

## **The U.S. Coast Guard and Recreational Boat and Yacht Safety**

Prepared and presented to the Maritime Law Association Recreational Boating Committee by Lieutenant Commander J. Travis Noyes, U.S. Coast Guard Office of Maritime and International Law on May 3, 2018.

### **Recreational Boating Safety**

Drownings continue to be the leading cause of death in recreational boating accidents.<sup>1</sup>

“Where cause of death was known, 80% of fatal boating accident victims drowned. Of those drowning victims with reported life jacket usage, 83% were not wearing a life jacket.”<sup>2</sup>

These deaths are preventable and wearing a Coast Guard approved personal flotation device is the best way to ensure safety on the water. Of particular note, the number of deaths and drownings associated with the use of paddle craft (canoes, kayaks, row boats, and stand up paddle boards) continues to rise as the use of paddle craft becomes more and more popular across the country.

### **Technology in the Maritime Domain**

As technology is increasingly adopted by boat manufactures, safety and navigation equipment manufacturers, and boat operators, it is important for boat owners and operators to know how technology, and particularly technology failure can impact the safety of their vessels.

Although not directly applicable to most of the recreational boating and yachting community, the International Maritime Organization continues to address the issue of cyber risk management. In July 2017, the Facilitation Committee and the Marine Safety Committee issued a joint circular that provides Guidance and Recommendations on Cyber Risk Management. While not significantly different in substance, these guidelines the previously issued MSC Circ. 1526.<sup>3</sup>

In addition to the Guidelines from IMO, the U.S. Computer Emergency Readiness Team within the Department of Homeland security issued a Joint Technical Alert with the Federal Bureau of Investigation on Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. The March 15, 2018 Alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear,

---

<sup>1</sup> U.S. Coast Guard Office of Auxiliary and Boating Safety, *2016 Recreational Boating Statistics*, May 22, 2017 (Available at: [http://www.uscgboating.org/statistics/accident\\_statistics.php](http://www.uscgboating.org/statistics/accident_statistics.php), accessed on May 5, 2018).

<sup>2</sup> *Id* at page 6.

<sup>3</sup> International Maritime Organization, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3, July 5, 2017 (available at: [http://www.imo.org/en/OurWork/Security/Guide\\_to\\_Maritime\\_Security/Documents/MS-C-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MS-C-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf), accessed on May 5, 2018).

commercial facilities, water, aviation, and critical manufacturing sectors. DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).<sup>4</sup>

Again, this is not directly applicable to many recreational vessels; however, as systems onboard these vessels are increasingly computerized, the same vulnerabilities that exist in the Industrial Control Systems may exist in the computer systems operating the recreational vessel systems to include engine controls and navigation systems. The Coast Guard does not have any specific guidance on how to mitigate these risks; however U.S. CERT has a number of helpful links and documents on their website to include advice on securing the internet of things, and good security habits.<sup>5</sup>

Technology in the Maritime Domain is not all about threats, there are a number of new technologies changing the way people and vessels get out on the water. Within the past 5-10 years, there have been a number of internet based companies trying to change the way that boaters own, charter, and use their boats.

### **Passenger Vessel Inspection and Mariner Licensing**

The Coast Guard' interaction with these platforms begins when the vessels cross the line from purely recreational uses into passenger vessel operations that are potentially subject to mariner credentialing and vessel inspection laws and regulations.

Coast Guard regulations require that

“If a person operates a vessel that carries one or more passengers-for-hire, he or she is required to have a valid Coast Guard license or MMC officer endorsement suitable for the vessel's route and service. He or she must have the license or MMC in his or her possession and must produce it immediately upon the request of a Coast Guard boarding officer.”<sup>6</sup>

Additionally, as the number of passengers increases, the regulatory requirements increase. For any vessel carrying more than six passengers, including at least one passenger for hire, the Small Passenger Inspection Requirements in 46 C.F.R., Chapter I, Subchapter T apply to the vessel.<sup>7</sup> And again, as the number of passengers onboard increases to more than twelve, including at least one passenger for hire, the Passenger Vessel Inspection Requirements in 46 C.F.R., Chapter I,

---

<sup>4</sup> U.S. Computer Emergency Readiness Team, Alert (TA18-074A) *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, Mar. 15, 2018 (available at: <https://www.us-cert.gov/ncas/alerts/TA18-074A>, accessed on May 5, 2018).

<sup>5</sup> <https://www.us-cert.gov/ncas/tips>.

<sup>6</sup> 46 C.F.R. § 26.20—1.

<sup>7</sup> 46 C.F.R. § 175.110.

Subchapter H apply to the vessel.<sup>8</sup> For many of these regulatory requirements, the enforcement provisions of the regulations or the underlying statutes can be applied to the owners, operators, or agents of vessels found non-compliant.

### **Fire Protection Equipment for Recreational Boats**

The Coast Guard's final rule Harmonization of Standards for Fire Protection, Detection, and Extinguishing Equipment, published on July 22, 2016, mistakenly applied the maintenance and inspection requirements contained in the National Fire Protection Association Standard for Portable Fire Extinguishers (NFPA 10) to all recreational vessels. This rulemaking will remove the NFPA 10's recordkeeping and inspection requirements as they apply to recreational vessels. It will also move recreational vessel fire safety requirements from 46 CFR subchapter C, which is a commercial subchapter, to 33 CFR subchapter S, where other recreational vessel safety rules are already located.<sup>9</sup>

---

<sup>8</sup> 46 C.F.R. § 70.10—1.

<sup>9</sup> Office of Information and Regulatory Affairs, Current Regulatory Plan and the Unified Agenda of Regulatory and Deregulatory Actions (available at: <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201710&RIN=1625-AC41>, accessed on May 3, 2018).