INTERNATIONAL MARITIME ORGANIZATION

E

SUB-COMMITTEE ON NAVIGATION, COMMUNICATIONS AND SEARCH AND RESCUE
12th session
Agenda item 10

NCSR 12/10
6 February 2025
Original: ENGLISH
Pre-session public release: ☒

DEVELOPMENT OF GUIDELINES FOR SOFTWARE MAINTENANCE OF SHIPBOARD NAVIGATION AND COMMUNICATION EQUIPMENT AND SYSTEMS

Draft guidelines for software maintenance of shipboard navigation and communication equipment and systems

Submitted by Liberia, Marshall Islands, ICS, BIMCO, IACS and CIRM

SUMMARY

Executive summary:	This document provides draft guidelines for software maintenance of shipboard navigation and communication equipment and systems. Implementation of these guidelines will help improve the efficiency, effectiveness, safety and security of shipboard software maintenance by ensuring it is conducted in accordance with a standardized, controlled and transparent process.
Strategic direction, if applicable:	2
Output:	2.17
Action to be taken:	Paragraph 18
Related document:	MSC 107/17/10

Background

1 MSC 107 considered document MSC 107/17/10, proposing development of requirements for software maintenance of shipboard navigation and communication equipment and systems.

2 The Committee agreed to proceed on a step-by-step basis by developing non-mandatory guidelines first and considering, at a later stage, the need to develop mandatory requirements (MSC 107/20, paragraph 17.33). The Committee agreed also that the scope of the output should only include shipboard navigation and communication equipment and systems regulated under SOLAS chapters IV and V, including those used for transmission and reception of SAR-related information.

3 Accordingly, the Committee agreed to include in its post-biennial agenda an output on "Development of guidelines for software maintenance of shipboard navigation and communication equipment and systems", with two sessions needed to complete the output, assigning the NCSR Sub-Committee as the associated organ.

4 In response to the above, the annex to this document provides draft guidelines for software maintenance of shipboard navigation and communication equipment and systems, that could be used as a basis for further discussions in the Sub-Committee.

Development of the draft guidelines

5 Software maintenance may be defined as "checking, updating, re-configuring, or upgrading software in order to prevent or correct faults, maintain regulatory compliance, and/or improve performance".

6 In 2014, a group of representatives of shipowners, service providers, classification societies and equipment manufacturers began development of an industry standard to address the challenges the different stakeholders experienced during shipboard software maintenance. In December 2017, the resulting Industry Standard on Software Maintenance of Shipboard Equipment ("Industry Standard") was published.

7 The draft guidelines set out in the annex have been adapted from the original Industry Standard by a working group consisting of software maintenance experts. The work has involved approximately 10 hybrid and remote meetings over the last three years.

8 Shipboard software maintenance involves multiple stakeholders. Therefore, in developing the draft guidelines the co-sponsors have facilitated input from representatives of shipping companies, classification societies, service providers, bridge equipment manufacturers, engine manufacturers and a flag Administration.

Discussion

9 The draft guidelines provide guidance for software maintenance of shipboard computer-based systems in SOLAS chapter IV (Radiocommunications) and chapter V (Safety of navigation).

10 The draft guidelines are intended to ensure that software maintenance is conducted in accordance with a controlled and standardized process, which will provide many benefits including:

.1 increasing the overall efficiency of software maintenance by ensuring that shipboard navigation and communication equipment and systems are updated in a coordinated manner by qualified and prepared service personnel;

.2 reducing system downtime, removing the need for follow-up ship visits by service personnel and ultimately cutting costs;

.3 reducing the likelihood of unforeseen problems occurring in integrated systems when the software of an underlying component piece of equipment is maintained;

.4 improving operational stability by enabling the shipboard equipment to roll-back to a previous software version in the event a software update has not been successful;

.5 improving awareness on board the ship about what software is installed on shipboard equipment, through upkeep of electronic software logs and supporting familiarization with any changes in functionality; and

.6 improving the safety and security of software maintenance by ensuring it is only carried out by authorized personnel using cyber-secure equipment, whether the maintenance is carried out on board, ashore, or remotely.

