**Paper for Consideration by HSSC 13**

**S-63 Cyber Security Report ENCWG**

|  |  |
| --- | --- |
| ***Submitted by:*** | T. Mellor, ENCWG Chair |
| ***Executive Summary:*** | Recommendation to create a new IHO ECDIS cyber security guideline |
| ***Related Documents:*** | IHO S-63 Data Protection Scheme |
| ***Related Projects:*** | NA |

**Introduction / Background**

1. HSSC tasked the ENCWG to investigate the issues raised by IEC regarding ENC authentication in ECDIS and provide a detailed analysis of the cyber risks associated to ECDIS and possible mitigations through IHO standards (Actions HSSC10/54, HSSC11/70 and HSSC12/22).
2. The IHO S-63 Standard was developed for encrypting, securing and compressing electronic navigational chart (ENC) data. It was first released in December 2002, and was based on the data distribution requirement, as they existed at that time.
3. There are several files within an IHO S-63 edition 1.2 encrypted ENC exchange set that currently carry no digital signatures for the purpose of authentication by data clients. These are:

• Auxiliary text and picture files (.TXT and .TIF)

• CATALOG.031

• README.TXT

• PRODUCTS.TXT

• MEDIA.TXT

• SERIAL.ENC

• STATUS.LST

1. The lack of authentication on these files is acknowledged as a possible weakness in the ENC supply chain which has the potential to be exploited by cyber criminals. For example, a fake CATALOG.031 file could be used to cause the cancellation and removal of ENC charts from onboard navigation equipment; or the fake contents of auxiliary text and picture files could cause serious mistakes in route planning, etc.
2. In response to the increased threat of cyber-attacks on shipping the International Maritime Organization (IMO) issued Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3 - 5th July 2017) and updated Resolution MSC.428(98) – 16th June 2017 to now include a new section on Maritime Cyber Risk Management in Safety Management Systems. In practice this means that by the first annual verification of a shipping company’s document of compliance after 1st January 2021, a cyber risk assessment must have been conducted and measures taken to protect the vessel from cyber-attacks.
3. The delivery of encrypted ENC data with metadata files carrying no authentication measures may present a problem for OEMs and shipping companies that want systems which comply with the future IEC standard IEC63154 ED1 – *Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results*.

**Analysis/Discussion**

1. There are four primary stakeholder groups effected by the proposed change detailed below:
2. IHO appointed Data Servers;
3. ECDIS OEMs;
4. ENC distributors; and
5. Shipping Companies (ECDIS Owners).

There is no direct impact on Hydrographic Offices.

**ENCWG - A Technical Solution**

1. To address the issue the ENCWG developed a technical proposal to digitally sign all the files listed in paragraph 3 above. This fix would be applied to S-63 and would impact Data Servers, ENC distributors, OEMs and ECDIS users.
2. A new S63\_SIGNATURES.XML file may be created to reside within the INFO folder of an S-63 exchange set. The file will hold digital signatures for all ENC data and all the associated meta data files within the exchange set being transferred.
3. The objective of the described proposal:

• Introduce digital signatures on all ENC files within an exchange set to reduce the cyber risk during transit to the end-user.

• Ensure the proposed method works on all existing OEM ECDIS systems without any operational issues; and also that it is workable on any OEM system which has developed support for the additional S-63 digital signature encoding within an S-63 ENC exchange set.

1. Whilst the technical solution presents a very good way to mitigate the risks there are other more manual procedural based methods which could achieve the same result which as of yet have not been considered by the ENCWG.

**Test Data**

1. To support a detailed assessment of the proposal by ECDIS manufacturers and Data Servers a set of test data based on the proposal was created and sent along with a questionnaire to capture respondent’s views. The information was sent to all members of the IHO S-63 Security Scheme and the CIRM Chief Technical Officer on 29th Nov 2020 with all responses to be received at the IHO by 29th Jan 2021.

**Survey**

1. The survey of S-63 Scheme members highlighted an issue with old, incorrect, or out of date contact information held at the IHO as many emails failed to deliver. IHO have attempted to establish contacts with these companies and ENCWG members are also assisting with this activity.
2. Of the 369 registered IHO Security Scheme participants, many members are not making commercially available systems and where ECDIS is being manufactured many are using a commercially available kernel.
3. Even taking this factor into account the number of results received from individual OEMs is disappointing. However, I have been able to discuss this issue and the proposal at length with the CIRM ECDIS WG and they have provided a consolidated response (Annex A).
4. To date the IHO have received sixteen responses from OEMs and ten responses from Data Servers.

