Guideline

Cyber security guideline for SAILOR products

February 2021

Awareness to Cyber security has been increasing over the recent years based on the growing use of information technology on-board ships, and the connectivity used to provide integration into the shore based supporting systems.
With the Implementation of IMO resolution MSC.428(98) **MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS** from January 1st 2021, cyber security is to be included in the risk assessment in the Safety Management System required by the ISM code.
Based on this, Cobham SATCOM is pleased to provide the following guidance in relation to the Cyber risks related to our products and the mitigation recommended.

Contents

Guideline

SAILOR FleetBroadband terminals

Includes: SAILOR Fleet One, SAILOR 150, SAILOR 250, SAILOR 500

Cyber security risks associated to these terminals are related to the terminal in itself and the internet connection.

Installation guidance

Installation and activation is to be performed by skilled personnel familiar with the terminal.

The following mitigation is to be observed in relation to the terminal itself:

- During installation and activation of the terminal, the default administrator password must be changed. The new password is recommended to be long, complex and random.
- The administrator password must be changed if there is any suspicion of misuse or hostile activity. It is recommended to change the password regularly.
- The terminal is delivered with relevant settings in secure mode. Changing these settings will reduce the security level of the terminal. Other functionalities are enabled to ease usage, but they can be disabled to increase the security level. Are any of these settings to be changed during installation, the Master or network responsible person on-board must be informed.
    - Settings, which can be changed to enhance security, but limit ease of use:
        - User privileges
- Any PC or mobile device connected to the terminal must be screened and confirmed cyber secure before connected to the terminal.
- To secure the internet access via the terminal, it is recommended to incorporate a firewall on land or arrange security measures with the service provider.
- Any device connector point are NOT to be used for charging of mobile devices.

The following mitigation is to be observed in relation to the internet connection

- This terminal provides access to the internet through the service provider's satellite network.
- The terminal in itself does not provide any protection of the internet connection and access.

- Any cyber security measures on the Internet connection are to be arranged separately. Among the many different options, the most common in an appropriate combination are:
  - To arrange with the service provider
  - To have all communication screened at a shore facility, e.g. a management office
  - To fit firewall and other security measures between the internet connection on the terminal and the on-board network and/or connected devices.

User guidance

The following mitigation is to be observed in relation to the terminal itself:

- The administrator password must be changed with regular intervals, and not less than annually. The new password is recommended to be long, complex and random.
- Changes in the set-up menu is to be performed by skilled personnel familiar with the terminal or under their guidance.
- The terminal is delivered with relevant settings in secure mode. Changing these settings will reduce the security level of the terminal. Other functionalities are enabled to ease usage, but they can be disabled to increase the security level. Are these settings to be changed during installation, the Master or network responsible person on-board must be informed.
  - Settings, which can be changed to enhance security, but limit ease of use:
    - User privileges
- To secure the internet access via the terminal, it is recommended to incorporate a firewall on land or arrange security measures with the service provider.
- Any device connector point are NOT to be used for charging of mobile devices.

The following mitigation is to be observed in relation to the Internet connection

- This terminal provides access to the internet through the service provider's satellite network.
- The terminal does not provide any protection of the Internet connection and access.
- Any cyber security measures on the Internet connection are to be arranged separately. Among the many different options, the most common in an appropriate combination are:
  - To arrange with the service provider
  - To have all communication screened at a shore facility, e.g. a management office
  - To fit firewall and other security measures between the internet connection on the terminal and the on-board network and or connected devices.

Guideline

SAILOR 4300 L-Band terminal

Cyber risks related to this terminal are related to the terminal itself and the Internet connection.

Installation guidance

Installation and activation is to be performed by skilled personnel familiar with the terminal.

The following mitigation is to be observed in relation to the terminal itself:

- Any PC or mobile device connected to the terminal must be screened and confirmed cyber secure before connected to the terminal.
- The terminal is delivered with relevant settings in secure mode. Changing these settings will reduce the security level of the terminal. Other functionalities are enabled to ease use, but they can be disabled to increase the security level. Are these settings to be changed during installation, the Master or network responsible person on-board must be informed.
    - Settings which can enhance cyber security, but limit ease of use:
        - LAN settings
        - ThraneLINK access
        - API via LAN access
        - HTTP enabled
- The service interface must not be exposed directly to the Internet.
- Is Internet access to the terminal enabled through the service interface, this interface must be protected with a network security device such as a firewall.
- Password must be changed if there is a risk of exposure. When you create a new password, make sure it is a strong password (long, complex, and random).
- Any device connector point are NOT to be used for charging of mobile devices.

