2D COMBAT ENGINEER BATTALION

2D COMBAT ENGINEER BATTALION
COMMANDING OFFICER'S
INFORMATION AND
OPERATIONAL SECURITY
POLICY STATEMENT

The information environment is critical terrain in which our enemies operate on a daily basis. They operate without moral or ethical standards and will exploit our Marines, Sailors, and their families without remorse. They systematically collect information from publicly available sources and our units' operational tempo and schedule to build profiles on individual servicemembers. It is incumbent on us to make ourselves, our families, and our units into hard targets to protect against information exploitation and attack.

When each Marine, Sailor, and family member carefully considers the type of information they post, and the details they post, they play a key role in removing themselves from the enemy's information source inventory, they protect themselves, and they improve our information operations fighting position.

Simple steps for guarding our critical information include

1) Pay attention to what we communicate on our professional networks, both NIPR and SIPR.

2) Consider carefully what we post on personal networks, especially posts made on social media.

3) Evaluate your information security posture daily and look for gaps and seams.

4) Consider how to include information operations more deliberately in our current and future operations.

The Marines and Sailors in 2d Combat Engineer Battalion must remain current with information and operations security training as outlined MCO 3070.2A. We must accurately apply classification markings on every document or email they produce. We must be on the lookout for public information that presents a risk. And every Marine and Sailor is responsible to ensure they keep their security clearance up to date. Refer any, and all security questions to our Security Manager in the S2.

B. S. PETERSON
Lieutenant Colonel, United States Marine Corps
Commanding Officer, 2d Combat Engineer Battalion