



UNITED STATES MARINE CORPS
CHEMICAL BIOLOGICAL INCIDENT RESPONSE FORCE
II MARINE EXPEDITIONARY FORCE
3399 STRAUSS AVENUE, SUITE 219
INDIAN HEAD, MD 20640-5035

1306

CO

30 APR 2014

CHEMICAL BIOLOGICAL INCIDENT RESPONSE FORCE POLICY LETTER #9-14

From: Commanding Officer
To: All Hands

Subj: GUIDANCE ON THE HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION AND THE USE OF NON-GOVERNMENT OWNED COMPUTERS, EMAIL ACCOUNTS, AND HARD DRIVES

Ref: (a) SECNAVINST 5239.3B
(b) MARADMIN 118/11
(c) MARADMIN 642/09
(d) MARADMIN 461/09
(e) MARADMIN 388/09

1. Purpose. Establish policy that directs the safe handling of personally identifiable information (PII) and the appropriate use of personal email accounts.
2. Cancellation. This policy will remain in effect until revised or cancelled by the appropriate authority.
3. Background. Compromises of PII through the loss of laptops and portable electronic devices (PED) has driven the need for the Marine Corps to implement data encryption solutions and safe computing practices that ensure the protection of personal information.
4. Action
 - a. All personnel requiring access to government information systems will complete training that covers information assurance (IA) awareness and PII awareness.
 - b. In the event that the transmission of PII is necessary via email, it will be limited to U. S. Government email accounts (.mil or .gov) and will meet the following requirements:
 - Digitally signed and encrypted using DOD approved public key infrastructure (PKI) certificates
 - Include "FOUO" in the subject line
 - Place the following statement at the footer of the email message: "FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES."

Subj: GUIDANCE ON THE HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION AND THE USE OF NON-GOVERNMENT OWNED COMPUTERS, EMAIL ACCOUNTS, AND HARD DRIVES

c. PII not be transmitted to personal email accounts (e.g., Hotmail, Gmail, Yahoo Mail, etc.) or commercial email accounts (such as those used by contractors supporting the battalion).

d. All external hard drives connected to government owned computers will be encrypted with the Marine Corps Enterprise Network (MCEN) encryption solution sets.

5. Tasks

a. All personnel shall continue to practice safe computing practices, safeguarding all PII.

b. All personnel accessing government information systems shall complete PII awareness and IA awareness training once every fiscal year. The battalion S-6 will keep records of the training.

c. Personnel shall report compromises of PII to the CBIRF Communications Officer immediately upon discovery.

6. The point of contact regarding any questions pertaining to this policy letter is the CBIRF Communications Officer at 301-744-1066.


S. E. REDIFFER