§ 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

the submitter of the data in accordance with 16 U.S.C. 1881a, or by NMFS.

(4) Any PII or other protected information sent electronically by the type-approval holder to the NMFS Office of Law Enforcement must be transmitted by a secure means that prevents interception, spoofing, or viewing by unauthorized individuals.

§ 600.1510 Notification of type-approval.

(a) If a request made pursuant to § 600.1501 (type-approval) is approved or partially approved, NMFS will issue a type-approval letter to indicate the specific EMTU/EMTU-C model, MCSP, or bundle that is approved for use, the MCS or class of MCSs permitted for use with the type-approved EMTU, and the regions or fisheries in which the EMTU/EMTU-C, MCSP, or bundle is approved for use.

(b) The NMFS Office of Law Enforcement will maintain a list of type-approved EMTUs/EMTU-C, MCSPs, and bundles on a publicly available website and provide copies of the list upon request.

§ 600.1511 Changes or modifications to type-approvals.

Type-approval holders must notify NMFS Office of Law Enforcement (OLE) in writing no later than 2 days following modification to or replacement of any functional component or piece of their type-approved EMTU, EMTU-C, or MTU configuration, MCS, or bundle. If the changes are substantial, NMFS OLE will notify the type-approval holder in writing within 60 calendar days that an amended type-approval is required or that NMFS will initiate the type-approval revocation process.

§ 600.1512 Type-approval revocation process.

(a) If at any time, a type-approved EMTU/EMTU-C, MCS, or bundle fails to meet requirements at §§ 600.1502 through 600.1509 or applicable VMS regulations and requirements in effect for the region(s) and Federal fisheries for which the EMTU/EMTU-C or MCS is type-approved, or if an MTU fails to meet the requirements under which it was type-approved, OLE may issue a Notification Letter to the type-approval holder that:

(1) Identifies the MTU, EMTU, EMTU-C, MCS, or bundle that allegedly fails to comply with type-approval regulations and requirements;

(2) Identifies the alleged failure to comply with type-approval regulations and requirements, and the urgency and impact of the alleged failure;

(3) Cites relevant regulations and requirements under this subpart;

(4) Describes the indications and evidence of the alleged failure;

(5) Provides documentation and data demonstrating the alleged failure;

(6) Sets a response date by which the type-approval holder must submit to NMFS OLE a written response to the Notification Letter, including, if applicable, a proposed solution; and

(7) Explains the type-approval holder's options if the type-approval holder believes the Notification Letter is in error.

(b) NMFS will establish a response date between 30 and 120 calendar days from the date of the Notification Letter. The type-approval holder's response must be received in writing by NMFS on or before the response date. If the type-approval holder fails to respond by the response date, the type-approval will be revoked. At its discretion and for good cause, NMFS may extend the response date to a maximum of 150 calendar days from the date of the Notification Letter.

(c) A type-approval holder who has submitted a timely response may meet with NMFS within 21 calendar days of the date of that response to discuss a detailed and agreed-upon procedure for resolving the alleged failure. The meeting may be in person, conference call, or webcast.

(d) If the type-approval holder disagrees with the Notification Letter and believes that there is no failure to comply with the type-approval regulations and requirements, NMFS has incorrectly defined or described the failure or its urgency and impact, or NMFS is otherwise in error, the type-approval holder may submit a written objection letter to NMFS on or before the response date. Within 21 calendar days of the date of the objection letter, the type-approval holder may meet with