Paper for Consideration by HSSC 15

Cyber Security Guidance Loading ENCs in ECDIS

Submitted by:	ENCWG
Executive Summary:	Report on the development of Mariner guidance to minimise cyber risk when loading ENCs in to ECDIS
Related Documents:	S-63 data protection scheme
Related Projects:	HSSC action14/43 HSSC 14/40 (former HSSC13/33, HSSC12/25)

Introduction / Background

HSSC14/43 agreed on the proposal from the ENCWG to create a new IHO ECDIS Cyber Security Guideline to manage cyber risk onboard when loading ENC data into ECDIS. It was decided that this was the preferable option rather than to produce a new edition of S-63 which would have had significant impact on in-service ECDIS systems.

Analysis/Discussion.

An expert group of contributors have developed the guidance over the last year, with significant contributions from industry. In addition to support from ECDIS OEMs UKHO have facilitated support from the Plymouth University's Marine Institute/CyberSHIP Lab.

The guidance is currently in the final signoff stage within the ENCWG, it will be included in the draft S-67 that is currently being prepared.

A draft copy of the guidance can be found in Annex A

Action Required of HSSC

HSSC 15 is requested to note the progress of the action

Annex A

Draft IHO Cyber Security Guidance

IHO ENC & ECDIS Cyber Security Guidance

1. Introduction

The benefits of digitalisation rely on interconnected systems which can safely transfer information to deliver operational optimisation, cost savings and safety improvements.

The Maritime industry is going through a significant period of change, driven by the increased availability of satellite communications, technological developments previously unachievable ten years ago are rapidly becoming possible. With increased digital interconnectivity comes the increased risk of cyber-attack and vessels which once considered themselves safe when at sea can no longer assume that they will not be a target of cyber criminals.

The goal of the IMO maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

MSC.428(98), states from 1st Jan 2021 all vessels must ensure that cyber risks are appropriately addressed in their Safety Management Systems (SMS).

ENC data used in ECDIS must be continually updated with changes, promulgated by the Hydrographic Office, to remain carriage compliant as required by SOLAS. This continual process of updating ENCs presents a permanent and persistent vulnerability which must be managed by shipping companies in their SMS.

This guideline prepared by the IHO seeks to support Shipping companies and Mariners in limiting their exposure to cyber risk when using ENCs in ECDIS.

Key to limiting risk is ensuring the data that goes into the ECDIS comes from a trusted source. It is possible to reduce risk by ensuring the ENC service that is purchased for the vessel come from a reputable ENC service provider, who will transfer the data to the vessel in an encrypted form.

Most commercial ENC services use the IHO data protection scheme S-63 to protect the data. S-63 provides a method for ensuring the data received in the ECDIS can be authenticated against a known and trusted list of providers. All ECDIS are tested during type approval to ensure they can load and decrypt S-63.

While all ECDIS are capable of loading and displaying ENC data in its native S-57 format, this offers no cyber security protection and is not advised.

There are a number of ENC service providers that convert the data on shore to the proprietary data format of the ECDIS. These are called SENC services and are specified to be protected by a security that provides equivalent or greater protections that IHO S-63.

2. Glossary of terms

ENC – Electronic Navigational Chart.

ECDIS – Electronic Chart Display & Information System.

3. References

MSC.428(98), 16 June 2017, Maritime Cyber Risk Management in Safety Management System (SMS)

MSC-FAL.1/Circ.3, 5 July 2017, Guidelines on Maritime Cyber Risk Management

Bimco, The Guidelines on Cyber Security Onboard Ships, version 4

IEC 61162-450

IEC 61162-460

4. Guideline Objectives

This guideline prepared by the IHO seeks to support Shipping companies and Mariners when developing plans to limit their exposure to cyber risk when using ENCs in ECDIS.

The document uses the established IMO Cyber Risk Management categories

4.1. **Identify**: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

4.2. **Protect:** Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

4.3. **Detect:** Develop and implement activities necessary to detect a cyber-event in a timely manner.

