April 9, 2009

MEMORANDUM TO: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
Commissioner Svinicki

FROM: R. W. Borchardt **/RA Bruce S. Mallett for/**
Executive Director for Operations

SUBJECT: CYBER ISSUE ASSESSMENT PROCESS AND CYBER ASSESSMENT TEAM

The purpose of this memorandum is to inform the Commission that the staff is establishing a Cyber Issue Assessment Process and a Cyber Assessment Team (CAT) in order to enhance the U.S. Nuclear Regulatory Commission's (NRC's) ability to address emergent cyber-related security issues and to enhance the effectiveness of the NRC's incident response.

The Cyber Issue Assessment Process will provide a consistent methodology and focal point for the evaluation and resolution of cyber-related security issues across multiple NRC organizations. Under the process, cyber-related security issues will be evaluated in accordance with the process flow path described in the Enclosure 1. The process includes two types of assessments. The first type of assessment will occur after an operating issue or a potential cyber issue is identified (e.g.; event or vulnerability). Under these conditions, the process results in the CAT making recommendations to the program office(s) on a course of action. Senior managers in the program office(s) will be responsible for any decision to implement a course of action.

The second type of assessment will occur after the Information Assessment Team (IAT) receives information identifying a potential or actual cyber-related security threat (e.g.; threat or exploit). The assessment of cyber-related security threats will be the responsibility of the IAT as was the case prior to the establishment of the CAT. The CAT will provide the IAT technical support during their evaluation of the potential cyber-related security threat. The CAT's technical support will include an assessment of the significance and urgency of the cyber-related security threat and of the potential vulnerabilities to nuclear facilities.

CONTACT: George A. Wilson, NRR/DE
(301) 415-1711

In contrast, recent cyber-related security issues have been handled on more of an ad hoc basis. Some cyber-related security issues were entered in the NRC's Allegations Program, while others required multiple assignments by multiple managers to multiple subject matter experts in multiple offices. In each case, the cyber-related security issue received the necessary evaluation but none were completed with the consistency and efficiency that will be provided by the Cyber Issue Assessment Process.

After the CAT has completed its evaluation and recommendations and provided to the program office or IAT, communications with stakeholders will normally be accomplished in accordance with Management Directive 8.18, "NRC Generic Communications Program," by the IAT, in the case of a cyber-related security threat, or by the program office for all other cyber-related security issues. The CAT or the program office will also inform other NRC offices and program owners, including the Office International Programs (OIP), the generic issues program owner, the inspection program owners, and the operating experience program owners, as appropriate.

The functions of the Cyber Assessment Team will provide assistance to the NRC line organizations on technical and regulatory matters involving cyber-related security issues, will interface with the industry and other stakeholders on generic cyber-related security matters, will provide information and support to OIP in cyber-related security interactions with NRC international counterparts, and will provide information to the appropriate NRC program office(s) to support the decisionmaking process and to facilitate alignment across multiple NRC program offices. The team concept of the CAT is intended to enhance the quality and timeliness of the NRC's response to cyber-related security issues, increase cohesiveness and synergy, and to identify potential policy or technical cyber-related security issues for further consideration by NRC management and the Commission.

The primary responsibilities of the CAT as an expert group will be (1) to assess and document the disposition of pertinent cyber-related security information received from industry, stakeholders, and other governmental agency representatives to facilitate early identification of technical issues that may warrant further NRC attention, (2) to make recommendations to the program offices for follow up to emergent cyber-related security issues, and (3) to provide technical support to the IAT which has the lead for cyber-related security threat evaluation. The CAT team responsibilities will be included in a charter that will include procedures for use by the team. The team charter will be similar to the charter currently used by the IAT.

The staffing of the CAT will be accomplished through a cooperative arrangement between the offices that possess experts in cyber security. Managers and staff in the various offices and regions with expertise in cyber security will be identified and serve as members of the CAT using a process similar to that used for the current IAT membership. Enclosure 2 includes a brief description of the CAT organizational structure. The CAT will coordinate as appropriate with their counterparts in other government agencies with the intent to identify available resources that can be leveraged to enhance the CAT's cyber security assessment capabilities. Where the appropriate resources or expertise does not exist within the NRC or other government agencies, the CAT will consider the use of qualified contractors to supplement the team.

