DEPARTMENT OF THE NAVY
COMMANDER
U.S. FLEET FORCES COMMAND
1562 MITSCHER AVENUE SUITE 250
NORFOLK, VA 23551-2487

3500
28 Dec 11

Team,

In the cyber domain, as in every other warfighting domain, our ships, submarines, aircraft, combat systems, and networks must BE READY. Operational readiness depends on our ability to reliably transport and secure mission critical information.

Regardless of where a unit may be in the FRTP cycle, or whether a ship is preparing for its first or last deployment, in the cyber domain, we are "OPERATING FORWARD" at the tactical edge the instant we connect to the network. The reality is that we do not have the luxury of accepting material shortfalls or lapses in information assurance practices, as these shortfalls translate into real and immediate operational risks across our Navy networks.

Make no mistake, cyber readiness is Commanding Officer business. Just as I expect you to understand the material condition of your ship, its weapons systems, and the readiness of your Sailors, I expect you to have a clear picture and understanding of your network readiness, the proficiency of your network operators, and to set clear and unambiguous expectations regarding cyber-related operations for your entire crew.

Success in this complex domain cannot be relegated solely to your Network Administrators and Information Assurance Managers. Success will require consistent, relentless adherence to standards and a culture of accountability from leadership to the deckplates. And that accountability begins with me. I owe you the tools, training and resources to meet the standards Navy expects. Accurate, timely and vigorous communications up and down the chain-of-command is required to enable us, repeat us, to meet cyber operational and readiness standards.

Bottom line, operating securely in the cyber domain is serious business requiring your attention. This handbook is designed to assist you in meeting those standards. Be vigilant, be ready, and sail safe.

J. C. HARVEY, JR.