficiencies in their preparation for other certifications.		
Cost	$795 for the full five courses (see the IAMSP Certification Program document)		

Name	CPP Preparation	Code	CMSP SPC 100
Pre-requisites	None	Testing	70% average across all attempts Computer-based
Element of	Element 1 (Certified Maritime Security Professional)	Estimated Effort	20 hours (not including readings)
Subject	Certified Protection Professional (CPP) Preparation / Security Management		
Description	This course is intended to assist members in preparing for the ASIS International Certified Protection Professional (CPP) course, a security management certification recognized worldwide. The IAMSP accepts this body of knowledge as meeting the Security Management (Element 1) of the CMPS when combined with the Marine Domain Awareness Course. The core domains (bodies of knowledge) are the following: • Investigations • Security Principles • Business Principles and Practices • Personnel Security Screening • Business Principles • Physical Security • Crisis Management • Information Management • Legal Elements This course is considered an intermediate to advanced level course that will involve an exposure to a level of conceptual structures, technical details and memorization. For those intending to write the CPP examination, the study package should be purchased through the ASIS International bookstore at www.asisonline.org. Please note that the CPP certification operates independently of IAMSP and has its own eligibility criteria to be met.		
Cost	$300 (US) individually Included within the CMSP overall fee		

Name	PSP Preparation	Code	CMSP PHY 100
Pre-requisites	None	Testing	70% average across all attempts Computer-based
Element of	Element 2 (Certified Maritime Security Professional)	Estimated Effort	20 hours (not including readings)
Subject	Physical Security Professional (PSP) Preparation / Element 2 CMSP		
Description	This course is intended to assist members in preparing for the ASIS International Physical Security Professional course, a physical security certification recognized worldwide. The IAMSP accepts this body of knowledge as meeting the physical security (Element 2) of the CMPS when combined with the Marine Domain Awareness Course. The core domains (bodies of knowledge) are the following: • Concepts in Security Management • Concepts of Physical Security and Physical Protection Systems • Lifecycle and Project management • Planning, Designing and Estimating • Security Controls (preventive, detection, response) • Crime Prevention Through Environmental Design • Electronic Security Systems This course is considered an intermediate to advanced level course that will involve an exposure to a level of conceptual structures, technical details and memorization. For those intending to write the PSP examination, the study package should be purchased through the ASIS International bookstore at www.asisonline.org. Please note that the PSP certification operates independently of IAMSP and has its own eligibility criteria to be met.		
Cost	$300 (US) individually Included within the CMSP overall fee		

Name	CISSP Preparation	Code	CMSP ITS 100
Pre-requisites	None	Testing	70% average across all attempts Computer-based
Element of	Element 3 (Certified Maritime Security Professional)	Estimated Effort	40 hours (not including readings)
Subject	Computer and Information Systems Security Professional (CISSP) Preparation / Element 3 CMSP		
Description	This course is intended to assist members in preparing for the (ISC)2 Computer and Information System Security Professional course, an information systems security certification recognized worldwide. The IAMSP accepts this body of knowledge as meeting the information systems (Element 3) of the CMPS when combined with the Marine Domain Awareness Course. The core domains (bodies of knowledge) are the following: • Security and Risk Management • Asset Security • Security Engineering • Communications and Network Security • Identity and Access Management • Security Assessment and Testing • Security Operations • Software Development Security This course is considered an advanced course and those undertaking can expect to encounter technical details. For those intending to write the CISSP examination, the study package should be purchased through the (ISC)2 bookstore at www.isc2.org bookstore Please note that the CISSP certification operates independently of IAMSP and has its own eligibility criteria to be met.		
Cost	$400 (US) individually Included within the CMSP overall fee		

Name	Marine Domain Applications	Code	CMSP MDA 100
Pre-requisites	CMSP SPM 100 CMSP PHY 100 CMSP ITS 100	Testing	Pass based on performance-based board review (blind)
Element of	Element 4 (Certified Maritime Security Professional)	Estimated Effort	20 hours (not including readings)
Subject	Application of Security within the Marine Environment / Element 4 CMSP		
Description	This course builds upon the first three elements, focussing on issues arising in the application of the security doctrine within specific marine environments. The course structure draws heavily upon the requirements outlined in the IMO model courses (IMO 3.19 through IMO 3.21 and IMO 3.23) and the International Ship and Port Facility Security (ISPS) Code. The following modules are currently put forward: • Historical elements • Marine Operations • Marine Security Policy (including Conventions and Laws) • Security Sensitive Information (SSI) • Roles and Responsibilities • Security Assessments • Security Plans This course also provides a significant number of links to resources to assist those in the domain with remaining current with guidance from the IMO and through other Conventions. This course is intermediate to advanced in content but has an expectation of advanced-level performance in the final assignment.		
Cost	$250 (US) individually Included within the CMSP overall fee		