The staff estimates completion of the following major milestones for establishing the Cyber Issue Assessment Process and the CAT: identify team members, hold initial CAT meetings, and communicate how the team is intended to function internally by April 2009; finalize the CAT charter, interface contact list, and cyber-related security assessment review procedures by May 2009; and initialize cyber security assessment database by December 2009. The staff is planning to evaluate the effectiveness of the Cyber Issue Assessment Process after an initial 12 month period of operation.

Enclosure 2 provides an estimate of the resources needed to staff the team, the anticipated time each member will spend on team activities, and the assumptions used in making the resource estimates.

Enclosures:
1. Cyber Issue Assessment Process
2. CAT Organizational Structure and Estimated Resources

cc: SECY
OGC
OCA
OPA
CFO

The staff estimates completion of the following major milestones for establishing the Cyber Issue Assessment Process and the CAT: identify team members, hold initial CAT meetings, and communicate how the team is intended to function internally by April 2009; finalize the CAT charter, interface contact list, and cyber-related security assessment review procedures by May 2009; and initialize cyber security assessment database by December 2009. The staff is planning to evaluate the effectiveness of the Cyber Issue Assessment Process after an initial 12 month period of operation.

Enclosure 2 provides an estimate of the resources needed to staff the team, the anticipated time each member will spend on team activities, and the assumptions used in making the resource estimates.

Enclosures:
1. Cyber Issue Assessment Process
2. CAT Organizational Structure and Estimated Resources

cc: SECY
OGC
OCA
OPA
CFO

DISTRIBUTION:

RidsEdoMailCenterResource
RidsOisResource
RidsNmssOdResource
RidsNroOdResource
RidsFsmeOdResource
RIdsCsoMailCenterResource
RidsRgn2MailCenterResource
RidsRgn47MailCenterResource
RidsNrrAdroResource
RidsAdmMailCenterResource
RidsHrMailCenterResource
RidsNrrOdResource
RidsResOdResource
RidsNsirOdResource
RidsRgn1MailCenterResource
RidsRgn3MailCenterResource
RidsNrrAdesResource

