

December 29, 2014

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 2014 (OIG-15-A-002)

This responds to the November 22, 2014, 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 recommendation, I submit the following.

Recommendation:

In support of continuous monitoring, develop a plan and schedule for updating all NRC system security plans, as well as the NRC Information Security Program Plan, to reflect [the National Institute of Standards and Technology Special Publication] NIST SP 800-53, Revision 4 [Security and Privacy Controls for Federal Information Systems and Organizations].

Response:

Agree. The Computer Security Office (CSO) is developing a template to facilitate the agency's implementation of NIST SP 800-53, Revision 4. CSO is also adding the requirement to update all system security plans to ensure they are compliant with NIST SP 800-53, Revision 4, to the annual risk management memorandum. The target date for updating all system security plans is the end of fiscal year 2015.

Completion Date: September 30, 2015

Point of Contact: Kathy Lyons-Burke, CSO

cc: Chairman Macfarlane
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
Commissioner Burns
SECY

December 29, 2014

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 2014 (OIG-15-A-002)

This responds to the November 22, 2014, 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 recommendation, I submit the following.

Recommendation:

In support of continuous monitoring, develop a plan and schedule for updating all NRC system security plans, as well as the NRC Information Security Program Plan, to reflect [the National Institute of Standards and Technology Special Publication] NIST SP 800-53, Revision 4 [Security and Privacy Controls for Federal Information Systems and Organizations].

Response:

Agree. The Computer Security Office (CSO) is developing a template to facilitate the agency's implementation of NIST SP 800-53, Revision 4. CSO is also adding the requirement to update all system security plans to ensure they are compliant with NIST SP 800-53, Revision 4, to the annual risk management memorandum. The target date for updating all system security plans is the end of fiscal year 2015.

Completion Date: September 30, 2015

Point of Contact: Kathy Lyons-Burke, CSO

cc: Chairman Macfarlane
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
Commissioner Burns
SECY

DISTRIBUTION: OEDO-14-00801, CSO-2015-200
See next page

ADAMS Accession No.:ML14321A355 (Pkg.) ML14356A593

OFFICE	CSO	CSO/PCTT	CSO/PCTT	CSO	CSO	OEDO
NAME	GSomerville	ASage	KL Lyons-Burke	JFeibus	TRich	DAsh
DATE	12/ 22/14	12/ /14	12/23 /14	12/23/14	12/23/14	12/29/14

OFFICIAL RECORD COPY

DISTRIBUTION

RidsSecyMailCenter
RidsOigMailCenter
KOlive, OEDO
JArildsen, OEDO
CCapernter, ADM
JMoses, OIS
CHaney, NMSS
GTracy, NRO
KSWest, RES
MCohen, OCHCO
RElisbuy, ADM
CDebnam, OIS
SStothoff, NMSS
EMadden OIS
BTharp, NSIR
SRupinta, RES
GLopez, OIS
WLawson, OCHCO
OBenjumea, NRR

RidsEdoMailCenter
RidsCsoMailCenter
CCorley, OEDO
TGraham, CSO
CRheaume, OIS
MWylie, OCFO
RWebber, OIS
JWiggins, NSIR
CPederson, RIII
BDean, NRR
KDerr, OIS
KBrosky, OCFO
JHughes, OIS
NBallam, NRO
KBrosky, OCFO
RKristobek, NSIR
JFoltz, RIII
RDeavers, ADM