March 18, 2008

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: MEMORANDUM REPORT: NRC'S PLANNED CYBERSECURITY PROGRAM (OIG-08-A-06)

As part of the Office of the Inspector General's (OIG) audit of NRC's Oversight of Licensees' Nuclear Security Officers, OIG interviewed agency staff to determine how upcoming changes to NRC's cybersecurity oversight processes might impact the agency's physical security inspection program. Through this work, OIG identified an issue that could adversely affect NRC's oversight of licensees' cybersecurity programs for nuclear power plants. In particular, although NRC is making progress in developing cybersecurity regulations and a corresponding inspection program, it lacks a clear plan for the inspection program.

BACKGROUND

Cybersecurity refers to the branch of security that protects information technology (IT) infrastructure. IT infrastructure encompasses not only the public internet, but also the less visible systems and connections of the Nation's critical infrastructures, such as nuclear power plants and electric power distribution grids. Cybersecurity is increasingly important to the nuclear power industry as plants upgrade from analogue to digital control systems, which are vulnerable to attacks by criminals and foreign governments. These cyber attacks can temporarily disrupt computer networks, or more seriously, cause failure of public services. According to the U.S. Central Intelligence Agency (CIA), for instance, extortionists recently penetrated computer systems of utility companies outside the U.S. and caused power outages that affected multiple cities.

In response to the current threat environment, Federal government agencies are taking programmatic and policy actions to strengthen public and private sector cybersecurity. The U.S. Department of Homeland Security (DHS), which is the federal government's focal point for cybersecurity, disseminates threat information, and provides private industry with guidance and analytic tools to assess cybersecurity measures and mitigate vulnerabilities. The U.S. Department of Energy (DOE) conducts research and development, and develops planning guidance, to help industries in the energy sector strengthen their defenses against cyber threats. Most recently, the U.S. Federal Energy Regulatory Commission (FERC) issued new cybersecurity regulations in January 2008 to give electric utilities a set of comprehensive standards for protecting the power transmission infrastructure against cyber attacks.[1]

NRC began a rulemaking process in 2006 to address cybersecurity at nuclear power plants. This rulemaking will amend the Code of Federal Regulations (CFR)[2] to incorporate elements of cybersecurity orders and guidance issued by NRC following the terrorism incidents of September 11, 2001.[3] The proposed new requirements would require that nuclear power plant licensees and license applicants implement a comprehensive cybersecurity program to ensure that applicable computer systems are protected from cyber attacks. NRC plans tentatively to oversee licensees' compliance with these regulations by adding cybersecurity inspections to the agency's baseline security inspection program.[4]

ISSUES FOR CONSIDERATION

NRC is taking steps to develop cybersecurity regulations and a corresponding inspection program, but has not determined how it will conduct and support inspections. Without a clear implementation plan for cybersecurity inspections, NRC could face difficulties in overseeing licensees' cybersecurity programs, thereby increasing the risks to nuclear power plant security.

Successful Implementation in 2010 Requires Advance Planning

NRC aims to begin inspections of licensee cybersecurity programs as early as calendar year 2010, following completion of the ongoing rulemaking and a grace-period for licensees to implement the new regulations. NRC's main objectives in establishing new cybersecurity regulations are, in order of priority:

[1] 18 CFR 40, "Mandatory Reliability Standards for Critical Infrastructure Protection."
[2] 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage."
[3] EA-02-026, *Interim Compensatory Measures*; and EA-03-086, *Design Basis Threat.*
[4] Inspection Procedure (IP) 71130, "Physical Protection."

- Maintaining safety and security;
- Increasing public confidence;
- Making NRC activities and decisions more effective, efficient, and realistic;
- Reducing unnecessary regulatory burden on stakeholders.

Internal NRC guidance recognizes that agency staff work most effectively when appropriately deployed and fully engaged in fulfilling the agency's mission. NRC security inspectors are trained and experienced to carry out specific physical security oversight tasks; cybersecurity, however, is a separate discipline requiring unique training and subject matter expertise. NRC's FY 2009 Performance Budget acknowledges a need to focus on recruiting and retaining skilled personnel in these fields.[5] In short, NRC has less than two years to develop an implementation plan, and recruit and train qualified staff.

