December 19, 2013

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

FROM: Darren B. Ash ***/RA/***
Deputy Executive Director
for Corporate Management
Office of the Executive Director for Operations

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2013 (OIG-14-A-03)

This responds to the November 22, 2013, memorandum transmitting the subject audit report, which conveyed the findings and recommendations of the Nuclear Regulatory Commission (NRC), Office of the Inspector General (OIG). With respect to the OIG's specific recommendations, I submit the following.

Recommendation 1:

Update the information in the NRC inventory for contractor systems to include missing information and to correctly classify contractor systems in accordance with CSO-PROS-2030, *NRC Risk Management Framework.*

Response:

Agree. The Computer Security Office (CSO) will formulate a plan of action to correct the inventory discrepancies related to cybersecurity fields, develop an inventory update process and procedure for the cybersecurity fields, and develop a tasking for contract support staff to update and maintain the cybersecurity fields of the inventory.

The Office of Information Services (OIS) will work with CSO to formulate a plan of action to ensure that all NRC systems, including contractor systems, are included in the inventory. OIS will request System Owners provide updated system information in the next inventory data call.

Completion Date: December 31, 2014

Point of Contact: Neil Forehand, OIS

Recommendation 2:

Based on the updated inventory of contractor systems, identify those that are not compliant with CSO-PROS-2030, *NRC Risk Management Framework,* and complete the appropriate authorization activities for those systems.

Response:

Agree. CSO is developing processes and oversight methods to ensure the system owners of contractor systems are compliant with CSO-PROS-2030, *NRC Risk Management Framework*, and will complete the appropriate authorization activities for those systems.

Completion Date: December 31, 2014

Point of Contact: Kathy Lyons-Burke, CSO

Recommendation 3:

Develop procedures for ensuring the annual IT [information technology] security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

Response:

Agree. CSO is developing processes and oversight methods to ensure the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

Completion Date: December 31, 2014

Point of Contact: Kathy Lyons-Burke, CSO

cc: Chairman Macfarlane
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

Recommendation 2:

Based on the updated inventory of contractor systems, identify those that are not compliant with CSO-PROS-2030, *NRC Risk Management Framework,* and complete the appropriate authorization activities for those systems.

Response:

Agree. CSO is developing processes and oversight methods to ensure the system owners of contractor systems are compliant with CSO-PROS-2030, *NRC Risk Management Framework*, and will complete the appropriate authorization activities for those systems.

Completion Date: December 31, 2014

Point of Contact: Kathy Lyons-Burke, CSO

Recommendation 3:

Develop procedures for ensuring the annual IT [information technology] security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

Response:

Agree. CSO is developing processes and oversight methods to ensure the annual IT security risk management activities for systems owned and/or operated by other agencies or contractors are completed in accordance with NRC requirements.

Completion Date: December 31, 2014

Point of Contact: Kathy Lyons-Burke, CSO

cc: Chairman Macfarlane
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

DISTRIBUTION: G20130826

RidsCsoMailCenter	RidsEdoMailCenter	RidsOigMailCenter
RidsSecyMailCenter	RidsOis Resource	KOlive, OEDO
JArildsen, OEDO	TRich, CSO	JFlanagan, OIS
KLyons-Burke, CSO	TGraham, CSO	MGivvines, OIS
CRheaume, OIS	NForehand, OIS	JFeibus, CSO

ADAMS Accession No.:ML13329A609(Pkg) ML13350A608(Memo) *email concurrence

OFFICE	CSO	CSO	CSO	OIS *	CSO	OEDO
NAME	GSomerville	KLyons-Burke SNevet for	JFeibus	ELeong	TRich	DAsh
DATE	12/ 17 /13	12/ 17 /2013	12/17 /13	12/ 17 /13	12/ 17 /13	12/19/13