4.4. **Respond:** Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

4.5. **Recover:** Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

5. Scope of applicability

The two principal data transfer methods used to load ENC data and cell permits into ECDIS are covered by this guideline

1. Removable media
2. Bridge networks

(Navigation and radiocommunication systems, covered by the following standards IEC 61162-460 or IEC 63154 can be used)

6. Transfer of ENC data and cell permits via physical removable media

Cyber Risk Management Categories	Issues / Considerations
Identify	• ECDIS • USB / DVD • Communication PC / Back of Bridge • Lack of cyber security training and awareness. • Vessel's network • Potential threat actors • Transfer of data and permits to ECDIS via USB / DVD. • Lack of Network boundaries and segmentation. • ECDIS operating system. • Outdated or lack of Anti-Virus on ECDIS. • Inadequate access controls
Protect	• Create a risk assessment matrix and quantify potential impacts based on the severity and likelihood of each cyber-attack scenario.
Detect	• Use approved ENC distributors that secure data transfer in S-63 or an equivalent security scheme • Scan physical media or USB with antivirus for malware or ransomware every time it's used. • Add access controls to the individual systems.
Respond	• Develop a response plan covering relevant contingencies.
Recover	• Preparation • Detection and analysis • Containment and eradication • Post incident recovery.

7. Identify Threats via USB or Physical Media.

The first stage of becoming more cyber secure is to identify the potential threat vectors for malicious code to infiltrate the vessels networks, systems or data sources. The internal and external threats to the vessels ECDIS need careful examination along with interdependencies on different systems and their data flows. Identifying the key resources involved in the management of the ECDIS, the operation/governance documents and crew members roles and responsibilities should all be considered.

7.1. **USB/DVD** – The ability for ECDIS to accept USB and DVD media presents a serious threat vector for malicious software to be installed onto the system. USBs and DVDs can auto-launch and easily transfer spyware and ransomware content onto the ECDIS. The threat level can be significantly heightened if the source of the physical media is unknown or if strict protocol and physical barriers to the upload media have not been enforced on the vessel.

7.2. **ECDIS** – The ECDIS itself and its underlying operating system could be a potential threat. Within the market today there's still a lot of ECDIS still running on Windows XP or older operating systems which have greater-known vulnerabilities and are more open to malicious attacks. ECDIS with newer operating systems can have regular updates, patches and service packs applied to them to mitigate for the latest known security threats.

7.3. **Communication / Back of Bridge system –** Vessels commonly use a back of bridge system connected to an external network through which to receive their navigational data updates and for route planning. The back of bridge system can be a primary target for malicious actors to use as a front door for ingesting viruses for onward transit onto an ECDIS via physical media.

7.4. Vessels Network – ECDIS can update via a ships external network as well as via physical media. Whilst threats regarding the human handling of media are not applicable other potential threats emerge. Networks that are not secured via gateways, firewalls and encryption make for an ideal target. If a vessels network is breached it can have catastrophic effects on other vessel systems connected to the same network. Attackers can flood the network with excessive data traffic to degrade the service in a denial-of-service attack if monitoring and threat detection isn't implemented.

7.5. **Potential Threat Actors** – A vessel relies upon external organisations data and services to ensure safe navigation on the latest up to date data. A trust and reliance on the internal crew members also exists in ensuring they follow strict protocol and have no potential motives to want to sabotage the safety of a vessel. Spearfishing emails, fake websites, redirects and cross site scripting all pose a significant security threat to the secure transfer of legitimate data onto a vessels network or back of bridge before its loaded onto an ECDIS.

7.6. Lack of cyber security training and awareness – The crew of a vessel and their cyber security awareness need to be assessed and continuously managed. As new physical and technical attack vectors emerge and evolve there's the potential for crews' awareness to decline and for the potential cyber security risk to heighten. If there's a lack of vessels protocol, training and documentation in place then responding to a cyber-attack will likely take longer with greater catastrophic effect.