NRC Lacks Clear Plan for Cybersecurity Inspections

NRC has not finalized a clear plan for implementation of a cybersecurity inspection program. New regulations governing nuclear power plant licensees' cybersecurity programs are expected to take effect in calendar year 2010, and a contractor has been tasked with writing inspection procedures. However, the agency has yet to resolve several issues that will impact implementation of the inspection program. In particular, agency management has not determined:

- respective roles of agency staff and contractors in conducting cybersecurity inspections;
- staff requirements for cybersecurity inspections and headquarters support, and;
- resources needed for initial training of cybersecurity inspectors, and for follow-on training to maintain technical proficiency.

Agency plans acknowledge the need to recruit and retain personnel in cybersecurity, however, the agency's plans vis-à-vis this objective are uncertain.

Inadequate Implementation Plan Could Compromise Physical and Cybersecurity Inspection Programs

The absence of a clear plan could jeopardize implementation of a cybersecurity inspection program in calendar year 2010. OIG believes that NRC management should carefully consider the implications of adding cybersecurity to the baseline security inspection program. First, inspecting licensees' cybersecurity posture

[5] U.S. Nuclear Regulatory Commission Performance Budget Fiscal Year 2009, p.131. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1100/v24/sr1100.pdf

requires a highly-trained staff to inspect and evaluate cybersecurity infrastructure. Several regional baseline security inspectors expressed concern that they are not qualified to perform the cybersecurity inspections. Specifically, inspectors commented that their experience and training in physical security does not directly apply to cybersecurity. Furthermore, agency staff commented that there are limits to which non-cybersecurity professionals can be trained for cybersecurity, which is a highly technical and dynamic field requiring continuous training.

Second, the added workload associated with the cybersecurity inspection module could adversely affect security inspectors' efforts in other areas of physical security oversight. Specifically, the time and effort spent by regional security inspectors on cybersecurity efforts could divert their attention from other physical security inspection tasks.

Third, without a clear implementation strategy for cybersecurity inspections, NRC may lack sufficient qualified staff to oversee licensees' cybersecurity programs. Without robust cybersecurity oversight, NRC faces increased risk that cyberattacks, human error, or technological failure could compromise IT systems that are critical to nuclear power plant operations.

RECOMMENDATION

OIG recommends that the Executive Director for Operations:

1. Develop and implement plans for a cybersecurity oversight program that captures skill set and workload requirements for cybersecurity inspections, and targets resources to prepare for program implementation in calendar year 2010.

AGENCY COMMENTS

During an exit conference on February 21, 2008, NRC officials agreed with the finding and recommendation in the draft report. Clarifying comments on the draft report were incorporated as appropriate. The agency opted not to submit formal written comments to this report.

Please provide information on actions taken or planned on the recommendation within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG follow-up, as stated in the attached instructions.

SCOPE AND METHODOLOGY

The OIG audit team reviewed relevant internal agency documents, such as NRC's inspection procedures, management guidance, budget plans, and cybersecurity policy development documents. The team also reviewed cybersecurity guidance developed and used by the nuclear industry to reinforce NRC guidance. To understand other Federal agencies' cybersecurity activities, the team reviewed relevant documentation from the U.S. Federal Energy Regulatory Commission, as well as reports from U.S. Government Accountability Office.

Auditors interviewed headquarters staff in NSIR to learn their roles and responsibilities as they pertain to the planned cybersecurity inspection program. Auditors also interviewed region-based physical security inspectors to obtain their views on cybersecurity and its relationship to NRC's physical security oversight processes.

This work was conducted from January 2008 through February 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The work was conducted by: Beth Serepca, Team Leader; Judy Gordon, Audit Manager; Paul Rades, Senior Analyst; and Jaclyn Storch, Management Analyst.