§ 600.1507 Communications security.

Communications between an EMTU/EMTU-C and MCS must be secure from tampering or interception, including the reading of passwords and data. The EMTU/EMTU-C and MCS must have mechanisms to prevent to the extent possible:

(a) Sniffing and/or interception during transmission from the EMTU/EMTU-C to MCS.

(b) Spoofing.

(c) False position reports sent from an EMTU/EMTU-C.

(d) Modification of EMTU/EMTU-C identification.

(e) Interference with Global Maritime Distress and Safety System (GMDSS) or other safety/distress functions.

(f) Introduction of malware, spyware, keyloggers, or other software that may corrupt, disturb, or disrupt messages, transmission, and the VMS system.

(g) The EMTU/EMTU-C terminal from communicating with, influencing, or interfering with the Global Positioning System antenna or its functionality, position reports, or sending of position reports. The position reports must not be altered, corrupted, degraded, or at all affected by the operation of the terminal or any of its peripherals or installed-software.

(h) VMS data must be encrypted and sent securely through all associated cellular, satellite, and internet communication pathways and channels.

§ 600.1508 Field and technical services.

As a requirement of its type-approval, a type-approval holder must communicate with NMFS to resolve technical issues with a VMS Unit, MCS or bundle and ensure that field and technical services includes:

(a) Diagnostic and troubleshooting support to NMFS and fishers, which is available 24 hours a day, seven days per week, and year-round.

(b) Response times for customer service inquiries that shall not exceed 24 hours.

(c) Warranty and maintenance agreements.

(d) Escalation procedures for resolution of problems.

(e) Established facilities and procedures to assist fishers in maintaining and repairing their EMTU, EMTU-C, or MTU.

(f) Assistance to fishers in the diagnosis of the cause of communications anomalies.

(g) Assistance in resolving communications anomalies that are traced to the EMTU, EMTU-C, or MTU.

(h) Assistance to NMFS Office of Law Enforcement and its contractors, upon request, in VMS system operation, resolving technical issues, and data analyses related to the VMS Program or system.

§ 600.1509 General.

(a) An EMTU/EMTU-C must have the durability and reliability necessary to meet all requirements of §§ 600.1502 through 600.1507 regardless of weather conditions, including when placed in a marine environment where the unit may be subjected to saltwater (spray) in smaller vessels, and in larger vessels where the unit may be maintained in a wheelhouse. The unit, cabling and antenna must be resistant to salt, moisture, and shock associated with seagoing vessels in the marine environment.

(b) PII and Other Protected Information. Personally identifying information (PII) and other protected information includes Magnuson-Stevens Act confidential information as provided at 16 U.S.C. 1881a and Business Identifiable Information (BII), as defined in the Department of Commerce Information Technology Privacy Policy. A type-approval holder is responsible for ensuring that:

(1) All PII and other protected information is handled in accordance with applicable state and Federal law.

(2) All PII and other protected information provided to the type-approval holder by vessel owners or other authorized personnel for the purchase or activation of an EMTU/EMTU-C or arising from participation in any Federal fishery are protected from disclosure not authorized by NMFS or the vessel owner or other authorized personnel.

(3) Any release of PII or other protected information beyond authorized entities must be requested and approved in writing, as appropriate, by