8. Identify Vulnerabilities

Inventory of CBSs (Computer Based Systems) and networks– Every vessel should ensure they create an inventory mapping the networks, the data flows and the hardware and the software used onboard the vessel. This inventory should be a living document which is constantly updated every time there's a modification to applications, operating systems and firmware.

Having an up-to-date wholistic overview of the vessels data ecosystem allows for easy analysis of the potential threats and helps highlight areas that need hardening or risk being an easy target for attackers. Good inventories should list IP addresses, port numbers and all the necessary information that could be drawn upon to halt an attack or to be used in recovering from one.

In the creation of an inventory stakeholders ranging from shipping company, ship designer, System Integrator and Classification Society should all be consulted and engaged to help build a detailed system map.

Inventories themselves pose a potential security threat should they get into the wrong hands and so should be physically and digitally secured and only accessed by necessary personnel.

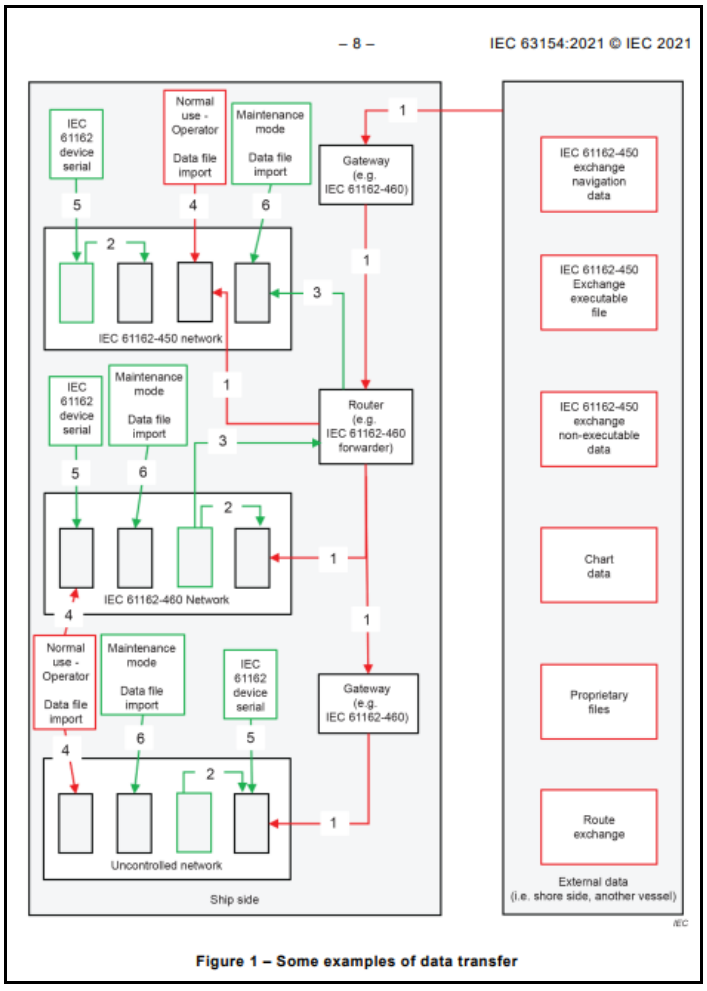

Figure 1 – Some examples of data transfer

Transfer of data and permits to ECDIS via USB / DVD – For up-to-date navigation mariners are required to load permit files and exchange sets into their ECDIS on a frequent basis. Whilst most of the exchange set information is encrypted and contains digital signature files there are still unsigned ancillary files that present a significant threat which could be modified or replaced with malicious code. Furthermore, there's an IMO/IHO requirement for ECDIS to be able to load unencrypted data that presents another threat vector for malicious software to be loaded onto the ECDIS system.

Vessels still use CD and DVD to update their ECDIS with the latest weekly data. These disks are often written by distributors and shipping companies before being sent via a courier onto a vessel. Malicious data could easily be transferred onto the disk, or the disk could be switched during transit by a threat actor before its applied to an ECDIS. Scanning disks with anti-virus software, using digital signatures (where possible) and verifying the source of the information can all help reduce the potential risk.

