# D8 Cybersecurity Guidance for FSO/CSO/OGAs

*Hello Port Partners!*
*This guide was created to provide a resource to further your understanding of cybersecurity and how it relates to the maritime nexus. This is not all-encompassing, rather a starting point should you need one. If you have questions or concerns, please reach out to your local COTPs for discussion.*

## Reporting Requirements:

⇒ **If a MTSA regulated entity reports SA, a BoS or a situation that could result in a TSI that is cyber-related only and it is reported to the NCCIC (National Cybersecurity and Communications Integration Center) at 888-282-0870; ensure that the MTSA regulated entity states to the NCCIC that they are a MTSA regulated entity in order to satisfy the reporting requirements of 33CFR101.305.**

⇒ **If the cyber-related SA, BoS or situation that could result in a TSI has another affect, (i.e. overtaking badge system and loss of access to a secured area); then the report must be made to the NRC at 800-424-8802.**

⇒ **When in doubt, and you are not sure, the MTSA regulated entity is advised to make the report directly to the NRC (National Response Center) at 800-424-8802; the NRC will notify the NCCIC as appropriate.**

⇒ **All non-cyber related SA, BoS or situation that could result in a TSI should continue to make reports to the NRC at 800-424-8802.**

⇒ **A MTSA regulated entity reporting to a local COTP DOES NOT satisfy the reporting requirement of 33CFR101.305.**

## Additional Information

*What we know about Cybersecurity today –*

1. We may not have all the tools in place to combat cyber security risks, but we are moving forward in this moment by educating ourselves and becoming more knowledgeable to reduce risks.

2. Learning basic principals outlined in this material will aid the maritime nexus' understanding of its' vulnerabilities and methods to consider to reduce their vulnerability.

3. Cyber is not going away; collectively, we need to know how to approach and handle it.

## Resources:

**CG-5P Policy Letter No. 08-16**
14 December 2016
SUBJ: Reporting Suspicious Activity and Breaches of Security

Homeport --- Missions > Maritime Security > Policy > CG-5P Policy Ltr No. 08-16, Reporting Suspicious Activity & Breaches of Security

# D8 Cybersecurity Guidance for FSO/CSO/OGAs

**COMDT Cyber Strategy - June 2015**
http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf

**Executive Order 13691 – Promoting Private Sector Cybersecurity Info Sharing**
https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing

- Lends insight to the NCCIC and their role and our partnerships.

## Homeport:
https://homeport.uscg.mil/

Missions > Maritime Security > Cybersecurity

- There are many additional resources if you follow the above path. Some examples are below.

### CG Maritime Cyber Bulletin 004-16: Shipboard VDR Vulnerabilities
Missions > Cybersecurity > Cyber News > CG MARITIME CYBER BULLETIN 004-16: SHIPBOARD VDR VULNERABILITIES

- The bulletin is provided to raise awareness in the maritime community of recent open source reporting highlighting cyber vulnerabilities associated with certain model(s) of Furuno Voyage Data Recorders (VDRs) and provide an overview of these vulnerabilities; and provide mitigation and remediation information.

### ABS: The Application of Cybersecurity Principles to Marine and Offshore Operation
Missions > Cybersecurity > Cyber Information > ABS THE APPLICATION OF CYBERSECURITY PRINCIPLES TO MARINE AND OFFSHORE OPERATION

- These Guidance Notes provide cybersecurity best practices and recommendations to marine and offshore organizations, and they are intended to enable members of the marine and offshore communities to take verifiable steps to protect an asset, its cyber-connected systems, its personnel, and its information from cyber intrusions. The overarching ABS cybersecurity guidance program provides these Guidance Notes as Volume 1: Cybersecurity.

### Guidelines on Cyber Security Onboard Ships
Missions > Cybersecurity > Cyber Information > Guidelines on Cyber Security Onboard Ships

- BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO has released this document is to offer guidance to shipowners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard their ships.

*April Tribeck*
*Port Security Specialist*
*USCG D8, dpi*
*500 Poydras Street*
*New Orleans, LA 70130*
*April.L.Tribeck@uscg.mil*

Last Updated: 3/6/2017 8:04 AM