12th CHRIS MEETING
Valparaiso, Chile, 23-25 October 2000

POLLING IHO MEMBER STATES ON ENC SECURITY SCHEME(S)

Responses to IHB CL 38/2000

(Status as of 18 November 2000)

On 5 September 2000, the IHB polled the IHO Member States on the subject of security scheme / encryption of ENC's, through Circular Letter 38/2000. Excerpt of this CL, signed by RAdm Neil Guy, is reproduced below.

"*The attention of Member States is drawn to CL 40/1999 dealing with the above subject. Since the issuing of this letter, several Member States have expressed concern about the release of their data without security. This has been reflected in national reports to past CHRIS and WEND meetings, e.g. from Australia, India, Malaysia and Russia, as contained in Document WEND/5/6A available on the IHO website (www.iho.shom.fr - Member States only). Additional requests have been received from industry requesting clarification on the intended IHO approach to the encryption of ENC data.*

The issue of security scheme(s) was addressed at the 11th CHRIS Meeting, November 1999, and then at the 5th WEND Meeting, March 2000. At the CHRIS Meeting, the majority felt that encryption was desirable. It was further agreed that, should encryption be introduced, it should be standardized, that IHO will eventually need to establish a position on this matter, and that a policy should be adopted before technical details can be decided upon (see IHB CL 3/2000). At the WEND Meeting, the European RENC PRIMAR indicated that the security scheme that they were using (i.e. an encryption algorithm known as "BLOWFISH" and several proprietary encryption protocols) would be made publicly available to those HOs desiring to adopt their scheme (see IHB CL 23/2000).

The security scheme used by PRIMAR, primarily intended for providing data authentication and for protecting the ENC data from unauthorized copying, use, or alteration, is described in Annex A. In particular, attention is drawn to paragraph 5.3 which details a possible method whereby the IHO could assume responsibility for the scheme and paragraph 4 which provides details on how to actually make use of this security scheme.

It has been reported that PRIMAR Security Scheme is at present being implemented or being developed by more than 10 ECDIS or ECS manufacturers."

Description of the security scheme used by PRIMAR (Annex A of CL 38/2000) is contained in Document CHRIS/12/9.1B "PRIMAR Security Scheme Outline". Member States were requested to respond, by 15 October 2000 so as to be able to report on the matter to the 12th CHRIS Meeting, to the following three questions (Yes/No):

1) Is it your intention to have your ENC data supplied in an encrypted format, e.g. directly or through a RENC?

2) If the answer is "YES" to Question 1), do you agree that there should be one IHO Recommended Security Scheme?

3) If the answer is "YES" to Questions 1) & 2), do you agree that the Security Scheme presently employed by PRIMAR, as described in Annex A, should become the IHO Recommended Security Scheme?

As of 18 November 2000, 31 IHO Member States had responded to CL 38. A summary of the replies received is at Annex 1. From this table it appears that, although all respondents said YES to the 1st question and a large majority (26) also said YES to the 2nd question, only seventeen (17) of them support the adoption of the PRIMAR Security Scheme as the IHO recommended security scheme, i.e. they clearly replied YES to the 3rd question. A number of comments have been further expressed, which can be found in Annex 2.

