June 7, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum**/RA/**
Assistant Inspector General for Audits

SUBJECT: MEMORANDUM REPORT: AUDIT OF NRC'S POLICY AND PRACTICES CONCERNING CAMERA CELL PHONES (OIG-05-A-12)

As part of the Office of the Inspector General's (OIG) audit of NRC's telecommunications program, OIG identified a problem outside the scope of the audit that warrants your attention. Specifically, NRC lacks a camera cell phone policy to:

- Establish requirements for Office of Information Services (OIS) acquisition of camera cell phones for use by employees.
- Remind employees and visitors that the prohibition against taking photographs in NRC buildings also applies to camera cell phones.
- Provide security guards with guidance on the handling of camera cell phones brought to the building by visitors.

Furthermore, the agency is not enforcing its current policy toward visitors with cameras. This increases the risk that the agency's classified and sensitive information could be deliberately or inadvertently made public or otherwise compromised.

Background

Camera cell phones, if misused, pose security and privacy threats because they enable people to covertly photograph images or scenes and transmit them immediately to the Internet. Since 2000, when camera cell phones were introduced, individuals have misused the devices in various ways, including secretly taking revealing pictures of people in locker rooms, cheating during

tests, and committing credit card theft. In addition, security professionals have identified the potential for other abuses, such as Government and industrial espionage.

The Federal Government, companies, schools, health clubs, and other entities are taking various steps to deal with the security and privacy threats posed by camera cell phones and other new wireless devices with photographic capabilities. On December 23, 2004, President Bush signed the Video Voyeurism Prevention Act of 2004. This law made it a crime to knowingly photograph, videotape, or record by any means an image of a private area of an individual without their consent on Federal property where the individual has a reasonable expectation of privacy. Punishment would include fines of up to $100,000 or up to a year in prison, or both. Some Government offices that handle classified information, companies, health clubs, and high schools have banned or restricted the use of camera cell phones on their premises.

Due to the growing popularity of camera cell phones, security professionals have urged companies and agencies to establish policies and restrictions on the use of camera cell phones and to ensure employee awareness of these rules.

Approximately 20 percent of U.S. cell phone users had camera cell phones during 2004 and, according to analysts, by 2006, 80 percent of the cell phones sold in the U.S. will be camera phones.

NRC Needs To Develop a Camera Phone Policy and Better Enforce Its Camera Policy

Guidance on Cameras

Management Directive (MD) and Handbook 12.1, *NRC Facility Security Program*, permit visitors and employees to bring personal cameras into NRC buildings, but prohibit the use of these devices to take pictures inside NRC buildings without permission from the Director, Division of Facilities and Security, or, in some cases, from the Director, Office of Public Affairs. This guidance, revised on April 14, 2004, represents a departure from the language contained in an earlier version of the MD and Handbook that prohibited employees and visitors from bringing cameras into the buildings without approval. MD and Handbook 12.1 also permit the use of NRC-owned photographic equipment within NRC facilities to conduct official NRC business, however, such use is prohibited in security areas[1] and other locations where it could result in the compromise of classified or sensitive unclassified information.

[1] According to MD and Handbook 12.1, a security area is a physically defined space (usually a room, or a series of interconnecting rooms, within a facility) containing classified information and subject to physical protection and personnel access controls.

Visitors and Employees Unaware

NRC has not ensured that employees and visitors understand that NRC's general prohibition against taking photographs within agency facilities also applies to camera cell phones. Similarly, the agency has not ensured that employees are aware of vulnerabilities associated with the use of camera cell phones.

Camera Phone Purchase Request

Recently, an NRC official requested that OIS provide the official with a camera cell phone. In the past, OIS typically accommodated all requests for cell phones, so this created a challenge for OIS, which ultimately denied the request for security reasons. Camera cell phones are small, easy to use, and provide immediate images that can be transmitted instantly to the Internet for widespread dissemination. Careless use can compromise classified or sensitive information or even physical security measures used to protect NRC facilities.