11 The draft guidelines are not intended or foreseen to have any impact on the frequency of software maintenance events, which would be planned and executed when needed, initiated by the master and planned between the crew and the service provider.

12 The draft guidelines describe the initiation, planning and execution of software maintenance, taking into account the related health, safety and environment (HSE) procedures, and cybersecurity considerations. They also introduce newly developed guidance on conducting remote software maintenance.

Training and certification of service providers

13 The draft guidelines specify that service personnel undertaking software maintenance should be trained and certified by the manufacturer of the equipment, whether they work for the manufacturer or a third-party service company. Training and certification of service personnel by the equipment manufacturer is already a widespread practice today.

Electronic service reports

14 The draft guidelines specify the minimum content of an electronic service report to be completed by the service provider after software maintenance. Service reports are routinely issued today after completion of software maintenance as part of the service agreement however, they are typically handwritten documents that are not standardized and the quality of the content therefore varies.

Onboard software log

15 The draft guidelines introduce an onboard software log for the recording of the outcomes of software maintenance events, which represents an administrative burden for the shipowner/operator. However, the co-sponsors firmly believe that introducing a software log, especially if it is connected to an inventory of software, will reduce the administrative burden because the ship will gain a comprehensive overview of the status of software installed on shipboard navigation and communication equipment and systems.

Cybersecurity and safety

16 Building on existing practices, the draft guidelines specify a range of operational procedures related to safe and cyber risk management of the software maintenance process, to be implemented by shipowner/operators, manufacturers and service providers. The co-sponsors' view is that the introduction of such procedures will result in more successfully executed software maintenance events, ensuring continuous and safe functioning of systems.

Proposal

17 The co-sponsors propose that the draft guidelines set out in the annex to this document be used as the basis for further development of the guidelines for software maintenance of shipboard navigation and communication equipment and systems.

Action requested of the Sub-Committee

18 The Sub-Committee is invited to consider the proposal contained in paragraph 17 of this document and take action, as appropriate.

***

ANNEX

DRAFT MSC CIRCULAR

GUIDELINES FOR SOFTWARE MAINTENANCE OF SHIPBOARD NAVIGATION AND COMMUNICATION EQUIPMENT AND SYSTEMS

1 The Maritime Safety Committee, at its […] session ([date]), approved the *Guidelines for software maintenance of shipboard navigation and communication equipment and systems*, as set out in the annex, prepared by the Sub-Committee on Navigation, Communications and Search and Rescue (NCSR), at its […] session ([date]).

2 MSC 107 instructed the NCSR Sub-Committee to develop guidelines for software maintenance of shipboard navigation and communication equipment and systems regulated under SOLAS chapters IV and V, including those used for transmission and reception of SAR-related information.

3 The aim of these Guidelines is to ensure that software maintenance carried out on shipboard navigation and communication equipment and systems is conducted in accordance with a controlled and standardized process.

4 Member States and international organizations are invited to bring these Guidelines to the attention of all parties concerned.

ANNEX

GUIDELINES FOR SOFTWARE MAINTENANCE OF SHIPBOARD NAVIGATION AND COMMUNICATION EQUIPMENT AND SYSTEMS

1 Introduction

1.1 These Guidelines provide guidance for software maintenance of the systems specified in paragraph [2.1].

1.2 The detailed procedures covered by these Guidelines are provided in sections [4 to 11].

1.3 The Company should ensure that software maintenance onboard its ships is conducted in accordance with these Guidelines.

1.4 The Company should establish and implement health, safety and environment (HSE) procedures covering all activities set out in these Guidelines.

1.5 All persons carrying out software maintenance should be trained and certified in accordance with the guidance in section [4]. When performing such activities onboard ships they should comply with instructions and procedures established by the Company.

1.6 The Manufacturer, the Certified Service Provider and the Company should ensure that all software maintenance-related training and operations are conducted in accordance with MSC-FAL.1/Circ.3/Rev.2 *Guidelines on maritime cyber risk management*, as may be revised, as well as the specific cybersecurity recommendations provided in these Guidelines.

2 Application

2.1 These Guidelines apply to shipboard computer-based systems in SOLAS chapters IV (Radiocommunications) and V (Safety of Navigation) that are capable of undergoing software maintenance.