Name	Values and Ethics	Code	CMSP ETH 100
Pre-requisites	None	Testing	70% (individual quizzes)
Element of	Element 5 (Certified Maritime Security Professional)	Estimated Effort	20 hours (not including readings)
Subject	Values and Ethics / Element 5 CMSP		
Description	This course provides the foundation for professional conduct within the IAMSP and is based upon four main modules: • The Duty of Care • Human rights • Legal elements • Use of Force Each of these courses has undergone both a critical review and has been reviewed by competent legal practitioners in the domain (they are not intended as legal advice).		
Cost	$250 (US) individually for non-members No charge for members of the IAMSP in good standing Included within the CMSP overall fee		

Name	Specialist in Performance-Based Systems	Code	SPBS
Pre-requisites	None	Testing	Scenario-based assignment
Element of	Formal Certification	Estimated Effort	30 hrs to 40 hrs
Subject	Specialist in Performance-Based Systems		
Description	**The Specialist Performance-Based Systems builds upon the knowledge of the various preparation courses and focuses on building the skills necessary to respond to requirements stemming from performance-based regulatory structures.** **The certification consists of three elements:** • **Risk Assessment Officer (SPBSRAO100)** • **Plan Development Officer (SPBSPDO100)** • **Compliance and Assessment Officer (SPBSCAO100)** **At the end of the three modules, those successfully completing it will be familiar with how to work from regulatory requirements and then build an evolving and measurable Physical Protection System.** **The testing for this certification is a running assignment that has individuals completing an assignment based on an operational profile and summary of threats. Once past the risk assessment, the output from that module is used as the foundation for the development of a Physical Protection System. Once that module is complete, the final step is the development of a concise compliance and assessment plan that monitors the performance of the various controls and links back to the risk assessment module.** **This course is an intermediate course that builds upon a significant body of knowledge. The assignment is expected to be at the advanced level and to a level of detail commensurate with real-world scenarios.**		
Cost	**The cost of the three modules is $500 (US)**		

Name	Risk Assessment Officer	Code	SPBSRAO100
Pre-requisites	None Assumes a level of security knowledge	Testing	Scenario-based assignment
Element of	Element 1 of the SPBS	Estimated Effort	10 hrs
Subject	Risk Assessment Officer		
Description	The Transportation System Risk Assessment Officer provides guidance with respect to the conduct of risk assessments in support of the development of Physical Protection Systems for performance-based regulatory regimes. The course consists fo four module: • An overview of the risk assessment process • Threat Assessment • Asset Valuation • Vulnerability Assessment This module is an intermediate to advanced level module. It assumes a level of security knowledge and requires the support of supplemental readings. Those attempting this course are also given higher access to instructors in terms of support. At the end of this module, individuals will be required to submit an assignment based on an operational profile and threat assessment.		
Cost	The cost of this module is $200 (US) The cost of this module is covered in the costs for the SPBS		

Name	Plan Development Officer	Code	SPBSPDO100
Pre-requisites	SPBSRAO100	Testing	Scenario-based assignment
Element of	Element 2 of the SPBS	Estimated Effort	15 hrs
Subject	Plan Development Officer		
Description	The Transportation System Plan Development Officer builds on the work completed in the Risk Assessment Officer course and links the risk assessment process to the design of the Physical Protection System. This module examines: • Generating goals based on requirements and risk • Focussing the controls • Developing sound systems of controls • Documenting controls This module is an intermediate to advanced level module. It is expected that those undertaking this module will be in contact with the IAMSP CLO as they work through the modules. Those completing the module will use the risk assessment from the SPBSRAO100 module to develop a performance-based Physical Protection System. As part of this exercise, candidates will be required to provide a copy (or link) to their home nation's regulations which will be used as part of the assignment.		
Cost	The cost of this module is $200 (US) The cost of this module is covered in the costs for the SPBS		