_____

Annex 1

ENC SECURITY SCHEMES
SUMMARY OF REPLIES TO IHB CL 38/2000

Country	**Is it your intention to have your ENC data supplied in an encrypted format, e.g. directly or through a RENC?**	**If the answer is "YES" to Question 1), do you agree that there should be one IHO Recommended Security Scheme?**	**If the answer is "YES" to Questions 1) & 2), do you agree that the Security Scheme presently employed by PRIMAR, as described in Annex A, should become the IHO Recommended Security Scheme?**
Argentina	Yes	Yes	Yes
Australia	Yes	Yes	No (comments)
Bahrain	Yes	Yes	Yes
Brazil	Yes	Yes	Yes (comments)
Canada	Yes	No	N.A. (comments)
Chile	Yes	Yes	No (comments)
China	Yes	Yes	Yes
Colombia	Yes	No	No vote
Denmark	Yes	Yes	Yes (comments)
Finland	Yes	Yes	Yes (comments)
France	Yes	Yes	No vote (comments)
Germany	Yes	Yes	Yes (comments)
Greece	Yes	Yes	Yes
Iceland	Yes	Yes	Yes
India	Yes	Yes	No (comments)
Japan	Yes	No	N.A. (comments)
Malaysia	Yes	Yes	Yes (comments)
Netherlands	Yes	Yes	Yes
New Zealand	Yes	Yes	No (comments)
Norway	Yes	No	N.A. (comments)
Pakistan	Yes	Yes	No vote (comments)
Peru	Yes	Yes	Yes (comments)
Portugal	Yes	Yes	No (comments)
Russia	Yes	Yes	Yes
Spain	Yes	Yes	Yes
Sweden	Yes	Yes	Yes (comments)
Tunisia	Yes	Yes	No vote (comments)
Turkey	Yes	Yes	No vote (comments)
United Kingdom	Yes	Yes	Yes (comments)
Uruguay	Yes	Yes	Yes
USA (NOAA & NIMA)	Yes	No	No (comments)
31 responses	**31 Yes**	**26 Yes** **5 No**	**17 Yes** **6 No** **3 N.A.** **5 No vote**

Annex 2

ENC SECURITY SCHEMES
IHB CL 38/2000 – Members States' Comments

ARGENTINA

No comments

AUSTRALIA

The PRIMAR security scheme may well exhibit all the desirable components of an IHO model, however it does not necessarily enjoy the level of industry support claimed in the supporting paper.

To impose the PRIMAR solution after only the limited involvement of those most affected is inappropriate. In keeping with recent discussions at the 2nd EIHC and subsequently at the TSMAD/C&SMWG Industry meeting, the IHO should try and confine itself to defining the requirements of a security regime, rather than proposing the solution.

Accordingly, ECDIS stakeholders, particularly ECDIS manufacturers, should now be invited to comment on a preferred method of achieving standardized security arrangements. This should be organized against a strict timetable. A decision must be reached well in advance of the introduction of the revised SOLAS V on 1 July 2002. Obviously, if industry is unable to come forward with suitable arrangements, then the PRIMAR model remains a fall back position.

BAHRAIN

No comments

BRAZIL

We see no reason for the development of another standard as this have been field tested and is under way to become an Industry Standard.

CANADA

1. Canada does not intend to implement an ENC Security System for at least two years.

2. We base this decision on the fact that we do not consider the security threat to be severe enough to warrant such a substantial investment in a protection system. In Canada we are confident that the commercial shipping industry will not be pirating ENC data nor knowingly use pirated data.

3. Furthermore we consider that as security technology rapidly evolves to meet the requirements of e-commerce and e-government, it is premature to settle on a standard which, over time, may prove to be non-standard vis-à-vis the rest of the world.

4. The government of Canada has declared that it will use the Public Key Infrastructure (PKI) approach to on-line access security with its citizens. PKI is an open standard being promoted by a number of nations for both e-Commerce and e-Government.

5. The use of ECDIS as the "heart and hub" of a marine electronic highway is a concept promoted by the Shipping Industry and rapidly gaining acceptance in Canada. In this vision the ECDIS will receive information from a wide variety of sources, only one of which is CHS. Other agencies supplying data also have security concerns but will be seeking a more global security system and not a piecemeal approach wherein each supplier provides its own security standard.

6. The candidate security system suggested in the CL has yet to be implemented at another RENC or HO. Canada has a project underway to determine the level of difficulty in implementing this approach. It is premature to judge the full cost of implementation but our initial investigation shows the task to be non-trivial and require extensive use of software engineers skilled in implementing security systems. This may be onerous for some HOs.

7. Having more that one approach to security will indeed make it more difficult for the systems manufacturers to implement. However this problem pales in comparison to the one they face daily - the paucity of official vector data. Systems suppliers currently base their marketing strategy on the flexibility of their system to adopt a variety of data standards and use terms such as dual-fuel, triple-fuel etc. to demonstrate the systems ability to adapt to whatever data is available. Having more that one security standard is a solvable problem.

CHILE

1. Of course, if we expect data pirating or a wicked intervention of a third party, our intention is to supply encoded ENC data. On another hand, if this is extremely bothersome and onerous, we are not going to encode the data, minimizing the interest of pirating, through the supply of data at a low cost, providing periodical publications which make obsolete the previous ENCs editions.

