NOT TO BE CITED WITHOUT PRIOR
REFERENCE TO THE SECRETARIAT

Northwest Atlantic Fisheries Organization

Serial No. N4769 NAFO/FC Doc. 02/20

24TH ANNUAL MEETING - SEPTEMBER 2002

Part VIII

PROVISIONS ON SECURE AND CONFIDENTIAL TREATMENT OF ELECTRONIC REPORTS AND MESSAGES TRANSMITTED PURSUANT TO Part III E, VI and VII OF THE CONSERVATION AND ENFORCEMENT MEASURES.

1. Field of application

The provisions set out below shall apply to all electronic reports and messages transmitted and received pursuant to Part III. E and to annex I, Part VI.A.3 and B of the Conservation and Enforcement Measures, hereinafter referred to as "reports and messages".

2. General Provisions

2.1. The NAFO Executive Secretary and the appropriate authorities of Contracting Parties transmitting and receiving reports and messages shall take all necessary measures to comply with the security and confidentiality provisions set out in sections 3 and 4.

2.2. The NAFO Executive Secretary shall inform all Contracting Parties of the measures taken in the secretariat to comply with these security and confidentiality provisions.

2.3. The NAFO Executive Secretary shall take all the necessary steps to ensure that the requirements pertaining to the deletion of reports and messages handled by the Secretariat are complied with.

2.4. Each Contracting Party shall guarantee the NAFO Executive Secretary the right to obtain as appropriate, the rectification of reports and messages or the erasure of reports and messages the processing of which does not comply with the provisions of the NAFO Conservation and Enforcement Measures.

2.5. Notwithstanding the provisions of Part III .E.2 and Part VI.B., the Fisheries Commission may instruct the NAFO Executive Secretary not to make available the reports and messages received under Part III and VI to a Contracting Party, where it is established that the Contracting Party in question has not complied with these security and confidentiality provisions.

3. Provisions on Confidentiality

3.1. Reports and messages shall be used only for the purposes stipulated in the Conservation and Enforcement Measures. No report or message referred to in section 1 shall be kept in a computer database at the Secretariat unless explicitly provided for in the Conservation and Enforcement Measures.

3.2. Each inspecting Contracting Party shall make available reports and messages only to

their means of inspection and their inspectors assigned to the Scheme of Joint International Inspection and Surveillance. Reports and messages shall be transmitted to the inspection platforms and inspectors not more than 48 hours prior to entry into the Regulatory Area.

3.3. The NAFO Executive Secretary shall delete all the original reports and messages referred to in section 1 from the database at the NAFO Secretariat by the end of the first calendar month following the year in which the reports and messages have originated. Thereafter the information related to the catch and movement of the fishing vessels shall only be retained by the NAFO Executive Secretary, after measures have been taken to ensure that the identity of the individual vessels can no longer be established.

3.4. The NAFO Executive Secretary shall not make available reports and messages to other parties than those specified explicitly in Part III.E.2 of the Conservation and Enforcement Measures.

3.5. Inspecting Contracting Parties may retain and store reports and messages transmitted by the Secretary until 24 hours after the vessels to which the reports and messages pertain have departed from the Regulatory Area without re-entry. Departure is deemed to have been effected six hours after the transmission of the intention to exit from the Regulatory Area.

4. Provisions on security

4.1 Overview

Inspecting Contracting Parties and the NAFO Secretariat shall ensure the secure treatment of reports and messages in their respective electronic data processing facilities, in particular where the processing involves transmission over a network. Contracting Parties and the NAFO Secretariat must implement appropriate technical and organisational measures to protect reports and messages against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all inappropriate forms of processing.

The following security issues must be addressed from the outset:

- System access control:
  The system has to withstand a break-in attempt from unauthorised persons.
- Authenticity and data access control:
  The system has to be able to limit the access of authorised parties to a predefined set of data only.
- Communication security:
  It shall be guaranteed that reports and messages are securely communicated.
- Data security:
  It has to be guaranteed that all reports and messages that enter the system are securely stored for the required time and that they will not be tampered with.
- Security procedures:
  Security procedures shall be designed addressing access to the system (both hardware and software), system administration and maintenance, backup and general usage of the system.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing of the reports and the messages.

Security measures are described in more detail in the following paragraphs.

4.2 System Access Control

For their main computer systems the Contracting Parties and the Secretariat shall aim to meet the criteria of a C2-level trusted system, (as described in Section 2.2 of the U.S. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC), DOD 5200.28-STD, December 1985).

The following features are some of the ones provided by a C2-level trusted system:

- A stringent password and authentication system. Each user of the system is assigned a unique user identification and associated password. Each time the user logs on to the system he/she has to provide the correct password. Even when successfully logged on the user only has access to those and only those functions and data that he/she is configured to have access to. Only a privileged user has access to all the data.
- Physical access to the computer system is controlled.
- Auditing; selective recording of events for analysis and detection of security breaches.
- Time-based access control; access to the system can be specified in terms of times-of-day and days-of-week that each user is allowed to login to the system.
- Terminal access control; specifying for each workstation which users are allowed to access.

4.3 Authenticity and Data Access Security

Communication between the Contracting Parties and the NAFO Secretariat for the purpose of the Conservation and Enforcement Measures shall use the X.25 Protocol. Where E-mail is used for general communication and reports outside the scope of provision 1. between the NAFO Secretariat and the Contracting Parties the X.400 Protocol or Internet shall be used.

4.4 Communication Security

If Contracting Parties and the NAFO Secretariat agree, the X.400 Protocol or the Internet can be used for communication of data under the Scheme, but then appropriate encryption protocols like “Pretty Good Privacy” (PGP) or “Digital Encryption Standard” (DES) shall be applied to ensure confidentiality and authentic ity.

4.5 Data Security

Access limitation to the data shall be secured via a flexible user identification and password mechanism. Each user shall be given access only to the data necessary for his task.

4.6 Security Procedures

Each Contracting Party and the NAFO Executive Secretary shall nominate a security system administrator. The security system administrator shall review the log files generated by the software, properly maintain the system security, restrict access to the system as deemed needed and act as a liaison with the Secretariat in order to solve security matters.