2.2 These Guidelines apply to the methods of software maintenance defined in paragraph [3.8].

2.3 These Guidelines may be applied on a voluntary basis to any shipboard computer-based system not included under paragraph [2.1] that is capable of undergoing software maintenance, including those listed in [appendix 3].

3 Definitions

3.1 *Category of software maintenance* means the type of software maintenance event based on the reason for undertaking the maintenance, which may be one or more of the following:

.1 bug fix (resolving software errors and improving performance/stability);

.2 feature release (adding functionality);

.3 compliance maintenance (maintaining conformity with regulations);

.4 security update (protecting against cyber threats); and

.5 obsolescence maintenance (addressing software and/or hardware that is no longer supported).

3.2 *Certified Service Provider* means the representative of the organization contracted to perform the software maintenance, who undertakes the software maintenance, and who is certified by the Manufacturer in accordance with section [4]. The Certified Service Provider may be a representative of the Manufacturer or a third-party organization.

3.3 *Company* for the purpose of these Guidelines means the shipowner or any other organization or person, such as the manager or the bareboat charterer, which has assumed the responsibility for the operation of the ship from the shipowner.

3.4 *Controlled network* means a shipboard network that has been designed to operate such that it does not pose any security risks to any connected network nodes.

3.5 *Critical update* means a software maintenance event that the Manufacturer has identified as critical to restoring or maintaining proper performance of the shipboard computer-based system.

3.6 *Firmware* means code embedded in electronic devices that provides control, monitoring and data manipulation of engineered products and systems.

3.7 *Manufacturer* means the original manufacturer or any entity which has taken legal and legitimate responsibilities for equipment when the original equipment manufacturer no longer exists or supports the equipment.

3.8 *Method of software maintenance* means the method by which software maintenance is undertaken, which may be:

.1 onboard (carried out on the ship);

.2 onshore (carried out, for example, at the premises of the Certified Service Provider); or

.3 remote (executed by accessing the shipboard computer-based system from a location external to the ship via communication links).

3.9 *Plan of approach* means a detailed description of the work to be undertaken in support of software maintenance, including appropriate assessments of the risks involved.

3.10 *Removable media/storage devices* means portable equipment used during software maintenance, including but not limited to USB memory sticks, laptop computers and external disk drives.

3.11 *Shipboard computer-based systems*, for the purpose of these Guidelines, means operational technology-comprising hardware and software that detects or causes a change, through the direct monitoring and/or control of equipment, assets, processes and events.

3.12 *Software* means programs and operating instructions used in shipboard computer-based systems, including firmware.

3.13 *Software maintenance* means updating, re-configuring, and associated checking of the software within shipboard computer-based systems.

3.14 *Uncontrolled equipment* means a device that is not part of a controlled network.

3.15 *Uncontrolled network* means a shipboard network that does not meet the definition of a controlled network.

4 Guidance for training and certification of service providers by manufacturers

4.1 Software maintenance of shipboard computer-based systems should be carried out by Certified Service Providers certified in accordance with this section.

4.2 Training in the software maintenance procedures and functions of shipboard computer-based systems should be provided by the Manufacturer to the service provider. This should include cybersecurity aspects of software maintenance, including:

.1 security controls and their validation (e.g. firewall settings);

.2 countermeasures (e.g. network port plugs);

.3 integrity checking of shipboard computer-based systems including how to identify that a system has been compromised;

.4 recovery procedures, including those for user data; and

.5 procedure for reporting security events to the manufacturer.

4.3 Upon successful completion of the training, a certificate should be issued by the Manufacturer to the service provider listing:

.1 issuing Manufacturer;

.2 date of issue;

.3 date of expiry;

.4 name of Certified Service Provider;

.5 Certified Service Provider's employer;

.6 list of shipboard computer-based systems produced by the Manufacturer which the Certified Service Provider is trained to maintain; and

.7 method(s) of software maintenance covered for each shipboard computer-based system produced by the Manufacturer (onboard, onshore, and/or remote).

