Department of Energy

Washington, DC 20585

July 19, 2006

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: SUMMARY: Special Inquiry Report Relating to the Department of Energy's Response to a Compromise of Personnel Data (OIG Case No. I06IG001)

INTRODUCTION

During a June 9, 2006, congressional hearing, Department of Energy officials publicly disclosed that a hacker had attacked an unclassified computer system at the National Nuclear Security Administration's (NNSA) Service Center in Albuquerque, New Mexico, and had exfiltrated a file containing the names and social security numbers of 1,502 individuals working for the NNSA. At the hearing, witnesses testified that: (1) senior Department officials, including you and the Deputy Secretary, were not fully apprised of the Albuquerque attack until the week of June 5, 2006, even though the attack had been detected in mid-2005; and, (2) employees had not been informed that their personnel data may have been compromised. On June 9, 2006, you requested that the Office of Inspector General examine aspects of Departmental actions in response to the discovery of the attack.

The Office of Inspector General initiated a Special Inquiry to examine the facts and circumstances regarding these matters. We also reviewed issues concerning a possible delay by the Department in completing an assessment of the impact of the intrusion, including the compromise of personnel data. We interviewed 46 current and former Federal and contractor employees of the Department and other agencies. The inquiry team analyzed thousands of classified and unclassified documents, including reports, electronic messages, notes and related records. We encountered certain inconsistent recollections, some concerning key issues, which could not be reconciled.

This unclassified memorandum provides a general summary of our findings. Our Special Inquiry report, which is classified and contains additional details, is being provided to you under separate cover.

SUMMARY

Our inquiry did not identify anyone in the Department who recalled briefing you or the Deputy Secretary on the specific details of the computer attack until June 2006. Additionally, we confirmed that Federal and contractor employees had not been notified that their personnel data was at risk until about ten months after the data compromise had been detected. Further, we

Printed with soy ink on recycled paper

determined that there was a lengthy delay in the Department's completion of an impact assessment on the intrusion.

Additionally, the current Chief Information Officer and the Director of the Office of Intelligence and Counterintelligence, both of whom began working at the Department in November 2005, informed us that they were not advised of the specifics of the data compromise until June 2006. It was our judgment that these individuals, given their duties and responsibilities, should have been directly engaged in this issue as early in the process as possible.

Witnesses provided their rationale for the actions taken in this matter. However, we concluded that the Department's handling of this matter was largely dysfunctional and that the operational and procedural breakdowns were caused by questionable managerial judgments; significant confusion by key decision makers as to lines of authority, responsibility, and accountability; poor internal communications, including a lack of coordination and a failure to share essential information among key officials; and, insufficient follow-up on critically important issues and decisions. Additionally, we found that the Department lacked clear guidance on procedures for notifying employees when personnel data is compromised. The bifurcated organizational structure of NNSA within the Department further complicated the situation.

During an interview with the Office of Inspector General, Ambassador Linton Brooks, the NNSA Administrator, stated that he took full responsibility for not ensuring that you and the Deputy Secretary were fully briefed on the matters relevant to the intrusion. In addition, he stated that he was the senior official responsible for not following-up to ensure that the employees and contractors were appropriately notified of the theft of their personnel information. In addition to Ambassador Brooks, we identified seven other senior officials who shared some level of responsibility for the way in which the matter was handled.

RECOMMENDATIONS

The Department and, in particular, the over 1,500 employees whose personnel data may have been compromised were not well served by the actions of officials in carrying out their duties during these events. Based on our review, we concluded that the Department should take the following steps to preclude a recurrence of this or similar situations:

1. Ensure that the Department has a clear, unambiguous policy on notifying employees affected by the loss of personnel data from Departmental systems;
2. Redefine and clarify roles and responsibilities for program managers, counterintelligence officials, cyber/information technology personnel, security managers, and others to ensure that the Secretary and Deputy Secretary are fully and timely briefed on cyber intrusions, security incidents and similar matters of significance to Departmental operations;
3. Clarify internal communication protocols to ensure that information critical to ongoing Department operations is shared among responsible program officials;
4. Clarify external communication protocols to ensure that decisions made by other agencies/authorities which may impact Departmental operations are fully understood and considered by Department decision makers;

5. Appoint a task force of senior Departmental officials, including NNSA, to address situational complications resulting from the bifurcation of Department and NNSA functions; and,
6. Review the facts in the Special Inquiry report and determine if personnel action is warranted.

I would be pleased to discuss this report in detail at your convenience.