DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
5000
LF
JAN 5 2012

Dr. Thomas Sinks
Deputy Director
National Center for Environmental Health/
Agency for Toxic Substances and Disease Registry
4770 Buford Highway, NE
Atlanta, GA 30341

Dear Dr. Sinks:

Over the years force protection vulnerabilities have been unintentionally created in some Camp Lejeune products, to include the upcoming Chapter B report. The purpose of this letter is to request your assistance to mitigate security risks involved in this situation.

In the years since your agency began working on Camp Lejeune drinking water research initiatives, the security environment has significantly changed and there is now a greater need to provide robust and effective force protection for Marines, Sailors, civilian employees and their families who live or work aboard our bases and installations. Force Protection includes not only physical protection measures (e.g., gates and fences), but also measures to protect the security of sensitive asset and infrastructure information (e.g., water systems information).

Broad force protection efforts to identify vulnerabilities are ongoing across the Marine Corps and the other services. The attached page includes a synopsis of some of the governing regulations.

Recognition that these force protection concerns intersected with information contained in your Camp Lejeune reports first arose during a July 2010 Data Mining Technical Workgroup meeting held at Camp Lejeune. In August 2011, the new commander at Camp Lejeune requested a security review of the type of information that was included in previous water modeling reports. This security review concluded that the release of some of the specific information pertaining to active drinking water systems aboard Camp Lejeune potentially places those who live or work aboard the base at risk.

Our respective staffs discussed these issues and the conclusions from the security review. Your staff rightly requested references to assist their understanding and to provide concise guidance about release of sensitive water system information into the public domain.

I know that some sensitive information has already been released into the public domain in such places as some Marine Corps and other government agency websites. Changing security threats and evolving

policy, however, compel us to continuously evaluate information available in the public domain. To that end, I request that we work together to review our public domain materials and take appropriate steps to protect critical infrastructure information.

More specifically, after consulting with our security experts, I have provided the following guidance to my staff. I encourage you to provide this information to your staff, too:

1) Review new information carefully to avoid releasing location information for active potable water wells, raw or treated potable water lines, water treatment plants or water storage tanks which may not be released to the public in coordinate, map, or other form.

2) Review information on active potable water wells, raw or treated potable water lines, water treatment plants or water storage tanks that have been released in the past and, to the extent possible, remove that information from existing web sites.

3) Release without restriction, where and when otherwise appropriate, the location information for inactive or demolished potable water wells or non-potable monitoring wells in coordinate, map, or other form.

The Marine Corps understands the need to share information with the scientific community. Prudence requires, however, that information sharing be within the rubric of responsible force protection. I greatly appreciate your cooperation and look forward to working with you in this on-going effort to protect our forces and families.

Sincerely,

J. A. KESSLER
Major General
Assistant Deputy Commandant
Installations and Logistics
(Facilities)

Attachment
References to Protection of
Critical Assets

References to Protection of Critical Assets

DoDI 2000.16: Department of Defense (DoD) Instruction 2000.16 (DoD Antiterrorism Standards) requires DoD components to identify critical assets, and subsequently develop and implement risk mitigation measures to reduce the vulnerabilities of DoD critical assets (e.g., water distribution infrastructure). Since July 2010, the Marine Corps has been conducting Mission Assurance Assessments on its bases and installations in order to identify and formally catalog all of our critical assets and infrastructure. Our consolidated Mission Assurance/All Hazards Risk Assessment Program integrates all aspects of Mission Assurance to include the identification of assets and infrastructure critical to mission execution. After the completion of these assessments, the Marine Corps will publish a policy document that addresses specific actions that will be taken to reduce risk and ensure the protection of our personnel and infrastructure.

U.S. Code Title 18, PART I, CHAPTER 37, Sec. 795 (a): "Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military post, camp, or station, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary." Further, Exemption 9 of the Freedom of Information Act (FOIA) broadly exempts disclosure of information pertaining to "geological and geophysical information and data, including maps, concerning wells."

SECNAV M-5510.36 requires that "a security and policy review shall be performed on all official DoD information intended for public release including information intended for placement on publicly accessible websites or computer servers." . . .

SECNAV M-5510.36, Department of the Navy Information Security Program Chapter 8: requires commanders to safeguard information pertaining to critical assets and infrastructure.

On 22 April 2011, the Commandant of the Marine Corps published guidance to all commanding Generals, all Commanding Officers, and All Officers in Charge on Information Protection. In that "White Letter" the Commandant directed a range of actions to improve operational security and protection of sensitive information and IT systems.