4.4 The Manufacturer should keep a record of all Certified Service Providers with valid certificates.

4.5 The certificate should:

.1 clearly show its expiry date, which should be no more than five years from the date of issue;

.2 become invalid if the Certified Service Provider changes employer; and

.3 have its validity suspended in the event the Manufacturer becomes aware of any shortfall in performance and should only be revalidated after the issuing Manufacturer is satisfied suitable corrective action has been taken.

4.6 The Certified Service Provider should make a copy of the certificate available to the Company.

5 Reports and records

5.1 Upon completion of software maintenance, an electronic service report should be completed and signed by the Certified Service Provider who carried out the work and countersigned by the Company's representative. The minimum content of an electronic service report is defined in [appendix 1].

5.2 An onboard software log should be available on the ship listing the current and previous software versions installed on shipboard computer-based systems, in accordance with [appendix 2]. Each software maintenance event should be recorded in the onboard software log and linked to the associated electronic service report provided by the Certified Service Provider.

5.3 Records of software maintenance events, including electronic service reports, should be stored in the onboard software log for a minimum of five years.

5.4 The onboard software log can be incorporated into an existing inventory management system.

6 Guidance for the Manufacturer

6.1 The Manufacturer should have a Quality Assurance system for software lifecycle activities, which documents relevant procedures, responsibilities and configuration management, including deliveries from suppliers, taking into account cyber risk management and cyber threats in connection with software maintenance.

6.2 Arrangements for software maintenance of shipboard computer-based systems should be specified in the maintenance manuals. Timely access to maintenance manuals and any other relevant technical documentation should be provided to the Certified Service Provider.

6.3 User manuals should specify how the user can communicate a software error or system malfunction.

6.4 Shipboard computer-based systems should:

.1 provide the means to display, at least on demand, the current software version or, where there is no display, provide version information by alternative means such as labelling or a standardized external interface;

.2 allow access for maintenance purposes;

.3 provide protection against unauthorized access[1];

.4 where applicable[2], support recovery procedures which may be implemented by a full back-up of software, configuration parameters and data stored by the user; and

.5 where applicable[2], include a mechanism, described in the maintenance manual along with the method of execution, to generate an on-the-spot diagnostic report after software maintenance has been performed. This mechanism should identify the software version running on the shipboard computer-based system and provide a means to check that interfaces and functionality are operating as intended after the software maintenance has been completed.

6.5 Where shipboard computer-based systems do not support recovery procedures, the Manufacturer should make replacement equipment available to the Certified Service Provider.

6.6 Timely access should be provided to the Certified Service Provider to information pertaining to availability of new software versions for shipboard computer-based systems, together with:

.1 the category of software maintenance;

.2 the method of software maintenance supported for applying it;

.3 where applicable, any dependency on the hardware platform;

.4 instructions on how to confirm the software maintenance has been successfully applied;

.5 a description of changes as specified in [6.9]; and

.6 where applicable, updated manuals as specified in [6.9].

6.7 If the Manufacturer has identified the need for software maintenance, this information should be made available to the Certified Service Provider and the Company, as necessary. The information should include affected software versions and guidance on how the user may check to determine if the installed software version is affected. Means for updating should be made available. If the Manufacturer does not know where the system is installed, and is therefore unable to relay the information to the Certified Service Provider or the Company, the Manufacturer should relay the information to the known purchaser of the system.

---

1 IEC 60945 imposes limitations on access to shipboard equipment by the end user.

2 The phrase "where applicable" is included as there are types of shipboard computer-based systems that cannot feasibly support this requirement.

6.8 If the software maintenance is designated as a critical update by the Manufacturer, this information should be accompanied by a recommendation that the software maintenance should be performed as soon as practicable. Means should be provided for undertaking the software maintenance in a way that ensures minimal downtime of the shipboard compute-based system.

6.9 The software maintenance should be assessed to determine and describe new functionalities, changes and improvements. A summary of new functionalities, changes and improvements should be provided to the Certified Service Provider as necessary, and the Manufacturer should provide updates to Maintenance and User Manuals, where applicable.

6.10 If a software maintenance event is to be performed by a crew member, it should be accompanied by detailed instructions. Provision of remote assistance should be considered.

