NAVAL REACTORS IMPLEMENTATION BULLETIN FOR DOE ORDER 203.1 - 106, REVISION 0

Consistent with the Naval Nuclear Propulsion Program (NNPP) overall concept of operations, the following provides specific implementation guidance for the Limited Personal Use of Government Office Equipment, Including Information Technology (IT) under the Director's cognizance. This Implementation Bulletin (IB) takes precedence over relevant guidance found in Department of Energy (DOE) Order 203.1, Limited Personal Use of Government Office Equipment, Including IT and other DOE or National Nuclear Security Administration (NNSA) related documents.

1. All references to DOE program employees should be changed to NR Program employees.

2. Government office equipment, including IT and similar equipment and resources funded by the Government in support of official Government business includes but is not limited to: personal computers, laptops, related peripheral equipment and software, land-line telephones, cell phones, Blackberry, Personal Digital Assistants (PDAs) and other similar portable electronic devices, facsimile machines, photocopiers, Internet connectivity and electronic mail (E-mail).

3. Naval Reactors (NR) Program sites provide employees with connectivity to the Internet to enable access to information resources for research, including the exchange of unclassified non-technical and non-sensitive E-mail associated with their NR Program responsibilities.

NR Program employees who use Government office equipment, including IT, are authorized to make limited use of these resources for personal purposes in accordance with the provisions of DOE Order 203.1 and this IB. Personal use is defined as any activity that is conducted for purposes other than accomplishing official or otherwise authorized activity (e.g. approved coursework).

4. Personal use of Government office equipment and IT resources should occur during off-duty hours (e.g., authorized lunch/break periods or before/after scheduled work hours). There may be limited circumstances where there is a need to use

these resources during on-duty hours. These situations should be limited to those that can not be reasonably made at another time and the duration must be minimized so it does not interfere with the performance of the employee's official duties. Site management is responsible for ensuring employees properly manage their time and their use of these resources is appropriate. DOE O 203.1 Section 4.a.

5. Employees using Government office equipment and IT resources do not have a right to privacy nor should they have any expectation of privacy while using these resources. DOE O 203.1 Section 4.b.(1).

Additionally, employees using Government office equipment and IT resources for personal use will have no right to an expected level of information confidentiality, integrity or availability. DOE O 203.1 Section 4.b.(1).

6. NR Program employees are expected to conduct themselves professionally in the workplace and to refrain from using Government resources for activities that are inappropriate. Inappropriate personal use of Government office equipment and IT resources includes, but is not limited to those identified in DOE O 203.1 Section 4.f and the following:

a. Activity including the creation, downloading, viewing, storing, copying, or transmitting of materials considered to be inappropriate, offensive or illegal regardless of the purpose or intent is prohibited.

b. Activity including creation, downloading, viewing, storage, copying or transmission of materials related to gambling is prohibited.

c. Peer-to-peer (P2P) file sharing systems provide Internet users with the ability to share files on their computers with other Internet users. The most popular P2P software is free and open source. Common P2P uses are music and movie file sharing, gaming and instant messaging. Government sponsored studies indicate the vast majority of the files traded on P2P networks are copyrighted movie and music files as well as pornography. Unauthorized P2P systems have also been used as an avenue for the spread of computer viruses and the compromise of sensitive information at numerous U.S. Government organizations.

Consistent with the guidance contained in Office of Management and Budget (OMB) Memorandum M-04-26 "Personal Use Policies and File Sharing" dated September 8, 2004, any activity that may impair the performance of a system or network resource including operating, accessing or providing any method of support to an unauthorized P2P network or resource is prohibited.

d. All personal E-mail must be transmitted and received through the user's assigned NR Program unclassified Internet access account. Employees may not use NR Program Internet access computers to access E-mail accounts other than those established by the site IT office. Access to web based E-mail services such as (but not limited to) America Online (AOL), HotMail and Yahoo is prohibited.

e. Use of Government resources to support a personal business including such use that assists relatives, friends, or other individuals is prohibited.

7. Report instances of Waste, Fraud, and Abuse to the cognizant security office as required by local policy. DOE O 203.1 Section 5.a.(4).

8. Employees may access their site unclassified E-mail account from other NR Program sites, or with a Government provided unclassified laptop while on travel. Navy/Marine Corps Intranet (NMCI) users may access unclassified (non-sensitive) NMCI resources from home computers in accordance with Naval Network Warfare Command (NETWARCOM) policy.

9. Users with an NR Field Office approved business need for automated transfers from Prime contractor unclassified Internet access systems to the classified NNPP Net must delete all personal E-mail arriving on NNPP Net computers as soon as practical. NR Program employees are not permitted to create, store, or process personal E-mail on classified computers.

10. NR Program Internet access system usage will be audited. If a manager has concerns about an employee's personal use of the Internet and E-mail, records of the user's activity may be provided to the manager by the site computer security organization. The site computer security organization can then aid the manager in analyzing the records. The site computer security organization also has the authority to initiate these reviews in accordance with local policy.