

## **IHO RECOMMENDED SECURITY SCHEME FOR ENC**

Reference: IHB Circular Letter 44/2002, dated 1 October 2002.

Dear Hydrographer,

CL 44/2002 requested Member States to approve the adoption of Version 1 of an IHO Recommended Security Scheme for ENC, the transfer of the role of Security Scheme Administrator to the IHB, and commencement of the development of Version 2 of the Scheme as soon as feasible.

The IHB thanks the 44 Member States who responded. The responses are summarized in the table in Annex A and Member States' comments are also included. Results of the vote are as follows:

1. To the question "*Do you approve the adoption of Version 1 of an IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme?*" 41 MS replied 'Yes';
2. To the question "*Do you agree that the role of Security Scheme Administrator be transferred to the IHB*" 44 MS replied 'Yes';
3. To the question "*Do you support that the development of Version 2 of an IHO Recommended Security Scheme be initiated as soon as feasible?*" 40 MS replied 'Yes'.

As of the date of CL 44/2002, there were 73 IHO MS, of which 70 were entitled to vote. Therefore, the simple majority required in this case (refer to: Article VI, Paragraph 6 of the IHO Convention) was therefore 36. As a result:

- Version 1 of the IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme is adopted;
- Transfer to the IHB of the role as Security Scheme Administrator is agreed; and
- Development of Version 2 of an IHO Recommended Security Scheme can be initiated as soon as feasible.

As regards the implementation plan for Version 1 of the RSS, as outlined in the schedule included in the DPSAG<sup>1</sup> report to the 14<sup>th</sup> CHRIS<sup>2</sup> Meeting (Document CHRIS-14-8A, available from [www.iho.shom.fr/general/ecdis/ecdisnew1.html](http://www.iho.shom.fr/general/ecdis/ecdisnew1.html)), the temporary unavailability of a key person at Primar Stavanger has entailed a slight shift in the various implementation steps. The IHB has checked with the Chair of DPSAG, Mr Robert Sandvik (Primar Stavanger), that plans are now as follows:

- Date for submission, by Primar Stavanger, of the security scheme to the IHB: 3 February 2003;

---

<sup>1</sup> Data Protection Scheme Advisory Group [now a sub-group of the Technology Assessment Working Group (of CHRIS)].

<sup>2</sup> Committee on Hydrographic Requirements for Information Systems.

- Date of actual roll-over of Scheme Administrator role from Primar Stavanger to the IHB: 12 March 2003;
- Date for Version 1 of the IHO Recommended Security Scheme coming into force: 12 March 2003.

Training of IHB staff by Primar Stavanger on security scheme management has been planned on 10-12 March 2003. It is intended to also organize a DPSAG meeting on 13-14 March, i.e. immediately after that training session. The main purpose of this meeting would be to address any issues/problems relating to the implementation of Version 1 and to initiate the development of Version 2, based on the schedule included in Document CHRIS-14-8A. In particular, it will be necessary to review the various steps in the development plan for Version 2 and, for each step, to identify the appropriate means to achieve and fund the relevant task(s).

It is hoped that the above explanations will satisfy, at least partly, the concerns expressed by some Member States in their comments as reported in Annex A. The Directing Committee reiterates its appreciation to the Norwegian Hydrographic Office and PRIMAR Stavanger for making the Primar security scheme available to the IHO. We would also like to express our thanks to the Canadian Hydrographic Service for providing the security scheme software kernel that has been developed by the CHS.