6.11 Following completion of software maintenance, any feedback received regarding the result of the maintenance should, if appropriate, be addressed and used for improving maintenance procedures.

7 Guidance for the Certified Service Provider

7.1 Maintenance-related operations should be carried out in accordance with a Quality Assurance System, covering:

.1 competence management;

.2 remote maintenance procedures if applicable (see section [10]);

.3 reporting procedures;

.4 shipboard operations safety briefing; and

.5 cybersecurity.

7.2 Quality standards and internal training for Certified Service Providers should be established by the organization contracted to perform the software maintenance in line with maintenance and competency requirements of the Manufacturer and should be specified in a quality manual.

7.3 The cybersecurity competencies and internal cybersecurity training of Certified Service Providers should be documented by the organization contracted to perform the software maintenance, and should address:

.1 general cybersecurity awareness, including system architecture, phishing attacks, password security, physical security, social engineering and remote working security;

.2 integrity checking of removable media/storage devices; and

.3 procedures for incident response.

7.4 The organization contracted to perform the software maintenance should make the Manufacturer aware of any shortfall in performance of its Certified Service Providers.

7.5 When planning the software maintenance, a Plan of approach should be created which should:

.1 provide a description of the work expected to be undertaken;

.2 be shared with and agreed to by the Company;

.3 include information on any risks to the ship and shipboard equipment, alongside associated mitigations;

.4 adhere to the HSE instructions provided by the Company, to ensure that the specific HSE requirements are known, understood and followed; and

.5 include procedures for validating the operation of the shipboard computer-based equipment after completion.

7.6 Where the Manufacturer has determined the need for a critical update and provided the necessary means, this software maintenance should be planned between the Certified Service Provider and the Company to ensure that it will be undertaken as soon as practicable and that downtime of the system is minimized.

7.7 Before arriving on board to perform software maintenance, the organization contracted to perform the software maintenance should ensure that:

.1 date, place and maintenance requirements, including port information and agent details, are planned and agreed with the Company;

.2 Certified Service Provider(s) are appointed to undertake the work, with the basis of the appointment documented and the certificate shared with the Company;

.3 confirmation that the information from the Company about the ship's equipment, system architecture, related configurations and software version(s) has been received and is sufficient;

.4 a shipboard operations safety briefing for the Certified Service Provider(s) is undertaken to ensure that any specific requirements related to safety, security and environmental protection that have been communicated by the Company are understood;

.5 the applicable software version(s) for the shipboard computer-based system are identified and prepared for installation;

.6 the identity of the Certified Service Provider(s) assigned to the job is forwarded to the ship for ISPS clearance and, where the assigned person(s) is subsequently unable to come on board, the Company is informed in advance about any replacement person(s) or about cancellation in case a certified person is not available; and

.7 all necessary tools and resources needed to access the shipboard computer-based system for software maintenance are prepared (for example: laptop, media device, specific tools recommended by the Manufacturer).

7.8 Where shipboard computer-based systems have been designed with recovery procedures, these should be utilized when required, for example if errors occur during software maintenance.

7.9 Procedures to protect against cybersecurity incidents during a software maintenance event should be agreed with the Company, including measures for demonstrating that removeable media/storage devices have been checked for malware.

7.10 Uncontrolled equipment used during software maintenance other than removable media/storage devices (as defined in these Guidelines) should not be directly connected to a controlled network. Such uncontrolled equipment should only be connected to a controlled network through a firewall or similar gateway device[3].

7.11 In order to complete the software maintenance event, the Certified Service Provider should:

.1 ensure that the system functions as intended after the software maintenance. Based on agreement with the Company, the Certified Service Provider may remain onboard to verify correct operation of the shipboard computer-based equipment during sailing;

.2 where the shipboard computer-based system provides a mechanism to generate an on-the-spot diagnostic report, execute this process and include the report in the electronic service report;

.3 complete an electronic service report in accordance with section [5], and provide a copy of the associated electronic file to the Company for adding to the onboard software log;

.4 demonstrate in the presence of the ship's representative that the shipboard equipment functions and operates as intended;

.5 if applicable, demonstrate to the relevant crew member(s) any new/changed functionality; and

.6 if applicable, provide updated User Manuals to the ship.