The following mitigation is to be observed in relation to the Internet connection

- This terminal provides access to the Internet through the service provider's satellite network.
- The terminal does not provide any protection of the Internet connection and access.
- Any cyber security measures on the Internet connection are to be arranged separately. Among the many different options, the most common in an appropriate combination are:
    - To arrange with the service provider
    - To have all communication screened at a shore facility, e.g. management office
    - To fit firewall and other security devices between the internet connection on the terminal and the on-board network and or connected devices. For guidance see IEC 63154

User guidance

The following mitigation is to be observed in relation to the terminal itself:

- Changes in the set-up menu is only to be performed by skilled personnel familiar with the terminal or under their guidance.
- The terminal is delivered with relevant settings in secure mode. Changing these settings will reduce the security level of the terminal. Other functionalities are enabled to ease use, but they can be disabled to increase the security level. Are these settings to be changed during installation, the Master or network responsible person on-board must be informed.
    - Settings which can enhance cyber security, but limit ease of use:
        - LAN settings
        - ThraneLINK access
        - API via LAN access
        - HTTP enabled
- The service interface must not be exposed directly to the Internet.
- Is Internet access to the terminal enabled through the service interface, this interface must be protected with a network security device such as a firewall.
- Any device connector point are NOT to be used for charging of mobile devices.

The following mitigation is to be observed in relation to the Internet connection:

- This terminal provides access to the internet through the service provider's satellite network.
- The terminal does not provide any protection of the Internet connection.
- Any cyber security measures on the Internet connection are to be arranged separately. Among the many different options, the most common in an appropriate combination are:
    - To arrange with the service provider
    - To have all communication screened at a shore facility, e.g. management office
    - To fit firewall and other security devices between the Internet connection on the terminal and the on-board network and or connected devices

SAILOR 6280 AIS system

Cyber risk related to this terminal is related to the terminal itself.

Additionally, the terminal can be exposed to Spoofing and Jamming of the position information (elaborated description below).

Installation guidance

Installation must be IMO compliant

The following mitigation is to be observed:

- During installation and activation, the default user password must be changed.
    - Changing the system administrator will complicate support cases and should be done with caution.
- The user password must be changed with regular intervals, and not less than at each technical service.
- Make the crew aware by markings or similar that any device connector point are NOT to be used for charging of mobile devices.
- Any removable memory sticks or other peripheral devices are to be screened and confirmed cyber secure before connected to the terminal.
- Any PC used for SW updates and configuration of the terminal is to be screened and confirmed cyber secure before connected to the terminal.
- Connection to networks or other equipment must observe:
    - IEC 63154 Module K for IEC 61162-1 and IEC 61162-2 connections
    - IEC 63154 Module L for IEC 61162-450 connections
- The AIS must not be exposed directly to the Internet.
- If Internet access to the AIS system is enabled, the interface must be protected with a network security measure such as a firewall.

For information:

- Spoofing and Jamming are external threats, which either set wrong positions or block the function of the internal GNSS. GNSS is the abbreviation Global Navigation Satellite System like GPS, which can provide global positioning coordinates based on satellite technology.
    - Spoofing: The main function of the internal GNSS is timing. A wrong position might not disable the ability to transmit and receive, but if spoofing happens there is a great risk of more equipment being hit if the same satellite navigation system e.g. GPS is used. This will lead to incorrect positions being send in the transmissions.
    - Jamming blocks the receiver in the GNSS, resulting in no TX functions of the AIS.

User guidance

Installation must be IMO compliant

The following mitigation is to be observed:

- The user password must be changed with regular intervals, and not less than at each technical service.
- Any device connector point are NOT to be used for charging of mobile devices.
- Any removable memory sticks or other peripheral devices are to be screened and confirmed cyber secure before connected to the terminal.
- SW updates and changes in the protected set-up menu are only to be performed by skilled personnel familiar with the procedure.
- The service Interface must not be exposed directly to the Internet.
- Is Internet access to the AIS system enabled, the interface must be protected with a network security device such as a firewall.

For information:

- Spoofing and Jamming are external threats, which either set wrong positions or block the function of the internal GNSS. GNSS is the abbreviation Global Navigation Satellite System like GPS, which can provide global positioning coordinates based on satellite technology.
    - Spoofing: The main function of the internal GNSS is timing. A wrong position might not disable the ability to transmit and receive, but if spoofing happens there is a great risk of more equipment being hit if the same satellite navigation system e.g. GPS is used. This will lead to incorrect positions being send in the transmissions.
    - Jamming blocks the receiver in the GNSS, resulting in no TX functions of the AIS.