2. In the case of an encoding, our wish is to standardize it and that it be an IHO recommendation, as the only way of ensuring such a standardization.

3. The PRIMAR Security Scheme seems to us very complicate and it would be most convenient to know the experiences of the involved actors. We believe that the establishment of a unique administrator of the scheme is extremely convenient.

CHINA

No comments.

COLOMBIA

We do not recommend to establish security schemes through the IHO; these protection procedures are part of the autonomy of the HOs. If some of them wish to make it with PRIMAR, that’s fine; if they desire to create schemes, that’s also fine. The technology ends by prevailing itself, without needing any IHO recommendations. If the PRIMAR scheme is of worldwide scope, with general adherence to, it will end by prevailing without any IHO support. First impression is that PRIMAR scheme appears “bureaucratic”, that is why a much deeper analysis will be required in Colombia.

DENMARK

For the time being the change to a new one should be controlled and coordinated allowing industry sufficient time to prepare.

FINLAND

The Security Scheme of PRIMAR has been implemented for the ten co-operating Hydrographic Offices. The Security Scheme is now operational and proven to be feasible.

In the documentation enclosed with the CL 38/2000, there were no estimation of the actual workload of the Scheme Administrator. Thus it is difficult to estimate the resources needed at the IHB if the IHO takes the role of the Scheme Administrator. For the time being it may be feasible that the IHO contracts out the practical work of the Scheme Administrator to PRIMAR, ECC AS, or other publicly known and reliable organization. There may even be different organizations for different parts of the world.

FRANCE

As regards question 3, our reply is, a priori, positive, as the scheme currently used by PRIMAR appears to be satisfactory. However, it would be useful to have an independent technical opinion (from a CHRIS Working Group, for example) and above all to have more details as regards the practical arrangements for the transfer of the scheme administration which is briefly outlined in para. 5.3 of IHB CL 38/2000.

GERMANY

It is unfortunate that the issue of a standard IHO Security Scheme is put to a decision by IHO only a posteriori, after PRIMAR has adopted its system. Adopting now a potentially superior security scheme different from PRIMAR ‘s would, however, send a confusing and probably upsetting message to the industry which has partly already implemented the PRIMAR schema.

It should be noted that the “IHO Standard Security System” will be limited to ENCs only. Dual-fuel users (e.g. ENC supplemented with ARCS) data will continue having to employ two different security systems. This problem can only be overcome by promulgating ENCs through a SENC distribution system when data from multiple sources are integrated by a service provider for the particular ECDIS under a single (proprietary) security schema.

GREECE

No comments.

ICELAND

No comments.

INDIA

Whilst the security system employed by PRIMAR is appreciated, the IHO recommended security system should have inbuilt safety to protect the copyrights of producer nations/charting agencies to avoid any hijacking of the issue by a particular country/group of countries.

JAPAN

The Hydrographic Department of Japan (JHD) considers that an encryption system which is suitable for application to ENC for small craft and GIS should be examined. As techniques of encryption are not established and are developing rapidly, JHD is opposed to standardize the encryption methods.

MALAYSIA

PRIMAR security scheme to be adopted as an initial start, but can be reviewed later if necessary.

NETHERLANDS

No comments.

NEW ZEALAND

1. An ENC review is currently being undertaken to determine the needs of New Zealand's mariners, and to plan a strategic approach to production and distribution. We expect to commence distribution of ENC data in two years time.

2. New Zealand endorses the use of encryption in the production of ENC data for the following reasons:
   - As proof of authoritative data to the mariner, especially if in an IHO format;
   - To protect the integrity of the data; and
   - To provide a secure tracking system of users for updating purposes.

3. New Zealand believes that if encryption is a requirement then the approach should be standardized and produced by the IHO.

4. It is noted that the IHO has limited knowledge in this area and should obtain advice and guidance from Member States (producing ENC's) and industry partners (ECS manufacturers).
5. New Zealand does not believe that the PRIMAR scheme should be used. Other systems are available and a rigorous comparison needs to be made to find the best solution.

