ENC Data Encryption

NOAA takes great care to ensure that NOAA electronic navigational chart (NOAA ENC®) data are complete and accurate at the time of download. Currently, NOAA does not apply an encryption scheme to its ENCs for a number of reasons, which are outlined in this paper.

The IHO S-63 Data Protection Scheme states that the purposes of encryption are:

- **Piracy Protection** to prevent unauthorized copying of data by encrypting the ENC information.
- **Selective Access** to restrict access to ENC information to only those charts for which a customer has acquired chart permits.
- **Authentication** by the use of digital signatures to provide assurance that the ENC data came from the approved source.

Since NOAA does not copyright its data, encryption is not needed to protect against copyright infringement. NOAA distributes its ENCs for free via the Internet and therefore selective access does not apply. Finally, NOAA has established a process whereby third parties can become trusted suppliers of ENC data and may themselves use encryption as a value-added part of their service to assure the mariner that the data does come from an approved and authoritative source.

Recently, some have expressed concerns that NOAA ENC data are not encrypted and therefore could be vulnerable to intentional tampering. There are four situations in which NOAA ENC data could be maliciously harmed whether or not encryption is used. These situations are:

1) during the NOAA ENC production process,
2) during the Internet download process,
3) at the ENC distributor's site, or
4) at the end-user's site.

Scenario 1: During the NOAA ENC Production Process

It is conceivable that data created at NOAA could be subject to tampering. However, NOAA's Marine Chart Division has implemented multiple layers of review and quality control to ensure that the data released to the public are complete, accurate and uncompromised. No degree of data encryption will prevent corruption during the production process.

Scenario 2: During the Internet Download Process

NOAA currently uses a 32-bit cyclical redundancy check (CRC-32) algorithm described in the IHO S-57 ENC Product Specification and defined by ANSI/IEEE Standard 802.3 as a check that the data have been transmitted correctly during download. This value is stored in the Catalog file that accompanies the cell upon download. In order to ensure that data are not intentionally or accidentally corrupted, the CRC value can be computed directly from the ENC file and compared with the CRC value stored in the Catalog file.

NOAA's Web servers and the NOAA ENC data server are each protected by standard Internet security methods to prevent unauthorized access. While no system is completely protected from expert hacker attacks, the risk of a successful attack with the intent to replace NOAA ENC cells with maliciously altered cells is extremely low. If a hacker were successful in replacing an ENC cell with an altered one, the CRC described above also provides a check whether the downloaded NOAA ENC data have been tampered with and re-loaded onto the server. The Catalog file and the CRC values contained within are created by the NOAA data server from information stored separate from the ENC cells. If any changes are made to an ENC cell, no matter how minor, the CRC value will always change. Thus, in addition to defeating the server security, an attacker would have to have detailed knowledge of the internal workings of the data server and know to alter the CRC values stored on it so that the Catalog file and the altered cells would match. Given that the risk of corrupted or altered data originating from the NOAA data server is extremely low, NOAA determined that encrypting ENCs would introduce unwarranted overhead and expense.

The use of encryption would result in limiting the distribution of the ENC to a select number of trusted partners and the ENC would no longer be accessible and free over the Internet. The number of ENCs distributed would be limited due to the complexity of encryption, encryption keys, and the implementation of a registration requirement, thus resulting in a reduction in use and unnecessarily limiting free access to information required for safe navigation.

As detailed above, the rigors of the NOAA Internet site security protocols and the CRC check protocols make it highly unlikely that corrupted data could be downloaded directly from NOAA. NOAA believes that encryption would add an unwarranted level of security that would effectively constrain public access to this official data.

Scenario 3: At the ENC Distributor's Site

NOAA will soon publish the Final Rule for Certification Requirements for Distributors of NOAA Electronic Navigational Charts/NOAA Hydrographic Products. Contained within Section 995.24(iii) of the rule is the following language addressing encryption:

"The NOAA ENC files may be encrypted by a Certified ENC Distributor (CED), providing that the encryption/decryption process does not result in any information loss and that CED makes the decryption software available to the end user as part of the redistribution service. Decrypted files must have the same CRC checksum value as the original files. CED shall make the encryption/decryption software and documentation available to NOAA for testing."

If the CED follows the procedures for checking the CRC value outlined in the final rule then the pipeline from NOAA to the CED will remain secure.

The CED/Certified ENC Value-added Distributor (CEVAD) will become trusted supplier to mariners and ideally offer encryption as a service to its customers. This is the same model used by the regional ENC coordinating centers (RENC) that has been established in Europe. The RENC receives unencrypted data from the member hydrographic offices, and then encrypts the data prior to distribution to its customers. Mariners who may be concerned about the vulnerability of ENC data they download directly from the NOAA website should acquire data from a CED/CEVAD who offers encryption.

Scenario 4: At the End-user's Site

The ECDIS performance standard (IMO resolution A.817(19)) allows for the capability of updating the base ENC for Notice to Mariner or other chart corrections. It is therefore possible for data to be altered by the end-user either intentionally or unintentionally by keying in incorrect updates. In this scenario the data could be altered after it is loaded into the ECDIS. Therefore, encryption will not prevent this type of corruption.

Conclusion

The end-users will have several data delivery options available to them. They may choose to download ENC data directly from the NOAA website, obtain it via a third party CED/CDVAD distribution mechanism, or the data may become available through a non-certified third party distributor. The prudent mariner will choose one of the first two options to ensure that they are receiving uncorrupted NOAA ENC data.

NOAA takes great care to ensure that the ENC data that are released to the public are accurate and up-to-date. NOAA believes that encrypting the data prior to distribution would add considerable overhead for minimal return. By not encrypting the data, NOAA can distribute the ENC data to a broader user base. Encryption is primarily designed to protect copyright and control access, which are not issues needing to be addressed by NOAA. NOAA believes that concerns about redistribution have been addressed in its certified distribution process.