SAILOR 6222 VHF

Cyber risk related to this terminal is related to the terminal itself.

Installation guidance

Installation must be IMO compliant

The following mitigation is to be observed:

- Any PC or mobile device connected to the terminal must be screened and confirmed cyber secure before connected to the terminal.
- The service interface must not be exposed directly to the Internet.
- Is Internet access to the terminal enabled through the service interface, this interface must be protected with a network security device such as a firewall.
- Any device connector point are NOT to be used for charging of mobile devices.

User guidance

The following mitigation is to be observed:

- SW updates and changes in the protected set-up menu is only to be performed by Cobham authorized personnel.
- The service interface must not be exposed directly to the Internet
- Is Internet access to the VHF enabled, the interface must be protected with a network security device such as a firewall.
- Any device connector point are NOT to be used for charging of mobile devices.

SAILOR 63XX MF/HF series

Includes: SAILOR 6310 MF/HF 150W DSC Class A; SAILOR 6320 MF/HF 250W DSC Class A, SAILOR 6350 MF/HF 500W DSC Class A

Cyber risk related to this terminal is related to the terminal itself.

Installation guidance

Installation must be IMO compliant

The following mitigation is to be observed:

- Any PC or mobile device connected to the terminal must be screened and confirmed cyber secure before connected to the terminal.
- The service interface must not be exposed directly to the Internet.
- Is Internet access to the terminal enabled through the service interface, this interface must be protected with a network security device such as a firewall.
- Any device connector point are NOT to be used for charging of mobile devices.

User guidance

The following mitigation is to be observed:

- SW updates and changes in the protected set-up menu is only to be performed by Cobham authorized personnel.
- The service interface must not be exposed directly to the Internet
- Is Internet access to the MF/HF enabled, the interface must be protected with a network security device such as a firewall
- Any device connector point are NOT to be used for charging of mobile devices.

Guideline

SAILOR 6390 Navtex

Cyber risk related to this terminal is related to the terminal itself.

Installation guidance

Installation must be IMO compliant

The following mitigation is to be observed:

- Any PC used for SW updates and configuration of the terminal is to be screened and confirmed cyber secure before connected to the terminal.
- The service interface must not be exposed directly to the internet.
- Is internet access to the terminal enabled through the service interface, this interface must be protected with a network security device such as a firewall.
- Any device connector point are NOT to be used for charging of mobile devices.

User guidance

The following mitigation is to be observed:

- SW updates and changes in the protected set-up menu is only to be performed by Cobham authorized personnel.
- The service interface must not be exposed directly to the internet
- Is Internet access to the Navtex enabled, the interface must be protected with a network security device such as a firewall.
- Any device connector point are NOT to be used for charging of mobile devices.

SAILOR 6110 Mini-C

Includes the SAILOR 3027 Mini-C antenna. This description also applies to the old SAILOR 3026 Mini-C antenna.

Cyber risk related to this terminal relates to the terminal itself.

Installation guidance

Installation and activation must be IMO compliant

The following mitigation is to be observed:

- During installation and activation, the default password must be changed. The new password is recommended to be long, complex and random with the following options to include the numbers 0-9. The password must be 8 characters long.
    - Distributor password should NOT be changed.
- The password must be changed with regular intervals, and not less than at each technical service.
- Any device connector point are NOT to be used for charging of mobile devices.
- Any removable memory sticks or other peripheral devices are to be screened and confirmed cyber secure before connected to the terminal.
- Any PC or mobile device connected to the terminal must be screened and confirmed cyber secure before connected to the terminal.
- The service interface must not be exposed directly to the Internet.
- Is Internet access to the terminal enabled through the service interface, this interface must be protected with a network security device such as a firewall.

User guidance

The following mitigation is to be observed:

- The password must be changed with regular intervals, and not less than at each technical service. The new password is recommended to be long, complex and random with the following options to include the numbers 0-9. The password must be 8 characters long.
    - Distributor password should NOT be changed.
- SW updates and changes in the set-up menu is only to be performed by Cobham SATCOM authorized personnel.
- Any device connector point are NOT to be used for charging of mobile devices.
- Any removable memory sticks or other peripheral devices are to be screened and confirmed cyber secure before connected to the terminal.
- Is Internet access to the Mini-C terminal enabled, the interface must be protected with a network security device such as a firewall.