***Via email**

ADAMS ACCESSION NOS.:ML090070209 EDATS: NRR-2009-0003

OFFICE	NSIR*	NRR*	OGC*
NAME	BDean	ELeeds	BMizuno
DATE	4/08/09	3/ 27/09	4/ 09 /09

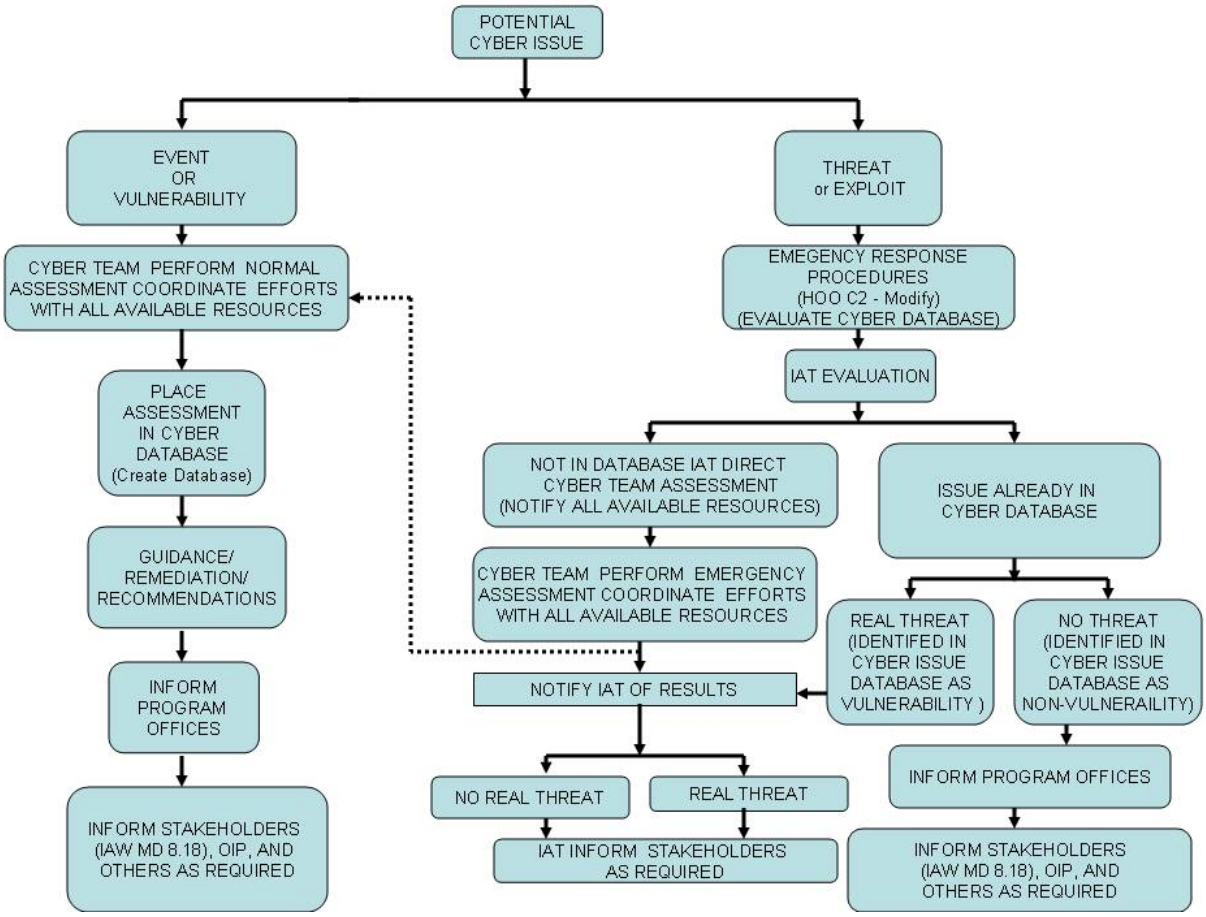
OFFICIAL RECORD COPY

Cyber Issue Assessment Process

The U.S. Nuclear Regulatory Commission will evaluate cyber-related security issues identified by stakeholders, mass media, and/or other governmental agencies associated with nuclear facilities.

Two types of cyber-related security assessments will be performed. The first type of assessment will occur after an operating issue or a potential cyber-related issue is identified (e.g.; event or vulnerability). The Cyber Assessment Team (CAT) will evaluate the event or issue using the expertise of all available members. The issue will be entered into a cyber security issue database and the team will make recommendations to program office management for addressing any potential concerns and also notify program offices and inform stakeholders in accordance with MD 8.18, "Generic Communications."

The second type of assessment will occur after the Information Assessment Team (IAT) receives information identifying a potential cyber-related security threat (e.g.; threat or exploit). The CAT will conduct reviews to provide technical assistance to the Information Assessment Team during cyber-related security threat assessments. The CAT member will be notified from a call list to assist the IAT as required. The CAT will evaluate the potential cyber-related security threat using all available resources.



Cyber Security Assessment Team
Organizational Structure

The CAT will be staffed with experts in cyber security from within the agency, re-employed annuitants, other federal agencies, and contractors when necessary. The number of experts at the NRC is limited, but currently there are experts in the offices of NRR, NRO, RES, NSIR, NMSS, CSO, and OIS. The office of NSIR will have responsibility to provide a team leader. The team will also establish informal cooperative agreements with experts in other Federal Agencies and the private sector (contractors) to assist in the assessment process.

Cyber Security Assessment Team
Budget Estimate

The budget estimates for the establishment and operation of the Cyber Security Assessment Team (CAT) was developed using the following assumptions:

- 1 FTE is equal to 1380 hours
- Estimated Start up (one time) investment for the CAT – 80 hours per member
- Estimated time for CAT member training – 40 hours per member year
- Estimated time for the assessment of cyber-related issues – 208 hours per member year
- Estimated time for the assessment of cyber-related events – 20 hours per member year
- Estimated time for communication of CAT activities – 20 hours per member year.

Based on the assumptions and the anticipated staffing level of the CAT provided above, the annual obligation of resources is estimated at 368 hours or 0.27 FTE for a primary team member and 0.14 FTE for an alternate member for the first year. This represents a total annualized agency obligation of resources for the start up and the first year of operation of the CAT at 2.45 FTE.