SHIP OPERATIONS COOPERATIVE PROGRAM

Business ▪ Government ▪ Education ▪ Workforce

Catalyst for Change™

SOCP January GAM Webinar

2021 is Here...Is Your SMS Ready for Cybersecurity?

JANUARY 21, 2021 (12:00 – 12:30 PM ET)

Serving the Needs of the Maritime Industry through Collaboration & Innovation

Welcome & Webinar Guidelines

Jayson Toth– SOCP President

- Use headset with microphone if calling in with computer, or use your phone for audio
- Do not place phones “On Hold”
- “Mute” when not speaking to avoid background noise
- Clearly identify yourself when speaking
- Professional Comments in Chat
- Q&A Protocol

Time: 12:00 - 12:30 PM ET

Presenter: John Jorgensen

ABS, Chief Scientist for Cybersecurity and Software

Mr. Jorgensen is Chief Scientist for Cybersecurity and Software at American Bureau of Shipping, responsible for cybersecurity service development for marine and offshore customers, as well as for related data integrity and software integrity methods development. Mr. Jorgensen started his career as a Surface Warfare Officer in the US Navy. After working in ship systems acquisition at Naval Sea Systems Command, he retired from active duty and worked in the private sector in systems engineering, architectures, and complex systems. In 2013, Mr. Jorgensen moved to ABS and now devotes himself to the full integration of cybersecurity, data integrity, software assurance, and system tests in the cyber domains. Not only does Mr. Jorgensen serve as the SOCP's Vice President and Secretary, but he also writes the Cyber Guy column in the SOCP monthly newsletter.

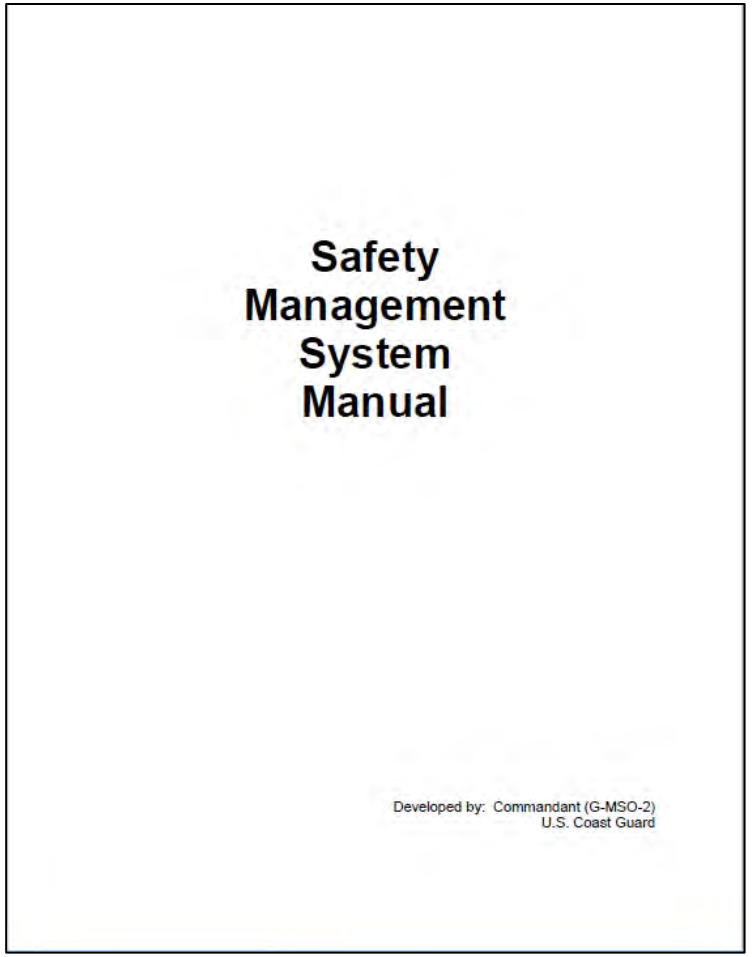
Time: 12:00 - 12:30 PM ET

Cybersecurity and IMO 2021

John Jorgensen | SOCP Gam
20 Jan 2021

ISM Layout for SMS

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review



USCG SMS Manual, 2014

Used for illustrative purposes only

IMO Requirements: Cyber Integration

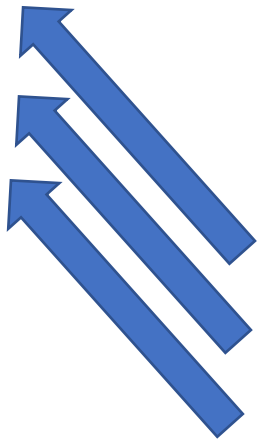
Preparatory actions

- Inventory connected systems
- Inventory software
- Check personnel jobs and roles for correct accesses
- Determine where connections exist
- Develop policies for bringing cybersecurity into the physical and safety world

MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 1	IDENTIFY PROTECT DETECT	Procedures are implemented for the training of personnel, ashore and onboard, to improve cyber awareness and skills to prepare for and respond to cyber threats, vulnerabilities and emergency situations. ► ISM Code 1.2.2.3, 1.4
Paragraph 2	ALL I-P-D-R-R	Company Safety and Environmental Policy is documented in the SMS. ► ISM Code 1.4.1
Paragraph 3	PROTECT	MSC-FAL.1/Circ.3 recommendations have been taken into account when assessing identified cyber risks to Company vessels, personnel, and the environment, and establishing appropriate safeguards instructions and procedures. ► ISM Code 1.4.2
Paragraph 4	RESPOND RECOVER	Procedures and personnel responsibilities are defined for: – Identifying, communicating, and responding to emergency situations – Recovering from cybersecurity events and incidents, and – Reporting and reviewing cybersecurity nonconformities, events, and incidents. ► ISM Code 1.4.3, 1.4.4, 1.4.5
Paragraph 5	IDENTIFY	Cybersecurity risks to ships, personnel, and the environment have been assessed. ► ISM Code 1.2.2.2
Paragraph 5/1 Paragraph 5/2	IDENTIFY PROTECT DETECT	Instructions and procedures take into account all identified cybersecurity risks and establish necessary safeguards to support the safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation. ► ISM Code 1.2.2.2, 1.2.3, 1.4.2, 1.4.3
Paragraph 5/3	IDENTIFY PROTECT	Procedures are implemented for identifying and protecting cyber-related IT and connected OT information systems considered essential for safe operation of vessels and protection of the crew and environment. ► ISM Code 1.2.2.1, 1.4

IMO Requirements Integration (1)

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review



MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 1	IDENTIFY PROTECT DETECT	Procedures are implemented for the training of personnel, ashore and onboard, to improve cyber awareness and skills to prepare for and respond to cyber threats, vulnerabilities and emergency situations. ► ISM Code 1.2.2.3, 1.4

Training for awareness and skills for operations and response

IMO Requirements Integration (2)

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review

MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 2	ALL I-P-D-R-R	Company Safety and Environmental Policy is documented in the SMS. ► ISM Code 1.4.1

Safety and Environmental Policy in the SMS

(PREP) Develop policies for bringing cybersecurity into the physical and safety world

IMO Requirements Integration (2)

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review

MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 3	PROTECT	MSC-FAL.1/Circ.3 recommendations have been taken into account when assessing identified cyber risks to Company vessels, personnel, and the environment, and establishing appropriate safeguards instructions and procedures. ► ISM Code 1.4.2

(PREP) Check personnel jobs and roles for correct accesses

(PREP) Determine where connections exist

Assess cyber risks using guidance of MSC-FAL/Circ.3

ABS

IMO Requirements Integration (3)

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review

MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 4	RESPOND RECOVER	Procedures and personnel responsibilities are defined for: – Identifying, communicating, and responding to emergency situations – Recovering from cybersecurity events and incidents, and – Reporting and reviewing cybersecurity nonconformities, events, and incidents. ► ISM Code 1.4.3, 1.4.4, 1.4.5

(PREP) Insert in Operating Procedures:

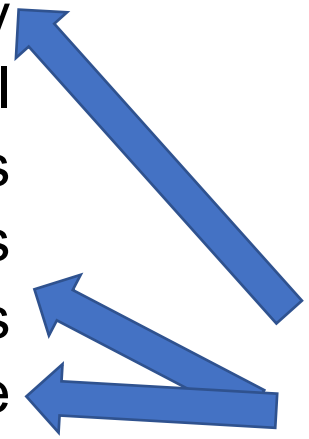
- Inventory connected systems
- Inventory software

Define procedures for casualty control, recovery, and reporting in case of cyber-related incidents

ABS

IMO Requirements Integration (4)

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review



MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 5	IDENTIFY	Cybersecurity risks to ships, personnel, and the environment have been assessed. ► ISM Code 1.2.2.2

Perform and record risk assessment for cyber-enabled systems

IMO Requirements Integration (5)

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review

MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 5/1 Paragraph 5/2	IDENTIFY PROTECT DETECT	Instructions and procedures take into account all identified cybersecurity risks and establish necessary safeguards to support the safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation. ► ISM Code 1.2.2.2, 1.2.3, 1.4.2, 1.4.3

Company procedures include cyber-related risks and safeguards that meet flag and international requirements

IMO Requirements Integration (7)

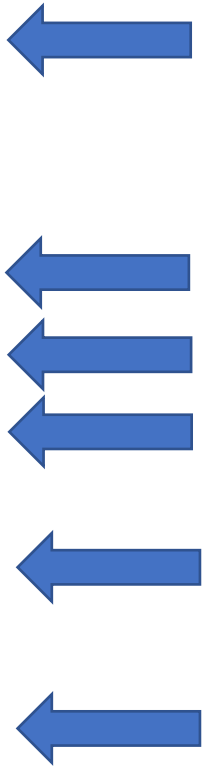
1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review

