TECHNICAL CIRCULAR No. 526 of 08th December 2018

To:	All Surveyors/Auditors
Applicable to flag:	All Flags
	Inmarsat Enhances Cyber Security Offering for Maritime Industry
Reference:	Inmarsat

Inmarsat Enhances Cyber Security Offering for Maritime Industry

Inmarsat has introduced two new components to its maritime cyber security service, Fleet Secure, as it continues to develop solutions that combat ever-increasing cyber threats faced by shipowners and ship managers.

Vessel operators will benefit from a powerful, multi-layered endpoint security solution, Fleet Secure Endpoint, which is based on industry leading technology from ESET, a world leader in digital security, and powered by Port-IT and protects desktop computers and other systems connected to a vessel's network.

Fleet Secure Endpoint has been developed to remove infections and thwart hackers before damage occurs to onboard endpoints and connected systems. The solution will be available for commercial use from January 2019 and is compatible across Inmarsat's maritime portfolio of services, including Fleet Xpress, FleetBroadband and Fleet One. It also complements the resilience of Inmarsat's own satellite and ground network enabling consistent cybersecurity standards to be maintained.

It is a priority for every fleet operator and ship manager - shore-side and at sea - to ensure their systems are properly protected. As this enhancement to Fleet Secure demonstrates, Inmarsat is constantly monitoring the ever-changing cyber security landscape and devising new tools and approaches for addressing potential problems; ensuring that ships and their crew remain safe – physically and virtually.
Inmarsat has also launched a training app for mobile devices, Fleet Secure Cyber Awareness. This enables seafarers to educate themselves on the tactics that cyber criminals might employ in attempting to infiltrate a company's IT infrastructure.
Many attempts to gain unauthorized access to IT infrastructure require some sort of activation by an end-user in order to infect a system and cause further damage. These attacks are often heavily disguised so as to trick and manipulate end-users into unwittingly granting permission.

Customer Service Center
5201 Blue Lagoon Drive, 9TH. Floor,
Miami, Fl., 33126
Tel: 1 (305) 716 4116,
Fax: 1 (305) 716 4117,
E-Mail:
joel@conarinagroup.com

Technical Head Office
7111 Dekadine Ct.
Spring, Tx., 77379
Tel: 1 (832) 451 0185,
1 (713) 204 6380
E-Mail: vbozenovici@vcmaritime.com

Crew education is therefore an indispensable component in realizing a well-rounded security strategy.

REFERENCES:

- Inmarsat-Cybersecurity

- ATTACHMENTS: No.

Kindest Regards,

Val Bozenovici
Naval Architect – Conarina Technical Director

Customer Service Center
5201 Blue Lagoon Drive, 9TH. Floor,
Miami, Fl., 33126
Tel: 1 (305) 716 4116,
Fax: 1 (305) 716 4117,
E-Mail:

joel@conarinagroup.com

Technical Head Office
7111 Dekadine Ct.
Spring, Tx., 77379
Tel: 1 (832) 451 0185,
1 (713) 204 6380

E-Mail: *vbozenovici@vcmaritime.com*