December 17, 2008

MEMORANDUM TO: R. W. Borchardt
Executive Director for Operations

FROM: Annette L. Vietti-Cook, Secretary **/RA/**

SUBJECT: STAFF REQUIREMENTS – SECY-08-0158 – PROPOSAL ON THE POTENTIAL PROGRAM TO PAY CREDIT MONITORING SERVICES

The Commission has approved the recommendation to provide credit monitoring services to individuals when 1) a breach of personally identifiable information (PII) results in notification of the individual(s); 2) the risk is evaluated as "high" using the quantitative risk analysis formula as proposed by staff; and, 3) Nuclear Regulatory Commission action or inaction is the cause of the breach of the employee's or private citizen's PII. The Commission has also approved the use of a GSA BPA when the staff determines that this is the most efficient and cost-effective means of providing credit monitoring services.

The NRC PII breach notification policy should be revised to incorporate the quantitative risk analysis formula and issued within 60 days.

NRC's breach notification policy should also be revised to state more clearly that the provision of credit monitoring services (separate and distinct from any notification obligation) is tied to the government's fault or responsibility in causing the breach.

If a breach of PII does occur, the staff should use this experience to evaluate whether the assumptions that have been made in Enclosure 1 of this paper for "Assigning Risk Score" need modification.

The staff should continue to seek ways to reduce the likelihood that a breached system would lead to a risk determination of "high" under the staff's proposed risk analysis system, the only risk category that would entitle individuals to the credit monitoring system.

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
Commissioner Svinicki
OGC
CFO
OCA
OPA
Office Directors, Regions, ACRS, ASLBP (via E-Mail)
PDR