The Deputy Secretary of Energy
Washington, DC 20585

June 22, 2007

MEMORANDUM FOR ALL HEADS OF DEPARTMENTAL ELEMENTS

FROM: CLAY SELL

SUBJECT: Security Incident (Including Cyber) Notification Protocol

These procedures will apply to security, cyber security (including loss of personal identifiable information), and counterintelligence issues that are or could be of concern to Congress.

For purposes of notification, "Congress" will include the staffs of the Armed Services and Energy Committees, the Appropriations Subcommittees on Energy, Water Development, and (for Counterintelligence issues only) the House and Senate Intelligence Committees. The Department's Office of Congressional and Intergovernmental Affairs[1] (after appropriate consultation with the Office of General Counsel) will inform these committees as soon as practicable of any of the following:

1. *Loss of personally identifiable information (PII) for ten or more individuals.* PII guidance as defined by the Chief Information Officer is at http://cio.energy.gov/documents/CS38APII.pdf and will exclude such information normally available to the public such as office listing or office phone numbers. "Loss" will mean disclosure outside of the Federal Government or its contractors. Inadvertent access by a Federal or contractor employee to PII to which he or she would not normally be authorized access, or the unencrypted emailing of PII that does not suggest any possibility of compromise, will not be considered "loss" for purposes of this protocol and need not be reported.

2. *Loss or compromise of classified material in either electronic (outside of the DOE firewalls) or paper form, in a way that may compromise national security.* This determination will be made by the appropriate program office in consultation with Departmental security officials upon

[1] For incidents involving only National Nuclear Security Administration (NNSA), the notification may be made by the NNSA Office of Congressional Affairs after consultation with the Assistant Secretary for Congressional and Intergovernmental Affairs. To ensure Department-wide consistency, however, the notification process will be overseen by the Assistant Secretary for Congressional and Intergovernmental Affairs.

determination that the situation presents a risk or threat to national security. Normal accounting problems that do not actually or potentially compromise national security and those instances in which compromise is considered remote but cannot be positively excluded need not be reported.

3. *Penetration of a classified network.* Any indication of a successful penetration of a classified network, whether or not data has been exfiltrated or compromised.

4. *Certain Intelligence and Counterintelligence incidents.* Such incidents falling within the guidelines of *Intelligence Community Policy Memorandum Number 2005-100-3, Reporting of Intelligence Activities to Congress,* especially the loss or compromise of classified intelligence information on such a scale or over such an extended period as to indicate the possibility of a systemic compromise, or a loss or compromise that investigation indicates poses a substantial risk to U.S. national security activities.

In addition to the notifications resulting from the circumstances above, the Department will offer a quarterly briefing to the staffs of the Congressional committees noted above covering the status of security, cyber security, and counterintelligence incidents during the quarter. This briefing will include a summary of all incidents identified based on the above criteria, to include: cyber security attacks, a summary of security incidents with an indication of whether there are any trends of concern, and a broad summary of on-going counterintelligence issues consistent with preserving the integrity of the investigations.

For purposes of this protocol, the following will have the lead on the substantive aspects of reporting:

- The CIO for all cyber security and PII issues including those that may ultimately have counterintelligence implications.

- The NNSA CIO for NNSA-related cyber security and PII issues, including those that may ultimately have counterintelligence implications.

- The Senior Intelligence Officer for all other counterintelligence issues.

- The Chief Health, Safety and Security Officer for all other non-NNSA issues.

- Chief of Defense Nuclear Security for all other NNSA issues.

These individuals will be informed by all elements of the Department of any incident within any departmental organization that may fall under the above guidelines.

Prior to information being provided to Congress, incident reports and presentations should be coordinated with the relevant Under Secretary.

In each instance where there is doubt as to whether an issue should be reported, the issue will be resolved in favor of reporting. Concurrent with notifications to the Office of Congressional and Intergovernmental Affairs, all Departmental elements should simultaneously notify NNSA Public Affairs (only for NNSA specific issues) and the DOE Office of Public Affairs (for both DOE and NNSA issues) for the appropriate determination of media applicability.