Whatever the update method removable media devices should be checked for malware and to validate legitimate software by digital signatures and watermarks before use.

ECDIS operating system – The vast majority of ECDIS are running on Windows XP or other legacy systems with well-known security and vulnerability issues. Vessel should ensure their ECDIS have patches installed regularly in a maintenance mode to address security vulnerabilities and other bugs or improve operating systems or applications. Vessel should ensure files and systems are backed up so they can recover if attacked or if they experience database corruption.

The vessels ECDIS user policy should adopt a principle of Least Functionality, whereby to provide only essential capabilities and to prohibit/restrict the use of non-essential functions, ports, protocols and services are disabled or otherwise prohibited. The ECDIS should be utilized for primary navigational use only and all other data validation and preparation should be carried out on a secure back of bridge system/network.

Outdated or lack of Anti-Virus on ECDIS - ECDIS and back of bridge systems should be protected against malicious code such as viruses, worms, trojan horses, spyware, etc. A virus can easily evade and hide within the ECDIS whilst self-replicating, spreading and acting maliciously, performing actions that end up affecting the system's navigational performance.

Antivirus, antimalware, antispam software will create a shield to block known threat vectors into the system and remove any viruses already detected within the system hardware.

Common means for virus infiltration into or via a back of bridge setup are electronic mail, electronic mail attachments, websites, removable media, PDF documents, web services, network connections and already infected networks.

If ECDIS cannot run or have installed anti-virus and anti-malware software, malware protection shall be implemented in the form of operational procedures, physical safeguards, or according to manufacturer's recommendations.

Inadequate access controls – The ECDIS, back of bridge system and network on the vessel should provide physical and digital measures to limit the ability to interact with the system itself. Access controls and user groups should be implemented where possible to

restrict access to system resources or gain knowledge of essential control system components and functions.

Access to the vessels onboard networks and access points should only be allowed to authorized personnel, under supervision or according to documented procedures, e.g., for maintenance. Other networks should be used for non-navigational requirements such as printing documents or access external uncontrolled networks such as the internet.

Transfer of ENC data and cell permits via a network

Cyber Risk Management Categories	Issues / Considerations
Identify	• Lack of cyber security training and awareness. • Vessel's network • Potential threat actors • Lack of Network boundaries and segmentation. • ECDIS operating system. • Outdated or lack of Anti-Virus on ECDIS. • Inadequate access controls • Use of unverified applications running on other back of bridge or systems connected to the network.
Protect	• Use an authorised ENC distributor where data contains certificates. • Ensure antivirus is up to date on back of bridge or systems connected to the ECDIS network • Use 460 network gateway • Pre-validation of data within distributors system. • Develop a incident response plan, checklists and drills for a possible attack including backup arrangement of ECDIS.
Detect (one in isolation may not indicate cyber-attack)	• Check URL and network addresses of data sender / white list. • ECDIS behaviour abnormalities present or a reduction in system speed. • Monitor system performance and speed. • Check alerts and notifications from anti-virus regularly. • How likely is your system to be infected based on network connectivity and amount of use? • Add access controls to the individual systems.
Respond	• Ensure master of the vessel is informed of a possible cyber issue as soon as it occurs and log the incident. • Primarily ensure the safety of the crew and vessel is accounted for. • Enact a contingency plan covering relevant contingencies and ensure vessel strictly follows response plan for cyber-attack. • Add an extra watch on the vessel (if possible) whilst vessel undergoes response plan. • Check redundancy systems – backup ECDIS, back of bridge, Paper chart etc. • Collect evidence of the attack (Screen shots, videos) to aid response plans and better respond to future

