August 19, 2011

MEMORANDUM TO: Stephen D. Dingbaum
Assistant Inspector General for Audits

FROM: Patrick D. Howard, Director **/RA/**
Computer Security Office

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2010 (OIG-11-A-03)

This responds to the January 5, 2011, memorandum transmitting the subject audit report, which conveyed the findings and recommendations. With respect to your specific recommendations, I submit the following:

Recommendation 1:

Implement an automated tool to ensure the agency's POA&M [Plan of Action and Milestones] procedures are consistently implemented.

Response:

The U.S. Nuclear Regulatory Commission (NRC) has implemented an automated tool (Xacta) to ensure the agency's POA&M procedures are consistently implemented. Additionally, the NRC updated the POA&M process (ML111020360) to reflect the use of the automated tool. CSO recommends that this item be close.

Recommendation 2:

Perform more frequent independent verification and validation of POA&Ms to ensure POA&Ms include all known security weaknesses, including those identified in OIG [Office of Inspector General] audits, contingency plan testing, and annual security control testing, and to ensure POA&Ms are updated in a timely manner.

CONTACT: Paul Ricketts, CSO/FCOT
(301) 415-5708

Response:

NRC uses an automated tool (Xacta), which enables centralized management of POA&Ms, to perform more frequent independent verification and validation of POA&Ms to ensure POA&Ms include all known security weaknesses, including those identified in OIG audits, contingency plan testing, and annual security control testing, and to ensure POA&Ms are updated in a timely manner. NRC has updated section 3.5 of the POA&M process (ML111020360) to include more frequent independent verification and validation of POA&Ms. CSO recommends that this item be close.

Response:

NRC uses an automated tool (Xacta), which enables centralized management of POA&Ms, to perform more frequent independent verification and validation of POA&Ms to ensure POA&Ms include all known security weaknesses, including those identified in OIG audits, contingency plan testing, and annual security control testing, and to ensure POA&Ms are updated in a timely manner. NRC has updated section 3.5 of the POA&M process (ML111020360) to include more frequent independent verification and validation of POA&Ms. CSO recommends that this item be close.

DISTRIBUTION: G20110008/EDATS: OEDO-2011-0008

RidsCsoMailCenter	RidsEdoMailCenter	RidsOigMailCenter
RidsOgcMailCenter	J. Arildsen	P. Ricketts
S. Nevet		

ADAMS Accession No.: ML11229A383 (Pkg.); ML11229A539 (Memo)

OFFICE	CSO/FCOT	CSO/FCOT	CSO
NAME	SNevet	PRicketts	PHoward
DATE	8/17/2011	8/17/2011	8/19 /2011

OFFICIAL RECORD COPY