

**THIS CIRCULAR LETTER REQUIRES YOU TO VOTE**

**IHB File No. S3/8151/CHRIS**

**CIRCULAR LETTER No. 44/2002  
1 October 2002**

**IHO RECOMMENDED SECURITY SCHEME FOR ENC**

- References:
- 1) IHB Circular Letter 38/2000, dated 5 September 2000
  - 2) IHB Circular Letter 15/2001 Rev.1, dated 15 March 2001
  - 3) CHRIS Letter 1/2002, dated 1st February 2002

Dear Sir,

This CL requests you to approve the adoption of Version 1 of an IHO ENC Security Scheme and the transfer of the role as Security Scheme Administrator to the IHB.

Circular Letter 38/2000 polled Member States on their views on developing a single IHO Recommended Security Scheme (RSS). Responses were reported in CL 15/2001 Rev.1. All Member States responding (31) wished to have their ENC data encrypted and a large majority of the Member States (26) agreed that IHO should adopt a single RSS. The only Security Scheme ready to be used at that time was the Primar Security Scheme, and a majority (17) of the Member States responding agreed that the Primar Security Scheme should be adopted as the IHO RSS.

CHRIS, at its 13<sup>th</sup> meeting (Athens, Greece, September 2001), revisited the issue of a RSS and agreed that a small advisory expert group investigate the implications of IHB becoming the security scheme administrator for a RSS and assuming responsibility for the maintenance of a RSS.

The advisory expert group, named Data Protection Scheme Advisory Group (DPSAG), reported back to the IHB in January 2002 that there were no technical implications to the IHB becoming the security scheme administrator and that the level of effort to administer the security scheme would involve approximately two man-weeks per year. The DPSAG provided a plan to develop an IHO RSS Version 1. By way of reference (3), the IHB sought the opinion of the CHRIS Members who endorsed the plan put forward by the DPSAG.

The advisory expert group was then tasked to develop a Version 1 of an IHO RSS based on the Primar Security Scheme. The Primar Security Scheme was chosen as the basis for the following reasons:

1. it is the de facto standard for ENC protection;
2. the majority of ECDIS and ECS manufacturers have already developed the necessary decryption facilities in their systems. A change would mean extra costs for the manufacturers with little, if any, added benefits.

A Version 1 of an IHO RSS with all necessary supporting documentation has now been developed and is ready to be transferred to the IHB giving the IHB the control of the security system on behalf of the

Member States. The formal transfer can be put into effect by 1st January 2003, with the necessary training of IHB Staff being completed by the end of the first quarter of 2003. The additional two man-weeks of effort can be accommodated within the resources of the IHB. This is reflected in the DPSAG report to the 14<sup>th</sup> CHRIS Meeting (Shanghai, China, August 2002), which is available from the IHO website ([www.iho.shom.fr/general/ecdis/ecdisnew1.html](http://www.iho.shom.fr/general/ecdis/ecdisnew1.html))<sup>1</sup>.

You are kindly requested to approve the adoption of Version 1 of an IHO Security Scheme and the transfer of the role as Security Scheme Administrator to the IHB. Additionally, the advisory expert group has drafted a plan for development of an IHO RSS Version 2 that can be put into effect if and when directed by the Member States and you are requested to approve the start of this development. CHRIS, at its 14<sup>th</sup> Meeting, supported the above proposals. Please indicate your response by completing the attached voting paper and returning it to the IHB before 1 November 2002.

The Directing Committee appreciates the generosity of the Norwegian Hydrographic Office and PRIMAR Stavanger for providing this security scheme Version 1 free of charge and the efforts of the advisory expert group in studying the implication and recommending a way ahead.

On behalf of the Directing Committee  
Yours sincerely,

*(original signed)*

Rear Admiral Kenneth BARBOR  
Director

---

<sup>1</sup> Relevant document is CHRIS-14-8A (PDF file) on the CHRIS Web page.

**IHO RECOMMENDED SECURITY SCHEME FOR ENC**

**Questionnaire / Voting Paper**

*[to be returned to the IHB by 1st November 2002*

*E-mail: [info@ihb.mc](mailto:info@ihb.mc) - Fax: +377 93 10 81 40]*

**Member State:** .....

1) Do you approve the adoption of Version 1 of an IHO Recommended Security Scheme for ENC, based on the Primar Security Scheme?

YES

NO

2) Do you agree that the role as Security Scheme Administrator be transferred to the IHB?

YES

NO

3) Do you support that the development of Version 2 of an IHO Recommended Security Scheme be initiated as soon as feasible?

YES

NO

Comments: .....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Name / Signature ..... Date: .....