**Results and Observations**

1. There has been a mixed response to the survey, but most OEMs seem to acknowledge that the proposed solution developed by the ENCWG would prove effective in addressing the vulnerability and be technically feasible to implement if necessary.
2. It must be stressed that currently only a small amount of ENC data is distributed to vessels via registered IHO Data Servers. The majority of ENC data is disseminated through resellers that receive ENC data from Data Servers and using their own back of bridge software to build vessel specific bespoke exchange sets based on their individual requirements, thus adding significant value in the supply chain.
3. From comments received from CIRM there is a reluctance to invest in a full-scale technical solution when the risk to ECDIS is small and with S-100 ECDIS transition on the horizon.
4. A concern of many respondents is how the technical solution would be introduced; would it be a full new edition of S-63 which would require new ECDIS type approval and ECDIS upgrades across the entire SOLAS fleet. Such a solution would also necessitate ENC distributor software upgrades to all back of bridge software without any financial gain for implementation. CIRM members are concerned this has potential to cause confusion in the market and ill-feeling on the part of the shipping industry, if manufacturers were to promote the need for customers to update existing ECDIS to address the S-63 vulnerability, and then shortly after (in relative terms) promote the need for those customers to upgrade their systems to S-100 ECDIS.
5. Alternatively a minor clarification to S-63, making the proposal optional for data servers and OEMs to implement, may not be universally adopted.
6. A technical solution to solving this issue would be preferable, however the cyber threat may also be reduced through good bridge team policies and a set of IHO approved cyber security procedures.

**Options**

|  |  |
| --- | --- |
| **Proposal 1** | No changes to IHO standards, create a new IHO ECDIS Cyber Security Guideline. |
| Description | No modification to current IHO standards S-63, S-64. |
| Risk | Based on current understanding the risk that an unsigned ENC meta file creates a significant cyber risk is considered low. |
| Considerations | No impact on shipping industry, issue will be addressed by S-100. Manage risk through bridge procedures in the interim period. |
| Benefit | Can be implemented quickly without significant delay. |
| Financial | No financial impact on any stakeholders. |

|  |  |
| --- | --- |
| **Proposal 2** | IHO S-63 Clarification new Informative Annex. |
| Description | New annex to S-63 with proposal for Data servers to sign all the files within an exchange set and the technical implementation required by OEMs to read new file. |
| Risk | Not mandatory to implement; may not be supported in ECDIS for years, if at all. |
| Considerations | Data Servers must upgrade production software to sign all ENC files and create new exchange sets.  ENC distributors will have to register to be IHO Data Servers within the IHO security scheme. Potentially 100 new applicants.  ENC distributors back of bridge software upgraded to digitally sign data sets on board a vessel; this is not recommended as it would greatly increases the risk of private key compromise.  Clarification of S-64 required to include new test data based on proposal.  OEMs must implement clarification for it to be effective.  Does not mitigate supply of unencrypted ENC exchange sets. |
| Benefit | Backwards compatible solution – would not affect existing ECDIS.  Data Servers could create new digitally signed exchange sets and send them to all ECDIS irrespective of age without any adverse effects. |
| Financial | No additional revenue from ENC sales to support this activity.  Data Server – create new signing service.  OEM – implement code fix to read new file, distribute software upgrades.  ENC Distributor - implement code fix to read new file, distribute software upgrades.  Shipping Company – ECDIS software must be upgraded to benefit from new signed data. If visit to vessel is required, this will incur significant cost. |

|  |  |
| --- | --- |
| **Proposal 3** | IHO S-63 New Edition. |
| Description | New Edition S-63 Data Servers must sign all the files within an ENC exchange set, technical implementation required by OEMs to read new signatures file. |
| Considerations | ENC distributors have to register to be Data Servers within the IHO security scheme. Potentially 100 new applicants.  ENC distributors back of bridge software upgraded to digitally sign data sets on board a vessel; this is not recommended as it would greatly increases the risk of private key compromise.  OEMs must implement new edition.  All ECDIS software across entire SOLAS fleet must be upgraded to comply with new edition of S-63.  New Type Approval of ECDIS.  New edition of S-64 to include new test data based on proposal.  Significant time required to implement fix.  Does not mitigate supply of unencrypted ENC exchange sets. |
| Financial | No additional revenue from ENC sales to support this activity.  Data Server – create new signing service.  OEM – implement code fix to read new file, distribute software upgrades.  ENC Distributor - implement code fix to read new file, distribute software upgrades.  Shipping Company – ECDIS software must be upgraded to comply with the standard in accordance with IMO regulations and benefit from new signed data. If visit to vessel is required, this will incur significant cost. |

**Recommendation**

1. Comparing the three options and in consideration of the valuable comments received from CIRM, it is the recommendation of the ENCWG to consider Option 1 “*No changes to IHO standards, create a new IHO ECDIS Cyber Security Guideline”* and that a new IHO ECDIS Cyber Security Guideline be developed to address the ENC issues identified and to offer best practice guidance in dealing with cyber threats related to ENC data and ECDIS.

**Justifica**t**ion and Impacts**

1. The impact of making any change to S-63 at this stage in its life cycle would cause significant cost and disruption to the shipping industry for an issue which had a very low risk associated. S-100 encryption will address this issue and given the problem can be mitigated in the short term by manual processes this would be the most pragmatic solution. All other alternatives would incur cost to every stakeholder at a time when we are seeking investment in development of S-100.

**Action Required of [HSSC] [Relevant HSSC WG]**

1. The HSSC is invited to:

a. endorse the proposal to create an IHO ECDIS cyber security guideline

b. agree that no new edition to S-63 will be issued