February 23, 2015

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

FROM: Thomas W. Rich, Director**/RA Jonathan Feibus for/**
Computer Security Office

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

This memorandum is the U.S. Nuclear Regulatory Commission's update to the status of the proposed actions to resolve the recommendations identified in the Office of the Inspector General's independent evaluation of the agency's implementation of the Federal Information Security Management Act for Fiscal Year 2013.

Enclosure:
As stated

cc: Chairman Burns
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
SECY

CONTACT: Alan Sage, CSO/PCTT
301-415-7060

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

FROM: Thomas W. Rich, Director**/RA Jonathan Feibus for/**
Computer Security Office

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

This memorandum is the U.S. Nuclear Regulatory Commission's update to the status of the proposed actions to resolve the recommendations identified in the Office of the Inspector General's independent evaluation of the agency's implementation of the Federal Information Security Management Act for Fiscal Year 2013.

Enclosure:
As stated

cc: Chairman Burns
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
SECY

CONTACT: Alan Sage, CSO/PCTT
301-415-7060

Distribution: G20140045, CSO-2015-243

RidsCSOMailCenter Resource	RidsOISResource	CCorley, OEDO
JFeibus, CSO	KLyons-Burke, CSO	TGraham, CSO
ASage, CSO	GSomerville, CSO	DOffutt, OIS
TCarr, OIS		

ADAMS Accession No.: ML15051A214 (Pkg.) ML15051A230 (Memo) e-mail concurs *

OFFICE	CSO	CSO/PCTT	CSO/PCTT	OIS	CSO	CSO
NAME	GSomerville	ASage	KLyons-Burke	DOffutt	JFeibus	TRich for JFeibus
DATE	2/20/15	2/23/15	2/23/15	2/26/15 *	2/23/15	2/23/15

OFFICIAL RECORD COPY

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2013

OIG-14-A-03

Status of Recommendations

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.

Agency Response Dated December 19, 2013

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.

OIG Analysis to the Agency Response Dated December 19, 2013

The proposed action meets the intent of the recommendation. This recommendation will be closed when the Office of Inspector General (OIG) receives documentation that the inventory includes all systems, including contractor systems, and that the contractor systems are correctly classified.

Response/Status Update:

CSO formulated an approach to correct the inventory discrepancies related to computer security fields, and tasked support staff to update and maintain the computer security fields of the inventory. In conjunction with OIS, CSO worked to ensure that all NRC systems are included in the inventory. During FY2014, substantial progress was made in reducing errors, increasing the accuracy of inventory data, and updating the CSO inventory user guide. FY2015 efforts will include increased standardization of inventory nomenclature and continue to improve the accuracy and completeness of the data.

Target Completion Date: December 31, 2015

Point of Contact: Kathy Lyons-Burke

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2013

OIG-14-A-03

Status of Recommendations

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 appropriate authorization activities for those systems.

Agency Response Dated December 19, 2013

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.

OIG Analysis to the Agency Response Dated December 19, 2013

The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives documentation that the updated inventory of contractor systems has identified the systems not in compliance with CSO-PROS-2030, NRC Risk Management Framework, and the appropriate authorization activities for those systems have been completed.

Response/Status Update:

In calendar year 2014, testing of all systems categorized as contractor systems was completed, and authorization of these systems will be completed by the third quarter of FY2015. The next update of the annual risk management activities guidance is planned to include the explicit requirement that all contractor systems be authorized as per NRC policy.

Target Completion Date: June 30, 2015

Point of Contact: Kathy Lyons-Burke

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2013

OIG-14-A-03

Status of Recommendations

Recommendation 3

Develop procedures for ensuring 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.

Agency Response Dated December 19, 2013

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.

OIG Analysis to the Agency Response Dated December 19, 2013

The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives documentation of the procedures for ensuring 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.

Response/Status Update

The next updates of the NRC Information Security Continuous Monitoring Process (CSO-PROS-1323) and annual risk management activities guidance are planned to include the explicit requirement that all contractor systems be authorized as per NRC policy.

Target Completion Date: December 31, 2015

Point of Contact: Kathy Lyons-Burke