	incidents. • Contact shipping company to inform them for onward communication to coastguards and discuss what assistance they can provide. • Inform shipping companies and distributors and describe symptoms, severity, all operations carried out on the bridge and operational contexts. • Inform coastal authorities VTS etc so nearby traffic can be alerted to the dangers. • As a last resort disconnect network cables and WiFi. • Communications of demand – In a ransomware scenario listen to demands of threat actor and stall for time before deciding how to proceed. • Ensure communication is shared with the entire crew of the vessel.
Recover	• Safety first, navigate to a port where systems can be assessed by a professional. • Complete uninstall/reinstall of ECDIS software by a professional.(if required). • Communicate with the system integrator responsible for the installation regarding the security vulnerability. • Ensure ECDIS is returned to a safe state and not the vessels normal state. • Containment and eradication – Analyse what caused the incident and ensure it's removed from the ECDIS and any network components. • Post incident recovery – Evaluate what went well and where improvements are required. Ensure incident is recorded and all experience is documented for use in future incidents.

9. Identify Threats (to your Network)

Lack of Network boundaries and segmentation – Networks which connect to the ECDIS need to be managed and have security zones established by your system integrator and shipping company to ensure viruses and malicious packets of data do not penetrate the ECDIS or other vessel systems.

Well defined security policies and capabilities need to be established to only allow explicit traffic across the different zones of the network to the ECDIS. Ensure your system integrator has installed 460-Gateways, Firewalls, Routers and isolated (air gaped) networks to manage the vessels connection with an external network.

Using Intrusion Prevention Systems (IPS) network traffic can be monitored. Using 460-Gateways, Forwarders and DMZs (demilitarized zones) it more difficult for an attacker to perpetrate an attack throughout the entire network and reach the ECDIS. Segmentation can help reduce the potential attack surface, prevent attackers from achieving lateral movement through systems and improve network performance.

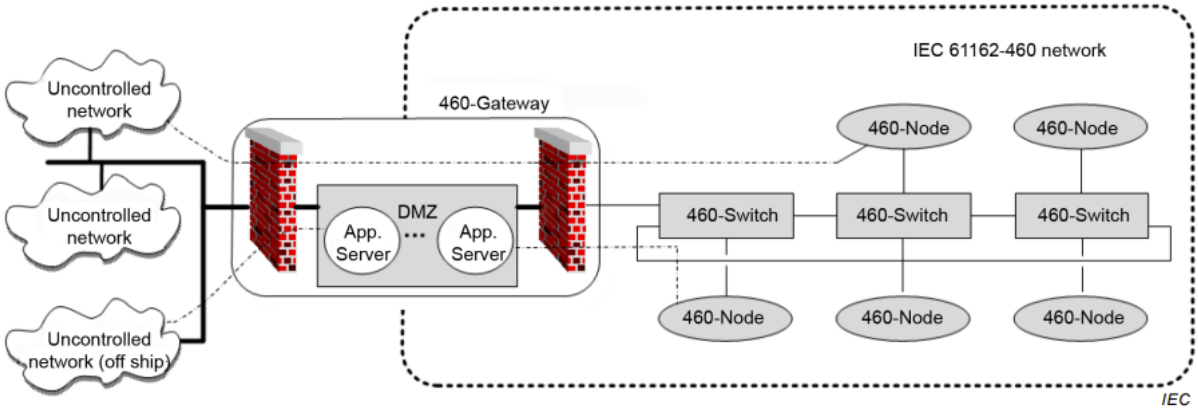

Figure 2 – 460-Network with 460-Gateway

Use of unverified applications running on other back of bridge systems connected to the network – The vessel should ensure the use of third party or applications not documented or on the CBS inventory are prohibited where possible. Crews' personal devices should be connected to a separate network to the vessels to reduce the risk of an attack to the critical underlying network of the vessel. Attackers may attempt to access onboard systems through the weakest vulnerability loopholes which is often a third-party application where there are known security vulnerabilities.

10. Protect

Use an authorised ENC distributor where data contains certificates – When receiving data via a network it's important to use a data provider who adds signatures to their data. Data containing a signature prevents a malicious actor modifying an original file via its transfer into the vessels ECDIS. If the ECDIS can't validate the signature file, it will prevent it being loaded into the ECDIS which significantly reduces the chance of a malicious attack on your systems. Some data producers make their ENCs available for free such as NOAA however it may be prudent to source these ENCs via a data server where signatures are provided.