7.12 Following completion of a software maintenance event, the Certified Service Provider should advise the Manufacturer of any issues or potential improvements to be considered for future software maintenance.

8 Guidance for the Company

8.1 The Company should ensure safe practices for the ship's safe navigation and operation during software maintenance and assess identified possible risks to the ship. Procedures should be in place to ensure that software is maintained taking into consideration the guidance of the Manufacturer. Such procedures could, for example, include annual performance tests, clean-ups, diagnostics and instructions for when this should take place.

[3] For example, international standard IEC 61162-460 specifies a device called a "-460 Gateway" and a device called a "-460 Wireless gateway" for the purpose of connecting controlled and uncontrolled networks.

8.2 Where an operational anomaly or software defect has been identified on a shipboard computer-based system, information should be provided to the organization contracted to perform the software maintenance about the equipment, connections, related configurations and software versions, along with port information and agent details.

8.3 When planning a software maintenance event, a change management procedure should be prepared. The following considerations should be included, depending on the category and method of software maintenance:

.1 identification of the need for additional familiarization, changes to operating procedures, and changes to onboard documentation;

.2 description of how to avoid security risks including preventing unauthorized access, inappropriate assignment of user privileges, and spread of malware;

.3 identification of the software, shipboard equipment, and network to be maintained;

.4 identification of all shipboard equipment affected taking into account the interface connections to the shipboard computer-based system requiring the software maintenance;

.5 identity of Certified Service Provider responsible for the software maintenance;

.6 preparation for remote access if this is agreed to be undertaken during the software maintenance (see section [11]);

.7 identification of appropriate crew member(s) to conduct or assist with the software maintenance; and

.8 coordination with the master to ensure safety of navigation.

8.4 During operational planning of a software maintenance event, the Company should ensure that:

.1 date, place and maintenance requirements for the shipboard computer-based system, including port information and agent details, are planned and agreed upon with the Certified Service Provider;

.2 information is sent to the Certified Service Provider about the ship's equipment, system architecture, related configurations, and software version(s);

.3 where the Manufacturer has determined the need for a critical update and provided the necessary means, the software maintenance is planned with the Certified Service Provider to ensure that it will be undertaken as soon as practicable and that downtime of the shipboard computer-based system is minimized;

.4 any specific HSE instructions are communicated to the Certified Service Provider so that these may be adhered to in the Certified Service Provider's Plan of approach; and

.5 a copy of the Certified Service Provider's certificate is requested.

8.5 Procedures should be in place to protect shipboard computer-based systems from malicious or unintentional security threats during software maintenance and they should include the following considerations:

.1 identification of Certified Service Provider coming on board; and

.2 Certified Service Provider access management.

8.6 When removable media/storage devices are used during software maintenance, the Company should ensure that the Certified Service Provider demonstrates that such devices have been checked for malware before the maintenance is carried out.

8.7 Each software maintenance event should be recorded in the onboard software log and linked to the associated electronic service report, in accordance with [appendices 1 and 2]. Such records should be made available on request by the Certified Service Provider in support of future software maintenance.

8.8 Following conclusion of a software maintenance event, the master should be responsible for confirming that the shipboard computer-based system functions as intended.

8.9 On completion of a software maintenance event, the Company should advise the Manufacturer of any issues or potential improvements to be considered for future software maintenance.

8.10 Following a software maintenance event, crew familiarization should be ensured for any new functionalities, changes or improvements.

9 Additional guidance for the Manufacturer – remote software maintenance

9.1 Shipboard computer-based systems that support remote software maintenance should:

.1 provide multi-factor authentication to verify the identity of remote users;

.2 have the capabilities necessary to manage interruptions to remote access sessions without compromising their integrity and availability;

.3 provide measures to terminate a remote software maintenance event;

.4 provide measures to ensure the integrity of the maintenance, including any data transferred; and

.5 include programs to enable testing of the remote access feature, including functional tests and failure tests.

10 Additional guidance for the Certified Service Provider – remote software maintenance

10.1 Planning for remote maintenance should be coordinated with the Company and ship's master.

10.2 Remote access should only be carried out on a shipboard computer-based system on a controlled network.

10.3 Remote access to any shipboard computer-based system must only be carried out with the express permission of the Company. Additionally, permission should be obtained from the ship's master before initiating each remote maintenance session.