MSC.428 /98/Add. 1 Annex 10. Reference	NIST CSF Element	Requirement Statement
Paragraph 5/3	IDENTIFY PROTECT	Procedures are implemented for identifying and protecting cyber-related IT and connected OT information systems considered essential for safe operation of vessels and protection of the crew and environment. ► ISM Code 1.2.2.1, 1.4

IT and OT systems critical to ship and personnel safety are identified and protected

IMO Requirements Integration (8)

1- Introduction
2- Safety and Environmental Policy
3- Company Authority
4- Designated Person(s)
5- Master's Responsibility
6- Resources and Personnel
7- Vessel Operating Procedures
8- Emergency Preparedness
9- Reporting Procedures
10- Maintenance
11- Documentation
12- Company Verification and Review



Eighth Requirement:
Communicate

Iterate
- Roles and accesses
- Environment and safety policies inclusive of safety-relevant computerized systems
- Documentation
- Training
- Casualty control procedures

Summary

- What We Know:
  - Risk is the heart of cybersecurity
  - Governance considers risk
  - Policy determines processes and procedural requirements in governance
  - Processes and procedures control identity, access, and connections
  - Identity, access, and connections are components of policy
  - Training implements policy and processes
  - Change management meters systems implementation and processes, in accordance with training

Contact us:

John M. Jorgensen, CISSP-ISSAP
Chief Scientist, Cybersecurity & Software
American Bureau of Shipping
(281) 877-6675 (office)
(832) 707-6165 (mobile)
JohnJorgensen@eagle.org

Questions and Discussion

Answers to questions on following page

Q&A

Q. What role does management of change play in the process?

A. Management of change applies to systems and to people. For the systems, we inventory and document them, note any specifics for operational characteristics and casualty control, and we ensure that the documentation spawns appropriate training. For the people, it becomes an exercise in both communications and repetition. As the IMO points out in their final requirement on the MSC.428(98), they expect all stakeholders to be included in the processes. Crew, maintenance personnel, and operators are all stakeholders who must understand and operate new gear, new systems, and new processes.

A Safety Management System (SMS) is one of a ship's more important documents, and it will be under change management processes itself. But the SMS should always work for the crew as a tool and a reference, referring to the company's Management of Change program instructions and procedures, also.

Q&A

Q. How will makers providing no clear path to upgrade Class approved systems be encouraged to support their customers?

A. There are two answers here.

1. Class societies, including ABS, have defined procedures for performing a cyber type approval activity for cyber-enabled systems. Because the process is fairly new to industry, it's still in early stages.

2. Owners, operators, maintainers, and crews should always look carefully at operating documentation for ports, protocols, services, communications paths, communications methods and requirements, installation needs (shielding, shelters for electronics, etc.), software or firmware versions, and vulnerabilities of the system or its software. Working with OEMs, owners and operators can help OEMs provide gear to ships and crews that helps the crews keep their systems safe, secure, and reliable.

Q&A

Q. Do you have any insight and requirements on sail-training vessels for Maritime Academies?

A. Sailing vessels with few – or no – operationally critical automation systems will only need to include electronic or cyber-enabled systems in the functions for which installed. The three basic factors – including cybersecurity considerations in the SMS, connecting critical systems to risk assessment, and training people on critical cyber-enabled systems for casualty control and response – might only require a couple of paragraphs, or a couple of pages, if the sailing vessel's systems are standalone, or not critical to operations. The IMO purposefully left the thoroughness of coverage as a judgment item for SMS holders.

Q&A

Q. When we start looking at the PLC & Sensor levels, aren't we duplicating what is already covered in a Company's maintenance management system?

A. The SMS should have enough detail to point effectively at the maintenance management systems, but it should be sufficient also so that the SMS stands alone. A company might collocate the SMS with the maintenance program, for easy reference, or simply include enough documentation and detail in the SMS to enable the training and familiarization, but with a link or a pointer to the detailed information elsewhere. The SMS is the crew's and owner's tool for operational use. Its organization and 'look' are what work for YOU.

References for IMO 2021 Requirements

- International Maritime Organization (IMO) Maritime Safety Committee (MSC) 96 WP.9, “Measures to Enhance Maritime Security,” 17 May 2016.
- IMO Resolution MSC.428(98), “Maritime Cyber Risk Management in Safety Management Systems,” adopted 17 June 2017.
- IMO MSC-FAL.1/Circ.3, “Guidelines on Maritime Cyber Risk Management,” 5 July 2017.
- U.S. Coast Guard, Safety Management System Manual, 2014.
- American Bureau of Shipping, *ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries – 2021.*
- ABS Group, *A Primer on IMO Cyber Risk Management Guidelines, What to Know and How to Comply,*” 2020.

Thank You

To become an SOCP Member, contact programadmin@socp.us to learn more.

SHIP OPERATIONS COOPERATIVE PROGRAM

Business ▪ Government ▪ Education ▪ Workforce

Catalyst for Change™

www.socp.us
programadmin@socp.us

Time: 12:00 - 12:30 PM ET