Name	Compliance and Assessment	Code	SPBSCAO100
Pre-requisites	SPBSRAO100 SPBSPDO100	Testing	Scenario-based assignment
Element of	Element 3 of the SPBS	Estimated Effort	15 hrs
Subject	Establishment of monitoring regimes to ensure compliance and performance.		
Description	The Transportation System Compliance Assessment Officer builds on the work completed in the Risk Assessment Officer and Plan Development Officer courses and links the two previous modules to the activities necessary for monitoring and compliance. This module examines: • Describing the differences between compliance and performance-based systems • Notes on the conduct of inspections • Notes on the conduct of assessments • Notes on the conduct of audits This module is an intermediate to advanced level module. It is expected that those undertaking this module will be in contact with the IAMSP CLO as they work through the modules. Those completing the module will use the risk assessment from the SPBSRAO100 module and the physical protection system developed in SPBSPDO100 in the development of the compliance and assessment activities.		
Cost	The cost of this module is $200 (US) The cost of this module is covered in the costs for the SPBS		

Name	IT / Information Security Primer	Code	ITSECAWR
Pre-requisites	None	Testing	Computer based testing
Element of	Awareness Suite	Estimated Effort	3 hours
Subject	IT Security Awareness for Non-Technical Personnel		
Description	**The maritime industry is becoming increasing connected and network-enabled. Consequently, IT Security has been gaining importance for those at sea or on shore.** **This collection of modules includes:** • **IT Security Awareness (Basic) focussing on non-technical elements (ITSECAWR001)** • **IT Security Awareness (Technical) at an intermediate technical level (ITSECAWR002)** • **Awareness of Security Sensitive Information focussing on security-related information handling (ITSECAWR003)** **Two modules (ITSECAWR001 and ITSECAWR003) are considered introductory in nature while technical awareness provides a primer for those that may be involved in more involved with technical issues.**		
Cost	**The cost of this module is $200 (US)** **Arrangements for corporate registrations can be made**		
Note	**For organizations seeking to integrate material into a more comprehensive IT Security program / Information Security program, consideration can be given to combining the IT / Information Security Primer with the CISSP preparation course. Contact us for details.**		

Name	IT Security Awareness (Basic)	Code	ITSECAWR001
Pre-requisites	None	Testing	Computer based testing
Element of	Awareness Suite	Estimated Effort	1 hour
Subject	IT Security Awareness for Non-Technical Personnel		
Description	The maritime industry is becoming increasing connected and network-enabled. Consequently, IT Security has been gaining importance for those at sea or on shore. This awareness module covers elements such as: • Common threats • Common vulnerabilities • Steps that can be taken to improve security This presentation provides awareness for persons who are looking to improve their understanding of basic IT Security controls. This course is basic with some elements approaching the intermediate level but is considered suitable for persons with limited security knowledge.		
Cost	The cost of this module is $50 (US) Arrangements for corporate registrations can be made		

Name	IT Security Awareness (Technical)	Code	ITSECAWR001
Pre-requisites	None	Testing	Computer based testing
Element of	Awareness Suite	Estimated Effort	1 hour
Subject	IT Security Awareness (intermediate)		
Description	The maritime industry is becoming increasing connected and network-enabled. Consequently, IT Security has been gaining importance for those at sea or on shore. This module looks at IT Security from a more advanced level than the basic module, including: • Core challenges on land and at sea • Core threats and vulnerabilities based on the OSI model • Steps that can be taken at each layer of the OSI model • Further general steps and controls intended to improve security This presentation is intended for persons with a more technical background or who are more technically inclined. It has a significant focus on technical elements of the IT security domain and is supplemented by readings (optional).		
Cost	The cost of this module is $100 (US) Arrangements for corporate registrations can be made		

Name	Security Sensitive Information	Code	ITSECAWR003
Pre-requisites	None	Testing	None
Element of	Awareness Suite	Estimated Effort	1 hour
Subject	Identifying, Handling and Controlling Security Sensitive Information (SSI)		
Description	While many organizations are familiar with privacy requirements, government sensitive information or proprietary information, gaps continue to persist with respect to the handling of unclassified but sensitive security information. This module provides awareness with respect to the nature of Security Sensitive Information (SSI) including: • Defining SSI based on national and risk-based criteria • Linking SSI to physical attacks • Linking SSI to the stages of cyber attacks • The handling of SSI This module is introductory and suitable for non-technical personnel. This module also provides links to sources of doctrine for certain nations to provide further documentation on the handling of sensitive information.		
Cost	The cost of this module is $50 (US) Arrangements for corporate registrations can be made		