On behalf of the Directing Committee  
Yours sincerely,

*(original signed)*

Rear Admiral Kenneth BARBOR  
Director

Encl: Annex A

**IHO RECOMMENDED SCHEME FOR ENC  
Responses to CL 44/2002**

Member State	Question 1 <sup>(*)</sup>	Question 2 <sup>(**)</sup>	Question 3 <sup>(***)</sup>	Comments
Argentina	Yes	Yes	Yes	
Australia	Yes	Yes	Yes	
Bahrain	Yes	Yes	Yes	
Bangladesh	Yes	Yes	Yes	
Brazil	Yes	Yes	Yes	
Canada	Yes	Yes	Yes	<p>1. All Member States have not indicated they wish to have their ENC data encrypted. Canada, for example, has no plans to implement encryption at this time. Canada's role in the Data Protection and Security Advisory Group (DPSAG) should not be interpreted as an endorsement of encryption for S-57 data, but rather as an effort to promote standards-based interoperability, among countries who do wish to implement encryption.</p> <p>2. The DPSAG, to the best of our knowledge, has not reported that there are no technical implications to the IHO becoming Scheme Administrator (SA). On the contrary, the DSPAG feels that there is a significant amount of work to be done. Specifically software will have to be written and IHO staff trained in its use. It is unclear at this time who will be writing this software or providing the required training. Further to this, it is felt by the DPSAG that, in the short term at least, the IHO can only become the SA in name, and that PRIMAR will have to continue to perform the real SA duties.</p> <p>3. Finally, the IHO Security Scheme Version 1 (IHOSV1) is not complete as the CL states. The software kernel is still being written and the supporting documentation is still being edited and reviewed. Substantial effort is still required to finish this work. Transferring the SA responsibility to the IHO should not occur until this work is completed.</p> <p>However, Canada remains committed to the PRIMAR Security Scheme as the basis for an interim security standard. We also agree with necessity for the IHO to eventually become its SA. Finally we feel that the development of a second, standards-based final security model is also necessary.</p>
Chile	Yes	Yes	No	The PRIMAR Security Scheme seems to be very complicated. So, before initiating a new version, it would be useful to know the experience of those countries who have started using it. Only then, bearing in mind the experience gained, would it be reasonable to develop a new version.
China	Yes	Yes	Yes	

<sup>(\*)</sup> Do you approve the adoption of Version 1 of an IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme?

<sup>(\*\*)</sup> Do you agree that the role as Security Scheme Administrator be transferred to the IHB?

<sup>(\*\*\*)</sup> Do you support that the development of Version 2 of an IHO Recommended Security Scheme be initiated as soon as feasible?

Member State	Question 1 <sup>(*)</sup>	Question 2 <sup>(**)</sup>	Question 3 <sup>(***)</sup>	Comments
Colombia	Yes	Yes	Yes	The Hydrographic Office of Colombia agrees, provided that the ENC Safety System is developed and managed by the IHB. Once this scheme is implemented, disseminated and made known, each HO can decide whether to use it or not.
Croatia	Yes	Yes	Yes	
Cuba	Yes	Yes	Yes	
Cyprus	Yes	Yes	Yes	
Denmark	Yes	Yes	Yes	
Estonia	Yes	Yes	Yes	
Finland	Yes	Yes	Yes	Finland strongly supports the IHO having one single Recommended Security Scheme for ENC.
France	Yes	Yes	Yes	France remarks that the sharing of responsibilities between IHO and IMO on certifying the systems used to disseminate digital information related to safety of navigation is still dangerously not sufficiently defined.
Germany	Yes	Yes	Yes	Approval of IHB to be the administrator is subject to the condition that the efforts at IHB to administer the Security Scheme do not exceed the level of two person weeks per year, as stated in CL 44/2002. The IHB is requested to routinely ascertain the actual level of efforts.
Greece	Yes	Yes	Yes	
Guatemala	Yes	Yes	Yes	
India	Yes	Yes	Yes	The IHO Security System should include the data encryption, data authentication and selective access to ENC data.
Italy	No	Yes	Yes	The Italian Hydrographic Office consider more appropriate the direct adoption of Version 2 of the recommended Security Scheme for ENC, in order to avoid the implementation of two different R.S.S. in a short period of time.
Korea (Rep. of)	Yes	Yes	Yes	
Kuwait	Yes	Yes	Yes	
Malaysia	No	Yes	Yes	It is believed that the best security scheme currently available is the PRIMAR Security Scheme. However, in the future, there may be better scheme made available by other bodies which should be considered. The RSS should be reviewed comparatively from time to time.
Mexico	Yes	Yes	No	It is necessary to know the advantages of Version 1 and whether it has deficiencies before developing a new version.
Monaco	Yes	Yes	Yes	

<sup>(\*)</sup> Do you approve the adoption of Version 1 of an IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme?

<sup>(\*\*)</sup> Do you agree that the role as Security Scheme Administrator be transferred to the IHB?

<sup>(\*\*\*)</sup> Do you support that the development of Version 2 of an IHO Recommended Security Scheme be initiated as soon as feasible?

