UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

November 29, 2017

MEMORANDUM TO: Dr. Brett M. Baker
Assistant Inspector General for Audits
Office of the Inspector General

FROM: Frederick D. Brown ***/RA by Kimberly A. Howell for/***
Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration and Human Capital Programs
Office of the Executive Director for Operations

SUBJECT: RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S INDEPENDENT EVALUATION OF THE NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017, DATED OCTOBER 30, 2017 (OIG-18-A-02)

This memorandum responds to the October 30, 2017, memorandum transmitting OIG-18-A-02, "Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017." The U.S. Nuclear Regulatory Commission (NRC) staff generally agrees with the Office of the Inspector General's (OIG's) findings and recommendations.

The OIG report makes seven recommendations to improve the management of the NRC's implementation of the Federal Information Security Modernization Act of 2014 for fiscal year 2017. Enclosed please find the NRC staff's responses to OIG's recommendations from the evaluation report.

Enclosure:
NRC's Response to OIG-18-A-02

CONTACT: Allen K. Sullivan, OCIO/GEMSD
(240) 415-8950

Response to the Office of the Inspector General's Independent Evaluation of the Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017, Dated October 30, 2017 (OIG-18-A-02)
DATE: November 29, 2017

DISTRIBUTION: OEDO-17-00685 (OIG-18-A-02)
RidsOCIO Resource
RidsOIGMailCenter
RidsEdoMailCenter
RidsOGCMailCenter
RidsADM Resource

ADAMS Accession No.: Pkg. ML17304A101 *Concurred via e-mail

OFFICE	QTE*	OCIO/GEMSD/ISPOB*	OCIO/GEMSD/ISPOB*	OCIO/GEMSD/DD*
NAME	JDougherty	AEskandary	ASullivan (BDabbs for)	JFeibus
DATE	11/21/2017	11/17/2017	11/21/2017	11/20/2017
OFFICE	OCIO/GEMSD/D*	OGC*	OCIO	DEDM
NAME	JMoses	MNorris	DNelson	FBrown KHowell for
DATE	11/20/2017	11/22/2017	11/27/2017	11/29/2017

OFFICIAL RECORD COPY

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 1:	Perform a gap analysis to identify required IT security program documents, IT security program documents that need to be developed, and IT security program documents that need to be updated and/or finalized.
Agency Response Dated November 16, 2017:	Agree. The NRC's Office of the Chief Information Officer (OCIO) will conduct an analysis to identify required IT security program documents that need to be developed or that need to be updated and/or finalized. **Target Completion Date:** April 30, 2018 **Point of Contact:** Allen K. Sullivan, (240) 415-8950
Recommendation 2:	Develop a schedule for developing, updating, and completing all required IT security program documentation.
Agency Response Dated November 16, 2017:	Agree. The NRC's Office of the Chief Information Officer will develop a schedule for developing, updating and completing all required IT security program documentation. **Target Completion Date:** June 30, 2018 **Point of Contact:** Allen K. Sullivan, (240) 415-8950
Recommendation 3:	Develop policies and procedures for keeping IT security program documentation up-to-date.
Agency Response Dated November 16, 2017:	Agree. The NRC's Office of the Chief Information Officer will develop policies and procedures for keeping IT security program documentation up-to-date. **Target Completion Date:** June 30, 2018 **Point of Contact:** William T. Dabbs, (301) 415-0524

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2017 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 4:	Develop and implement a schedule for reviewing and updating all security categorizations.
Agency Response Dated November 16, 2017:	Agree. The NRC's Office of the Chief Information Officer will develop and implement a schedule for reviewing and updating all security categorizations. **Target Completion Date:** December 31, 2018 **Point of Contact:** William T. Dabbs, (301) 415-0524
Recommendation 5:	Develop and implement a schedule for reviewing and updating all business impact assessments and for developing them if they are missing.
Agency Response Dated November 16, 2017:	Agree. The NRC's Office of the Chief Information Officer will develop and implement a schedule for reviewing and updating all existing business impact assessments and will develop any that are missing. **Target Completion Date:** December 31, 2018 **Point of Contact:** Carl W. Bauer, (301) 415-5842
Recommendation 6:	Develop and implement a schedule for reviewing and updating all contingency plans.
Agency Response Dated November 16, 2017:	Agree. The NRC's Office of the Chief Information Officer will develop and implement a schedule for reviewing and updating all contingency plans. **Target Completion Date:** December 31, 2018 **Point of Contact:** Michael D. Mangefrida, (301) 415-2264

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2017 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 7:	Develop procedures for monitoring completion of all continuous monitoring activities, including those that are not explicitly tracked on the Cybersecurity Risk Dashboard.
Agency Response Dated November 16, 2017:	Agree. The NRC's Office of the Chief Information Officer will develop procedures for monitoring the completion of all continuous monitoring activities, including those that are not explicitly tracked on the Cybersecurity Risk Dashboard. **Target Completion Date:** December 31, 2018 **Point of Contact:** Alan J. Sage, (301) 415-7060