



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 17, 2008

SECRETARY

COMMISSION VOTING RECORD

DECISION ITEM: SECY-08-0158

TITLE: PROPOSAL ON THE POTENTIAL PROGRAM TO PAY
CREDIT MONITORING SERVICES

The Commission (with all Commissioners agreeing) approved the subject paper as recorded in the Staff Requirements Memorandum (SRM) of December 17, 2008.

This Record contains a summary of voting on this matter together with the individual vote sheets, views and comments of the Commission.

A handwritten signature in black ink, appearing to read "Annette Vietti-Cook", written over a horizontal line.

Annette L. Vietti-Cook
Secretary of the Commission

Attachments:

1. Voting Summary
2. Commissioner Vote Sheets

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
Commissioner Svinicki
OGC
EDO
PDR

VOTING SUMMARY - SECY-08-0158

RECORDED VOTES

	APRVD	DISAPRVD	ABSTAIN	NOT PARTICIP	COMMENTS	DATE
CHRM. KLEIN	X				X	11/7/08
COMR. JACZKO	X				X	11/12/08
COMR. LYONS	X				X	11/4/08
COMR. SVINICKI	X				X	11/17/08

COMMENT RESOLUTION

In their vote sheets, all Commissioners approved the staff's recommendation and provided some additional comments. Subsequently, the comments of the Commission were incorporated into the guidance to staff as reflected in the SRM issued on December 17, 2008.

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary
FROM: CHAIRMAN KLEIN
SUBJECT: SECY-08-0158 – PROPOSAL ON THE POTENTIAL
PROGRAM TO PAY CREDIT MONITORING SERVICES

Approved xx Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below _____ Attached xx None _____



SIGNATURE

11/7/08

DATE

Entered on "STARS" Yes No _____

Chairman Klein's Comments on SECY-08-0158
Proposal on the Potential Program to Pay Credit Monitoring Services

I commend staff for providing a comprehensive paper providing policy options for addressing credit monitoring following a PII data breach. Further, I believe the staff's quantitative risk analysis formula is a reasonable approach for determining when to offer credit monitoring services to affected individuals. It should be incorporated into the revised breach notification policy and issued within 60 days.

I approve the provision of credit monitoring services when a breach of an individual's personally identifiable information (PII) results in a requirement to notify the individual and the risk is also evaluated as "high" using the quantitative risk analysis formula. I approve the staff's proposal to use the General Services Administration blanket purchase agreements to acquire credit monitoring services (Option 2) and approve staff's request to revise the agency's policy for a breach of PII by including the quantitative risk analysis formula.

I agree with Commissioner Lyons' comments that if a breach occurs, staff should use the experience to evaluate whether the assumptions that have been made in Enclosure 1 of this paper for "Assigning Risk Score" need modification.



Dale E. Klein

11/07/2008

NOTATION VOTE

RESPONSE SHEET

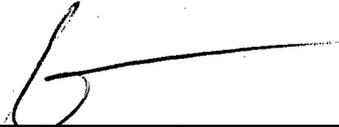
TO: Annette Vietti-Cook, Secretary
FROM: COMMISSIONER JACZKO
SUBJECT: SECY-08-0158 – PROPOSAL ON THE POTENTIAL PROGRAM TO PAY CREDIT MONITORING SERVICES

Approved X Disapproved Abstain

Not Participating

COMMENTS: Below X Attached None

I approve the staff proposed option number 2 to provide for credit monitoring services in the event of a loss of personally identifiable information. Although the staff cost estimates for such service were intended to provide an upper bound on the possible costs, the analysis shows that some breaches may require significant resources to address. Therefore, I encourage the staff to 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.



SIGNATURE

11/12/08

DATE

Entered on "STARS" Yes X No

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary
FROM: COMMISSIONER LYONS
SUBJECT: SECY-08-0158 – PROPOSAL ON THE POTENTIAL PROGRAM TO PAY CREDIT MONITORING SERVICES

Approved X Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below ___ Attached X None ___


Peter B. Lyons
SIGNATURE

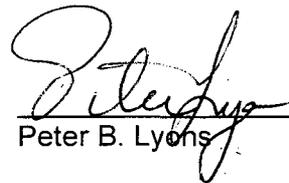
11/ 4 /08
DATE

Entered on "STARS" Yes X No _____

Commissioner Lyons' Comments on SECY-08-0158
Proposal on the Potential Program to Pay Credit Monitoring Services

I would like to thank the staff for providing a thorough discussion of this issue in a timely manner for the Commission's consideration. I approve Option 2 which would allow the agency to acquire commercial monitoring services from vendors participating in the GSA blanket purchase agreement (BPA) program. Even though this Option has the disadvantage of limiting the NRC's access to three current vendors, it has the advantage of eliminating a time-consuming competition and of being cost-free until such time as a task order requesting these services is issued. Using Option 2, the NRC should enter into a BPA arrangement as soon as possible so that in the event of a personally identifiable information (PII) breach, the agency can respond as quickly as possible.

I believe the staff has established a process that ensures the "bar is set low enough" as to be protective of individuals affected by a breach of their PII without being so low as to make this process unworkable. However, 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. Additionally, the staff should consider whether this process can be applied retroactively in the event we learn that a PII breach occurred within a reasonable period of time (e.g., perhaps within two years) prior to implementation of this program.


Peter B. Lyons 11/4/08
Date

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary
FROM: COMMISSIONER SVINICKI
SUBJECT: SECY-08-0158 – PROPOSAL ON THE POTENTIAL
PROGRAM TO PAY CREDIT MONITORING SERVICES

Approved XX Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below ___ Attached XX None ___



SIGNATURE

11/17/08

DATE

Entered on "STARS" Yes No _____

Commissioner Svinicki's Comments on SECY-08-0158
Proposal on the Potential Program to Pay Credit Monitoring Services

I approve Option 2 to provide credit monitoring services to individuals when 1) a breach of personally identifiable information (PII) results in a requirement to notify 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. I further approve the revision of the NRC PII breach notification policy (to be completed within 60 days) to incorporate the quantitative risk analysis formula.

I would note that the decision rendered by the U.S. Government Accountability Office regarding the use of appropriated funds to provide credit monitoring services stated as follows:

"[W]e recently issued a decision stating that credit monitoring services for federal employees are generally personal expenses not chargeable to an agency's appropriation. . . . The facts here lead us to a different outcome. Because the proposed purchase of credit monitoring services [as proposed by NRC] relates to a breach caused by the government and may be a means of mitigating damage resulting from the breach, appropriated funds are available for this purpose."

Therefore, I believe that 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. Finally, given the wide range of potential cost estimates for such services, I support the comment of Commissioner Jaczko that staff continue to find ways to reduce any information security vulnerabilities that increase the likelihood that a breached system would lead to a risk determination of "high."



Kristine L. Svinicki

11/17/08