OIS officials said that the lack of guidance on camera cell phones required them to seek advice from an agency security official on the security vulnerabilities posed by these devices. OIS officials said that denying the request was somewhat awkward because of the past practice of accommodating requests. OIS officials held discussions with the requestor to explain the security vulnerabilities associated with having the camera feature on the cell phone. This situation highlights the need for a policy stipulating the conditions for granting or denying requests for camera cell phones and informing staff of the risks posed by these devices. According to an OIS manager, such a policy would need to go beyond camera cell phones and address other wireless devices with photographic capabilities, such as some types of personal digital assistants.

Personal Camera Cell Phones

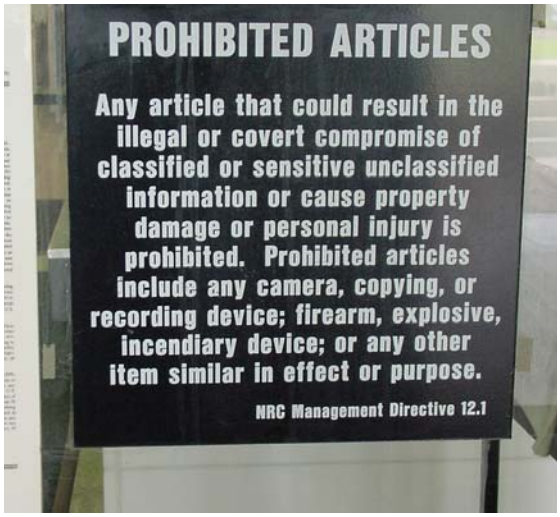
Employees may similarly be unaware of the risks posed by their personal camera cell phones. These phones are an emerging technology and more and more employees are likely to have personal camera cell phones as time goes by. Employees who might not otherwise consider taking a picture within the agency may be tempted to do so because of the camera cell phone's convenience.

Security Guards

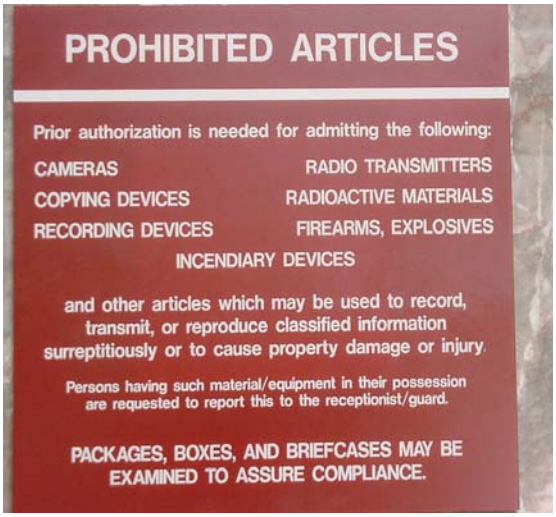
Security guards impose no requirements on visitors with camera cell phones and impose inconsistent requirements on visitors with cameras that are not in accordance with the requirements in MD and Handbook 12.1. Guards in both

buildings recognized the risks posed by camera cell phones, but said NRC has not issued instructions to them on how to deal with visitors who have these phones. Therefore, they do not try to determine if visitors have these phones and would not take any special measures even if they knew a visitor had one.

Auditors also determined that security guards in the two headquarters buildings are imposing different requirements on visitors with cameras. In neither case are the requirements imposed in accordance with MD 12.1. In the Two White Flint North headquarters building lobby, guards act on outdated guidance by confiscating cameras from visitors entering the building. Visitors may read this prohibition, which appears on a guard desk sign that lists prohibited articles, including cameras. However, guards in the One White Flint North headquarters building lobby allow visitors to keep their cameras with them provided their escort has been notified about the camera. A sign in this building states cameras are permitted with authorization, although OIG notes that MD and Handbook 12.1 make no mention of a need for such authorization.