10.4 The shoreside external access points of remote connections should be secured to prevent unauthorized access.

10.5 Where the remote maintenance involves real-time communication and/or monitoring, the means of communication should be arranged before initiating the remote maintenance.

10.6 A time slot for when the shipboard computer-based system is connected and powered up should be agreed with the ship's master. Procedures to ensure the identity of the Certified Service Provider should be in place. After concluding the maintenance, procedures for how to determine when the shipboard connection can be closed should be agreed.

10.7 The Plan of approach should document:

.1 how the remote maintenance will be carried out in a safe and secure way including a description of the work expected to be undertaken, and any communications between the Certified Service Provider and the ship;

.2 how all cybersecurity related aspects of remote maintenance will be controlled from the start to the end of the remote software maintenance event, including but not limited to data integrity and security, access rights and operational state of the shipboard computer-based system;

.3 the communications channel(s) to be used for the remote software maintenance event and its essential technical requirements (e.g. bandwidth);

.4 what measures will be taken if the remote connection is lost during the remote maintenance event; and

.5 how the responsible crew member(s) on board can terminate the remote connection during remote software maintenance.

10.8 In the event of an error or disruption during the remote software maintenance event, an assessment will be conducted jointly with the ship as to whether the event should be continued with, or recovery procedures should be undertaken.

11 Additional guidance for the Company – remote software maintenance

11.1 Remote access should only be allowed to shipboard computer-based systems on a controlled network.

11.2 The remote access connection should be restricted to the shipboard computer-based system undergoing software maintenance.

11.3 For the purposes of planning and executing a remote software maintenance event, the Company should ensure that:

.1 permission is provided to the Certified Service Provider to undertake remote maintenance, specifying who has access, when they have access, and what equipment they have access to;

.2 permission is provided by the ship's master before every remote maintenance session;

.3 procedures are in place to ensure that those service providers certified to remotely access shipboard computer-based systems for the purposes of software maintenance can do so;

.4 procedures are in place detailing the measures to be taken if the remote connection is lost during the remote maintenance event;

.5 procedures are in place to ensure that remote maintenance takes place during safe and suitable conditions; and

.6 confirmation is received from the ship that the remote software maintenance event has been completed successfully.

11.4 In the event of an error or disruption during the remote software maintenance event, an assessment will be conducted jointly with the Certified Service Provider as to whether the event should be continued with or recovery procedures should be undertaken.

APPENDIX 1

ELECTRONIC SERVICE REPORTS

This appendix specifies the minimum content of the electronic service report which is to be completed by the Certified Service Provider at the end of a software maintenance event.[4]

Format

The format of the electronic service report is not standardized as its detailed content is dependent on the business system used by the Certified Service Provider. The format of the electronic service report should be suitable for electronic filing and its content should be searchable. As minimum it should be possible to store these electronic service report documents in individual electronic folders.

Content

The following template identifies the minimum content of a service report. Pages should be numbered (as for example: 1 of 10)

"1 General information

Information about the ship:

.1 shipowner / operator;

.2 ship name;

.3 IMO number; and

.4 MMSI number.

Information about the Certified Service Provider:

.1 name and contact information of organization contracted to perform the software maintenance;

.2 name of Certified Service Provider; and

.3 employee ID of Certified Service Provider.

2 Information about the shipboard computer-based system and software

For each piece of equipment undergoing software maintenance, the following details should be provided:

.1 manufacturer;

.2 model;

.3 type;

.

[4] ISO 24060-2 specifies requirements for electronic service reports.

4 serial number;

.5 software version prior to maintenance; and

.6 date of previous software maintenance (installation date if no prior maintenance).

3 Details and purpose of software maintenance event

.1 date and time of start of software maintenance event;

.2 date and time of end of software maintenance event;

.3 location of ship at the time of completion of software maintenance event;

.4 method of maintenance (onboard; onshore; remote);

.5 category of software maintenance (indicate as appropriate):

.1 bug fix;

.2 feature release;

.3 compliance maintenance;

.4 security update;

.5 obsolescence maintenance;

.6 combination of the above (specify);

.7 other (specify); and

.6 if it was a critical update (Yes/No).