Using an ENC distributor to provide ENCs over a network can also reduce the cyber security risk due to their ability to pre validate the data that is sent. Distributor systems can scan content for any malicious files or for suspicious content that could present a risk to your networked ECDIS. Having a distributor in the data transfer flowline to the ECDIS adds another layer of resilience and provides a point of contact for any questions or concerns with the data that's been sent.

Develop a contingency plan – Develop an incident response plan should a cyber attack on the vessels network or ECDIS occur. This response plan should contain checklists of practical actions the crew can take to detect, respond and limit the consequences of cyber incidents. The plan can help inform the crew of how to implement breakpoints of compromised equipment, prioritised response options, detect signs of what to look for when being attacked and how to carry on operating during an attack without using infected networks or hardware.

11. Detect

Check URL and network addresses of data sender / white list – If your ECDIS is connected via a network ensure you whitelist the connection URL, so your ECDIS trusts only that network path. Where possible the network should be configured so only trusted data sources can have access to the network. Ensure network addresses are constantly reviewed and validated with your data provider should a new or modification to an existing network address be required.

ECDIS behaviour abnormalities present - To help detect an attack on a networked ECDIS there are several symptoms you can look for.

1. Any screen flickering abnormalities or unresponsive user interfaces.
2. Does the system reboot without instruction, is the PCs temperature stable and is there abnormal system noise from fans and hard drives.
3. Is the ECDIS timing consistent with that of the GPS. An attacker could spoof your position using GPS timing or be sending the ECDIS incorrect packets of positional data from your GPS.
4. Monitor system performance and speed. If you experience a noticeable degradation of speed and system performance, then you could be under a cyber attack where malicious software is running in the background of the ECDIS.

If you notice one or more of these symptoms above, you should stop what you're doing, notify the master/crew of the vessel and take caution and ascertain if you're under attack before deciding to continue operation.

Check alerts and notifications from anti-virus regularly – Ensure your system integrator or shipping company keeps your antivirus software up to date. If the vessels type approved ECDIS can't run an antivirus, then ensure the back of bridge system or any other systems connected to the same network as the ECDIS utilise it.

Antivirus checks should be run frequently on the ships network, to a schedule and reviewed to heighten the chances of detecting and removing malicious files before they have a chance to spread and take effect.

How likely is your system to be infected based on network connectivity and amount of use? – When trying to detect a network based cyber-attack its prudent to constantly evaluate how much use the network has had and how much data has been ingested into the ECDIS. If frequential transfer of multiple files has occurred, there's a heightened risk of a cyber-attack. After heavy network use for a prolonged period, it would be wise to run a virus check or seek a professional system check by a system integrator of technician to run a health check on your system.

12. Respond

When responding to a cyber-attack ensure the master of the vessel and all crew members are informed and the incident is logged in the vessels SMS. Enact the contingency plan and ensure all crew members are safe from any immediate threats. Where the vessels ECDIS could be compromised and misleading the navigator you could add an extra watch to the vessel to ensure the vessel stays clear or potential dangers and other vessel traffic.

When its safe to do so are where possible use the redundant navigation system such as a secondary ECDIS or paper chart to base navigational decisions off. Whilst under a cyber-attack try to obtain evidence of the observed behaviours an abnormality via system screenshots or via phones.

Whilst under an attack contact the coastal authority for the area, your shipping company and distributor of the vessels data. By informing all parties the coastal authority can forewarn vessels in the area via radio warnings and maybe able to aid protect the vessel and ensure it stays safe. Whilst trying to resolve the threat record all operations carried out and any observations documented. If all attempts to overcome the attack on the network have failed, then it might be applicable to disconnect all systems from the compromised network. Throughout the attack ensure all vessel crew are kept informed of developments and decisions made.

13. Recover

When it's safe to do so and your confident your network has been attacked then you'll need to safely navigate to port for your systems to be cleaned of the cyber threat/virus.

When making your way to the nearest port its important to do so by enacting your contingency plan and using backup ECDIS or hardware you can be assured have not been compromised. Once in port the vessel will need to contact the ECDIS OEM, the system integrator and vessel technicians to analyse the network and connected systems to remove the malicious files and address the underlying vulnerability.

Where applicable it might be required to completely uninstall operating software and applications connected to the network to ensure no vulnerabilities or attack vectors remain.

Whilst the systems and ECDIS are restored it should be retuned to a safe working state by the OEM or system integrator. Where vulnerabilities or threats are discovered by poor vessel practice these should be shared with the crew and addressed before onward navigation.

Once the incident has been resolved evaluate what went well and where improvements are required in the contingency plans. Ensure the incident is recorded in the vessels SMS and all experience is documented for use in future incidents.

Checklist for the creation of a response plan for an ECDIS using USB or Physical Media

Actions/Mitigations General	Signed	Approved
Use an approved ENC chart distributor that uses either the IHO data protection scheme S-63 or a type approved SENC delivery method to secure the data.		
Ensure crew have adequate access to cyber security training		
Change onboard default equipment and software passwords regularly		
Install virus checking software onboard		
Ensure virus checking software is kept up to date with the latest software releases		
Be vigilant of spam emails and attached files.		
Actions/Mitigations USB	**Signed**	**Approved**
When removable USB devices are to be used to transfer the digital files from a communication PC to the ECDIS they should be scanned for viruses		
Use only dedicated removable media (USB stick) to download and transfer ENC data and permits to ECDIS		
Clearly label the USB device to clearly mark it as dedicated to the transfer of ENC data and permits.		
Do no use this item for anything else than data download / import to ECDIS.		
Do not store digital files on this device.		
Do not leave removable media unattended.		
Reformat USB after use		
After using the USB, store it in safe place where only authorized personnel have access		
Actions/Mitigations ECDIS	**Signed**	**Approved**
Before transferring data to the ECDIS via USB pun permits and ENC data through anti-virus and anti-malware tools		
Do no not allow crew's personal devices to be connected to ECDIS		
Keep ECDIS updated to latest IHO standards		
Keep ECDIS updated for the latest software releases as recommended by the ECDIS manufacturer		

Checklist for the creation of a response plan for a networked ECDIS

(majority of actions are performed by the system integrator or shipping company. We need to add some wording to split these out accordingly, highlighting the difference.)

Action	Signed	Approved	Date Last Assessed
Create an inventory of the hardware, software networks and connections of the vessels systems to expose any vulnerabilities.			
Change network Passwords/authentication			

credentials onboard regularly.			
Ensure your Shipping Company or system integrator installs firewalls and virus checking software onboard across the networks.			
Ensure your Shipping Company or system integrator checks software is kept up to date with the latest software releases.			
Ensure your Shipping Company or system integrator installs networks that are segmented and air gaped where possible from one another.			
Ensure your Shipping Company or system integrator has the vessels ECDIS only connected to external networks via a 460-Gateay or 460 Wireless Gateway and is utilising DMZs in front of your ECDIS network to minimise threat vector.			
Ensure your Shipping Company or system integrator has configured your network so all other systems running on the same ECDIS network are connected via 460 switches and forwarders.			
Install intrusion prevention systems and monitor network traffic for abnormalities.			
Networks and ports are designated for certain essential activity only.			
Access to network ports are digitally or physically secured to certain personnel only.			
Implement access controls, multifactor authentication and user groups on the networks to control use and functionality.			

A separate isolated network is used for personal use to external network (internet).			
Network paths and configurations are backed up regularly in a secure location.			
Allowable Network paths are whitelisted to the ECDIS.			
Network connections are automatically closed after being idle for an amount of time.			
If ECDIS is connected to the communication PC via a firewall make sure the hardware is running the latest software version from your provider			
Map remote accesses and data flows.