Two White Flint North lobby sign



One White Flint North lobby sign

Lack of Policy

Employees may be unaware of the vulnerabilities posed by camera cell phones and the prohibition against taking photographs in NRC buildings because there is no policy on wireless devices with photographic capability, including camera cell phones, and because the prohibition against taking photographs is not well publicized. The prohibition is mentioned within MD and Handbook 12.1 as part of a discussion of physical security requirements for the protection of classified information, but is not likely to be read by all or most employees. New employees

are even less likely to be aware of the prohibition because they are not briefed at the new employee orientation on the prohibition against taking photographs in the NRC buildings. At the time of this audit, OIS was working to develop a policy on wireless devices.

Visitors are also unlikely to be aware of NRC's expectations concerning camera cell phones because NRC has not directed security guards to try to identify these phones, caution visitors about these phones, or take some other measure to ensure that the NRC photography policy is enforced.

Deliberate or careless use of camera cell phones can compromise classified or sensitive information or even physical security measures used to protect NRC facilities. These phones provide immediate images that can be transmitted instantly to the Internet for widespread dissemination. The growing popularity of camera cell phones highlights the need to heighten employee and visitor awareness about NRC's prohibition against photographs inside agency facilities.

By implementing a camera cell phone policy that addresses camera cell phones and clarifies agency requirements concerning cameras in general, and consistently implementing its overall camera policy, NRC will strengthen its protection against information and physical security threats.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Develop a policy that (a) establishes requirements for OIS acquisition of camera cell phones and other wireless devices with photographic capability for employee use, (b) conveys that NRC's prohibition against taking photographs in NRC buildings also applies to camera cell phones, and (c) communicates NRC's expectations concerning visitors with camera cell phones.

2. Issue a Yellow Announcement to remind employees of the NRC prohibition against using any type of device to take pictures inside NRC buildings.

3. Inform new employees of the prohibition against taking photographs with any type of device inside NRC buildings during the new employee orientation.

4. Inform visitors of the prohibition against taking pictures with any device inside NRC buildings through the display of posters at the building, auditorium, and meeting room entrances.

5. Include, in the security guard orders, instructions for the security guards to use in handling visitors with camera cell phones.

Agency Comments

During an exit conference held May 18, 2005, agency managers generally agreed with the report's findings and recommendations and provided a comment concerning the draft audit report. We modified the report as we determined appropriate in response to this comment. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

Scope/Contributors

To accomplish this limited scope review assessing the agency's policies and procedures to prevent inappropriate use of camera cell phones in its headquarters facilities, auditors reviewed relevant criteria such as the current version of MD and Handbook 12.1, *NRC Facility Security Program* (dated April 14, 2004). Auditors also reviewed the prior version of MD and Handbook 12.1 (dated October 16, 2000) to assess the changes reflected in the updated guidance and, for comparison purposes, a Department of Defense Directive, dated April 14, 2004, concerning use of commercial wireless devices.

Auditors interviewed security guards in the One and Two White Flint North lobbies to learn what practices they employ toward visitors with cameras and camera cell phones. They also interviewed OIS officials and an official from the Office of Administration to obtain their perspectives on whether NRC should purchase camera cell phones for use by employees.

This work was conducted over a 2-week period during the month of April 2005 in accordance with generally accepted Government auditing standards and included a review of management controls related to the audit objective. The work was conducted by Beth Serepca, Team Leader; Shyrl Coker, Audit Manager; and Judy Gordon, Audit Manager.

Please provide information on the actions taken in response to the recommendations directed to your office by July 18, 2005. Actions taken or planned are subject to OIG followup. See Attachment for instructions for responding to OIG report recommendations.

If you have any questions or concerns regarding this report, please contact me at 415-5915 or Beth Serepca at 415-5911.

cc: Chairman Diaz
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons

Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Hubert T. Bell, Inspector General
Janice Dunn Lee, Director, Office of International Programs
William N. Outlaw, Director of Communications
William N. Outlaw, Acting Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Frank J. Congel, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Acting Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Paul H. Lohaus, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV