

CHARLES E. GRASSLEY, IOWA, CHAIRMAN

ORRIN G. HATCH, UTAH
TRENT LOTT, MISSISSIPPI
OLYMPIA J. SNOWE, MAINE
JON KYL, ARIZONA
CRAIG THOMAS, WYOMING
RICK SANTORUM, PENNSYLVANIA
BILL FRIST, TENNESSEE
GORDON SMITH, OREGON
JIM BUNNING, KENTUCKY
MIKE CRAPO, IDAHO

MAX BAUCUS, MONTANA
JOHN D. ROCKEFELLER IV, WEST VIRGINIA
KENT CONRAD, NORTH DAKOTA
JAMES M. JEFFORDS (II), VERMONT
JEFF BINGAMAN, NEW MEXICO
JOHN F. KERRY, MASSACHUSETTS
BLANCHE L. LINCOLN, ARKANSAS
RON WYDEN, OREGON
CHARLES E. SCHUMER, NEW YORK

United States Senate

COMMITTEE ON FINANCE

WASHINGTON, DC 20510-6200

KOLAN DAVIS, STAFF DIRECTOR AND CHIEF COUNSEL
RUSSELL SULLIVAN, DEMOCRATIC STAFF DIRECTOR

June 20, 2006

The Honorable Samuel W. Bodman
Secretary of Energy
Department of Energy
1000 Independence Avenue S.W.
Washington, D.C. 20585

Dear Mr. Secretary,

I am writing about some very disturbing testimony your agency presented recently to the House Energy and Commerce Committee.

That testimony appears to indicate that the National Nuclear Security Agency (NNSA) failed to notify over 1500 agency and contract employees that their personal identity information had been compromised. This particular cyber intrusion was detected in September 2005 at the NNSA Albuquerque Field Office. Just as disturbing was the testimony by NNSA Administrator Brooks that he failed to notify you of this incident until it became clear that the issue was to be made public. For over nine months these victims, your employees, were not notified that they were victims of a crime. Furthermore, they could not take precautionary steps to insure that their stolen identity information was not used to conduct fraud.

I call your attention to a pertinent article in the Business Section of the Washington Post on June 18, 2006, entitled "Be Prepared for ID Theft: A Quick Response Helps." The article makes one point crystal clear: "It's very important to move quickly and in an organized way" in cases involving the theft of social security numbers. Those affected need to contact the three major credit card bureaus immediately to place 90-day fraud alerts on their credit files. Your employees were denied that option.

Subsequent to Director Brooks' testimony, Deputy Inspector General (IG) Chris Sharpley provided me with details on other recent incidents, including: 1) personal identify information of over 4,000 Hanford Site contractor employees was discovered on June 2, 2006 in an illegal drug lab in Washington State; 2) ten laptop computers have been stolen from the Germantown, Maryland Department of Energy (DOE) office on June 12, 2006 that may contain additional personal information; and 3) on May 28, 2006, a computer was stolen at the Oakridge site that may also contain personal information on contractor employees. Previous and on-going investigations by the Department's IG have revealed missing computers from a number of DOE sites throughout the country. The theft of DOE computers and data appears to be a persistent, ongoing problem.

Mr. Secretary, I hope you share my concern that all these issues appear to be symptoms of a larger problem within the Department's security apparatus. In their testimony before the House Energy and Commerce Committee on June 9th, Director Brooks and the DOE official responsible for Cyber Security, Mr. Tom Pyke, made it clear that due to a lack of central security authority not only were the employees not informed of stolen data, but you yourself were not informed until days before the hearing. Director Brooks made it clear that he believed the Department's Counter Intelligence section informed you, and Mr. Pyke, the cyber "czar," stated he did not even know of the stolen data until just a few days before the hearing. Even the Department's IG failed you. The Inspector General Act makes it clear the IG has the duty and responsibility "to report immediately to the Secretary whenever the Inspector General becomes aware of particularly serious or flagrant problems..."

In my previous letter to you, dated May 23rd, I made it clear that the Department of Energy was remiss in not having an overall security authority to coordinate, standardize, and direct all security operations. The incidents described above are just another in a long line of examples that the current security design of the Department may be flawed. This applies not only to the physical security of facilities, but also to the security of the data contained within those facilities.

When confronted with why he did not inform you, NNSA Administrator Brooks pointed his finger at another section within the department that has security responsibility. When confronted about why the employees were not notified, the head of cyber security said he didn't know about it. When asked why they won't meet the design basis threat (DBT) or conform to a security policy, the individual lab/facility security directors often blame others for the strictness of the policy or the unrealistic expectation of the DBT. When asked why policies are not being followed, the Office of Security and Safety Assurance suggest they lack any authority to force the other entities within the Department to conform with established standards.

Mr. Secretary, I would very much like for you to explain to me what efforts the Department of Energy has made to centralize security. If such efforts were tried and failed in the past, please explain to me why they failed. Please explain to me where the accountability for flaws in security lies within the Department.

It's obvious that some serious errors in judgment were made during recent security breaches at various DOE sites. Please identify how this information should move up the chain of command, and identify at what point did your subordinates decide not to inform you or the affected employees? Has the IG checked with all DOE facilities and sites to determine if there are other incidents of theft of personal data that have not been properly reported and addressed? I would like to know how and where the breakdown in communications occurred, and who is chiefly responsible for what happened? I would also like to know why the IG failed to meet his responsibilities under the IG Act and notify you about these problems in a timely manner as required by law.

Mr. Secretary, you needed to have this information as soon as possible in order to take appropriate corrective action. By keeping you in the dark and not reporting these incidents up the chain of command, your staff, including the IG, left affected agency employees vulnerable to fraud and left you vulnerable to criticism.

Your continued cooperation in this matter is appreciated. I look forward to hearing from you.

Sincerely,


Charles E. Grassley
Chairman

Copies to:
Senator Domenici
Senator Bingaman