Name	Technical Briefs	Code	See below
Pre-requisites	None	Testing	None
Element of	Technical Materials	Estimated Effort	1 hour
Subject	Various technical controls		
Description	**Technical briefs are short presentations that include working tools intended to assist persons with focussed tasks. These tools are developed in response to questions received at the IAMSP or that have arisen in common discussions.** **Technical briefs generally include the following:** • **A presentation describing the challenge and response to that challenge** • **An unlocked version of the working tool associated with the challenge** • **Community-based support through forums** **Currently, technical briefs are included for the following:** • Return on Security Investment **(TECH01ROSI)** • Estimating Effectiveness of Layers of Defense **(TECH02LOD)** • Use of CARVER / MSHARPP for Estimating Exposure **(TECH03EXP)** **Working tools are available to be used for commercial purposes but are not to be resold without the written permission of the IAMSP after arrangements are made.**		
Cost	**The following costs apply:** • **Per technical brief – $50 US** • **2 technical briefs - $75 US ($37.50 each)** • **3 technical briefs - $100 US ($33.33 each)** • **For each technical brief after the third (more coming) add $25 US to the total cost.**		

Name	Supplements	Code	SUPP
Pre-requisites	None	Testing	None
Element of	Awareness Suite	Estimated Effort	1 hour
Subject	Supplementary information on specific topics or subjects		
Description	Supplements address a specific topic and provide refined detail and information regarding that topic. They are intended to be used as continuing education or training for those maintaining their credentials or those maintaining an effort towards continuous learning. Supplements are produced periodically on subjects that are either attached to the IAMSP research projects or questions. Currently, supplements available include: • Risk with Ship / Port Interactions (SUPPRSK010) Supplements generally count towards 2 continuing education units for certified members.		
Cost	Supplements costs are as follows: • One supplement - $50 US • Two supplements - $75 US • Three supplements $100 US Plans are in process to make the full suite available to organizations at a significantly reduced price.		

Part III – Other Modes / Supporting Modes

Name	Rail – Security Challenges	Code	RAILAWROPS
Pre-requisites	None	Testing	None
Element of	Awareness Suite	Estimated Effort	1 hour
Subject	This module is intended to prove an awareness of security challenges within the Rail Industry when interacting with maritime security		
Description	While 90% of the world's international trade moves by sea, the maritime industry is one mode within an interconnected system of modes. The rail industry is a significant factor in the movement of persons and goods overland and, as has been shown in many instances when services were disrupted in ports or in rail movement, a vital partner in moving goods to and from seaports. This module is intended to provide: • A broader awareness of security challenges in the rail industry • A broader understanding of approaches to meet those challenges • Several vetted links to help keep abreast of industry changes. This module is intended for those broadening their knowledge and is considered introductory in nature. It is intended for those maintaining their credentials through continuous learning		
Cost	The cost of this module is $50 (US) Arrangements for corporate registrations can be made		

Name	Rail – Security and Dangerous Goods Regulations	Code	RAILAWRTDG
Pre-requisites	None	Testing	Computer based
Element of	Awareness Suite	Estimated Effort	1 hour
Subject	Awareness material for incoming Canadian regulations regarding the security of dangerous goods being moved by rail.		
Description	The movement of dangerous goods by rail received significant attention in Canada and is currently being regulated through Transport Canada. This module is intended to provide Canadian and USA personnel with an awareness of these regulations and security doctrine that may be affected. Topics include: • A description of general risks and attack types • What is being done to address the issue and proposed requirements • Notes to assist in recognizing and responding to suspect conditions • Additional resources in the form of readings and reference material This module can be combined with the SPBS modules and preparation courses to prepare Rail Security Coordinators for this challenge.		
Cost	Module - $50 US when purchased in isolation ($5 per intended user for groups of ten or more) Module +SPBS: $500 with unlimited use of this module within your organization Module + SPBS + CPP or PSP Preparation: $600 with unlimited use of the module within your organization.		