Member State	Question 1 <sup>(*)</sup>	Question 2 <sup>(**)</sup>	Question 3 <sup>(***)</sup>	Comments
Mozambique	Yes	Yes	Yes	
Netherlands	Yes	Yes	Yes	
New Zealand	Yes	Yes	Yes	Whilst New Zealand will not be encrypting its ENC data we support the adoption of a single security scheme, administered by the IHB, for those Member States who are required to encrypt their data.
Norway	Yes	Yes	Yes	
Oman	Yes	Yes	Yes	
Pakistan	Yes	Yes	Yes	Version 2 of IHO RSS should be adopted after the implementation and recommendation of users and producers of ENC.
Peru	Yes	Yes	Yes	<ol style="list-style-type: none"> <li>1. We think that this Safety Scheme is most welcome and its present implementation meets the requirements of the Hydrographic Offices, namely of those which, having already developed the Electronic Navigational Charts, are restricted as to their distribution and commercial sale, specifically due to the lack of a standardized safety system. This is a step forward and will facilitate the distribution and commercialisation of the ENC data available.</li> <li>2. In addition, it is recommended that the officially established RENCs are the best placed through their distributors' network, to use the standardized Safety System, avoiding thus the use of other Safety Systems or non official or exclusive encoding algorithms, which could result in complications in the use of ECDIS.</li> </ol>
Portugal	Yes	Yes	Abstain	The IHPT would like to know who is going to develop the IHO RSS Version 2, what are the costs and who will pay them. Without this data it is difficult to provide an answer to this question.
Singapore	Yes	Yes	Yes	Our support for the adoption of Version 1 is only on condition that IHB would be the Security Scheme Administrator.
Slovenia	Yes	Yes	Yes	Slovenia supports the coordinating role of IHB and the adoption of single standard for Security Scheme which should be as simple as possible and consistent with International Data Security Standards. IHB should also find a way to make the Security Scheme economically affordable and accessible for HOs with less experience on ENCs and with minor ENC portfolio.
South Africa	Yes	Yes	Yes	
Spain	Yes	Yes	Yes	The Security Scheme for ENC must be a standard. The establishment and management of standards must be one of the main missions of the Organization.

<sup>(\*)</sup> Do you approve the adoption of Version 1 of an IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme?

<sup>(\*\*)</sup> Do you agree that the role as Security Scheme Administrator be transferred to the IHB?

<sup>(\*\*\*)</sup> Do you support that the development of Version 2 of an IHO Recommended Security Scheme be initiated as soon as feasible?

Member State	Question 1 <sup>(*)</sup>	Question 2 <sup>(**)</sup>	Question 3 <sup>(***)</sup>	Comments
Sweden	Yes	Yes	Yes	
Thailand	Yes	Yes	No	IHO RSS Version 1 should be used for some time. If it contains some errors, the corrections can be incorporated in Version 2. Security Schemes should not be changed very frequently because this causes some problems.
Tunisia	Yes	Yes	Yes	The Tunisian Hydrographic Service (THOS) believes that such kind of recommended Security Scheme will provide more protection for ENC's.
Turkey	Yes	Yes	Yes	
Ukraine	No	Yes	Yes	We consider that it is preferable to skip Version 1 and to go directly to Version 2 in order to avoid creating two different protection schemes over a 2-3 year period of time, which means extra costs in development, production, etc. Version 2 should be developed then verified by all interested parties: data producers, Hydrographic Offices, end users, RENC, etc.
UK	Yes	Yes	Yes	<ol style="list-style-type: none"> <li>1. A prerequisite to the transfer of the Version 1 of the scheme from PRIMAR to the IHO is the successful review and passing of all documentation, source code, test data and any updates by the DPSAG.</li> <li>2. Our understanding is that successful implementation of Version 1 of the scheme by all OEMs is also a prerequisite.</li> <li>3. The UKHO fully supports the adoption of the scheme by the IHO and is working as part of the DPSAG to ensure the transfer is both smooth and timely.</li> </ol>
<b>RESULTS</b> (44 voting MS)	Yes: 41 No: 3 Abstain: 0	Yes: 44 No: 0 Abstain: 0	Yes: 40 No: 3 Abstain: 1	<p><b>IHB Comment:</b> As of the date of CL 44/2002 (1st October 2002), there were 73 IHO MS, of which 70 were entitled to vote. The simple majority, which was required in this case (re: Article VI, Paragraph 6 of the IHO Convention), was therefore 36. As a result:</p> <ul style="list-style-type: none"> <li>• Version 1 of the IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme is adopted;</li> <li>• Transfer to the IHB of the role as Security Scheme Administrator is agreed; and</li> <li>• Development of Version 2 of an IHO Recommended Security Scheme can be initiated as soon as feasible.</li> </ul>

<sup>(\*)</sup> Do you approve the adoption of Version 1 of an IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme?

<sup>(\*\*)</sup> Do you agree that the role as Security Scheme Administrator be transferred to the IHB?

<sup>(\*\*\*)</sup> Do you support that the development of Version 2 of an IHO Recommended Security Scheme be initiated as soon as feasible?