4 Cybersecurity

The following information should be recorded for any removable media/storage device used to perform maintenance:

.1 version and make of the anti-virus/malware software used;

.2 last update of the anti-virus/malware database; and

.3 confirmation and date of clean anti-virus/malware scan.

5 Technical report

.1 detailed description of the work performed;

.2 outcome of the maintenance event; and

.3 for each piece of equipment undergoing software maintenance, record the software version after completion.

6 Hardware changes

Should a hardware component of a shipboard computer-based system be added, removed or replaced, the following information should be recorded for the new hardware and any hardware that has been replaced:

.1 manufacturer;

.2 model;

.3 type; and

.4 serial number.

7 Operational status after maintenance event

For each shipboard computer-based system undergoing software maintenance indicate [Yes]/[No]/[N/A] for the following:

.1 all available self-test mechanisms have been completed successfully;

.2 there was a demonstration in the presence of the ship's representative that the shipboard computer-based system functions and operates as intended after the software maintenance;

.3 additional new functionalities were demonstrated to the ship's representative; and

.4 an on-the-spot diagnostic report was generated after software maintenance job completion and is appended to the electronic service report.

Should a follow-up be deemed necessary, provide reason/details.

8 Post-event acceptance

.1 has the software maintenance event been completed to the satisfaction of the ship's representative (Yes/No); and

.2 capture feedback comments from the ship's representative about the maintenance event.

9 Signatures

.1 Certified Service Provider; and

.2 Company representative.

Digital signatures that prevent tampering and confirm the originality of the content of the report should be considered."

APPENDIX 2

ONBOARD SOFTWARE LOG

1 The onboard software log is a repository of information relating to the software installed on shipboard computer-based systems, including associated software maintenance events and the related electronic service reports.[5]

2 Electronic service reports should be linked to individual software maintenance event records.

3 The onboard software log is implemented and maintained by the Company and made available on board. The onboard software log is updated after each software maintenance event.

4 Each onboard software log should include the following fields as a minimum:

.1 Ship details:

.1 ship name;

.2 Company name; and

.3 IMO number;

.2 Shipboard computer-based system details:

.1 type;

.2 Manufacturer;

.3 model;

.4 serial number;

.5 previous software version;

.6 current software version; and

.7 software maintenance event details:

.1 date of software maintenance event;

.2 initiator (Manufacturer/Certified Service Provider/Company);

.3 method of software maintenance;

.4 category of software maintenance;

.5 status of equipment on arrival;

.6 status of equipment on completion; and

[5] ISO 24060-1 specifies requirements for a Ship Software Logging System (SSLS).

.7 Certified Service Provider details:

.1 name of organization contracted to perform the maintenance;

.2 name of Certified Service Provider; and

.3 employee ID.

APPENDIX 3

ADDITIONAL SHIPBOARD COMPUTER-BASED SYSTEMS TO WHICH THESE GUIDELINES MAY BE APPLIED

1 These Guidelines may be applied on a voluntary basis to any shipboard computer-based system not included under paragraph [2.1].

2 A list of such systems is included below (note that this list is not intended to be exhaustive).

.1 alarm and monitoring systems for propulsion systems

.2 ballast transfer valve remote control system;

.3 bilge level detection and associated control of pumps;

.4 bunkering control system;

.5 drilling systems;

.6 dynamic positioning system of equipment classes 2 and 3 according to MSC/Circ.645 on *Guidelines for vessels with dynamic positioning systems*;

.7 electric power system (including power management system);

.8 fuel oil treatment system;

.9 liquid cargo transfer control system;

.10 propulsion system of a ship, meaning the means to generate and control mechanical thrust in order to move the ship;

.11 security, access control and surveillance system;

.12 ship safety systems covering fire detection and fighting, flooding detection and fighting, internal communication systems involved in evacuation phases, ship systems involved in operation of life-saving appliances equipment;

.13 ship to shore integrated systems (e.g. remote control systems);

.14 stabilization and ride control systems; and

.15 steering system control system.