NORWAY

Comment No. 1

Every approach within this field should primarily be driven by objectives seeking increased safety for the user, better cost efficiency and improved overall characteristics/capability throughout the complete producer-distributor-user chain. Commercial constraints should be taken into consideration by IHO/HOs only if such constraints have no significant impact on these major objectives.

The NHS answer to Q1 is Yes, but the encryption scheme for Norwegian waters is limited to imposing a digital signature, i.e. highest priority is given to the first four objectives above. If the situation with respect to unauthorized copying, data piracy, commercial consequences, etc. is more difficult than now envisaged, this decision should be evaluated. Finally, we would like to emphasize the importance of confidence between all serious players operating within this field.

Comment No. 2

The NHS answer to Q2 is a this time No, the actual choice should be based on developments and trends in the market. Various alternative are available of which PRIMAR's solution is probably the most mature. For instance, the US alternative AES as described in the last document referred to above seems interesting and promising and it is premature to make a firm decision in this direction now. We recommend hover the IHB to closely follow the US development efforts.

PAKISTAN

The Security Scheme employed by PRIMAR seems suitable to adopt as standard. However, it is suggested that it may be compared with other such schemes and most suitable may be adopted as IHO Standard Security Scheme for ENC Data.

PERU

The involvement of having the IHO adopt the Security Scheme, which is presently being applied by PRIMAR, specially related to management, roles and responsibilities, should be taken into consideration more deeply, as the possible operation of such system is not very clear yet.

PORTUGAL

We believe that IHO should allow a testing period of PRIMAR and other security systems that may be developed in the near future before it becames an IHO recommended Security Scheme. If needed, an Industry – HOs – PRIMAR meeting should be planned and a common solution to be provided.

RUSSIA

No comments.

SPAIN

No comments.

SWEDEN

As has been mentioned earlier in other contexts, it should be noted that the Security Scheme is not only a guard against piracy or illegal copying. It is furthermore, and not the least, a guarantee that a delivery contains original data.

TUNISIA

With regard to paragraph 3, the Tunisian Hydrographic and Oceanographic Service suggests the creation of a technical working group to study into details all the aspects affecting the ENC, such as encryption problems, distribution process and updating models.

Later on, the recommendations of the WG will be submitted to the HO's Member States by Circular Letter for voting and eventual comments.

TURKEY

Despite the fact that the e-commerce and the related technologies are evolving too fast, TN-DNHO supports that there must be a universal standard for encryption of ENC Data, which will provide maximum security, taking into account the cost and the operational concerns. Therefore PRIMAR's Security Scheme can be adopted as the IHO Recommended Security Scheme but the financial aspects and/or burden of this to the HOs, especially for those who are not one of the Cooperative HOs with PRIMAR shall also be defined in clear terms, before it's final approval. We are not in a position to answer Yes or No to this question, without knowing these details.

UNITED KINGDOM

For the UKHO, the primary requirement for the security scheme is as a tool to facilitate the assurance of data and service integrity.

The UKHO believes most strongly that a single IHO Standard Security Scheme would be beneficial to HOs, ECDIS/ECS manufacturers and, most importantly, to ECDIS/ECS users. It is a logical extension to the IHO agreed concept of a single standard for the format and content of HO-produced vector navigational charts.

As mentioned in Annex A to CL 38/2000, the UKHO has been heavily involved in the development of the Security Scheme used by PRIMAR. Recent studies by independent consultants have confirmed both the suitability and currency of the technical solution for the intended purposes. Furthermore, a significant number of ECDIS/ECS manufacturers have implemented the PRIMAR Scheme, are working on implementation or have stated their intention to do so. Early adoption of the Scheme by the IHO would be extremely welcome by these companies and it would greatly assist the take up of ECDIS by the shipping industry by removing one of the related uncertainties. Further delay is likely to be detrimental to the whole concept of ECDIS and ENCs.

URUGUAY

A virtual RENC should be established in South America.

USA

The area of encryption and security is rapidly changing, both technologically and legally. We firmly believe that it is premature to settle on a system in these evolving times. Instead we suggest the IHO assume the role of developing and drafting “performance requirements”, noting just what is expected of these encryption systems, keeping in mind both the safety of navigation as well as security. Once such performance requirements are completed, industry should be allowed and encouraged to determine the most effective means of implementing the requirements utilizing current technology.

_____