




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

August 31, 2022

MEMORANDUM TO: Those on the Attached List  Signed by Nelson, David  
on 08/31/22

FROM: David J. Nelson, Chief Information Officer  
Office of the Chief Information Officer

SUBJECT: FISCAL YEAR 2023 CYBERSECURITY RISK MANAGEMENT  
ACTIVITIES

I want to express my appreciation for your continued efforts to improve the U.S. Nuclear Regulatory Commission's (NRC's) cybersecurity posture and the agency's goal to minimize security risks. These improvements have come through the hard work of you and your staff and are reflected in our Quarterly Federal Information Security Management Act ratings and audits conducted by the Government Accountability Office and our Inspector General. These improvements come with additional scrutiny, and continued attention is needed to ensure that we maintain our risk posture and the security controls over the NRC's information systems and data in light of the constantly changing threat landscape.

The Federal Information Security Modernization Act of 2014 (FISMA) and our implementing framework delineate the risk management activities that we are required to conduct periodically. This past year, the National Institute of Standards and Technology also introduced expanded guidance through the release of Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," issued September 2020. The control enhancements include a focus on supply chain risk management as well as additional privacy considerations, among other outcome-based controls. They include the following:

- system security categorization
- privacy threshold analysis and privacy impact assessment updates
- system cybersecurity assessments
- periodic reviews and risk management reporting
- contingency planning and testing
- continuous monitoring of NRC FISMA systems
- cybersecurity and privacy awareness training
- cybersecurity role-based training

CONTACT: Garo Nalabandian, OCIO/CISO  
301-415-8421

Additionally, given the recent Cybersecurity Executive Order 14028, “Improving the Nation’s Cybersecurity,” dated May 12, 2021, and the related Office of Management and Budget directives, agencies are required to modernize and implement cybersecurity standards, transition to secure cloud services, adopt a zero-trust architecture, and enable endpoint detection and response and enhanced logging throughout systems and networks. These activities will require additional investments to support meeting the increased requirements.

Succeeding in such important efforts requires support from all NRC office directors, Regional Administrators, and system owners. The agency’s success also depends on completion of the risk management activities outlined in the enclosed Cybersecurity Risk Management Activities Instructions, Fiscal Year 2023. The instructions provide detailed guidance on the required activities, such as making the specified documentation available to required staff, including the Office of the Inspector General.

Contract vehicles are available to NRC Headquarters and regional offices to support these activities. If you require contract support, please ensure that sufficient resources and time are available by coordinating requirements with your designated contracting officer’s representative for cybersecurity program support services.

Additionally, I will continue to focus on ensuring that the agency identifies needed resources in the budget formulation process for all aspects of required cybersecurity for the life of its systems, including plans for hardware and software upgrades, maintenance, and system changes.

Please feel free to contact Garo Nalabandian or me with questions. As always, I expect and appreciate your support as we work to jointly accomplish the agency’s mission and minimize cybersecurity risk to the NRC.

Enclosure:

1. Cybersecurity Risk Management Activities Instructions, Fiscal Year 2023

SUBJECT: FISCAL YEAR 2023 CYBERSECURITY RISK MANAGEMENT  
ACTIVITIES 8/31/22

**DISTRIBUTION**

See Next Page

**ADAMS Accession Number: ML22230A151**

**\*via email**

OFFICE	OCIO/GEMSD/COT	QTE*	OCIO/GEMSD/COT	OCIO/GEMSD/CSB
NAME	ASage	JDougherty	BBauer	BPartlow
DATE	08/18/2022	08/12/2022	08/19/2022	08/29/2022
OFFICE	OCIO/CISO	OCIO/GEMSD/DD	OCIO/GEMSD/D	OCIO/D
NAME	GNalabandian	DSilberfeld	JFeibus	DNelson
DATE	08/29/2022	08/30/2022	08/30/2022	08/31/2022

**OFFICIAL RECORD COPY**

MEMORANDUM TO THOSE ON THE ATTACHED LIST DATED:

August 31, 2022

Scott W. Moore, Executive Director, Advisory Committee  
on Reactor Safeguards

E. Roy Hawkens, Chief Administrative Judge, Atomic Safety  
and Licensing Board Panel

Marian L. Zobler, General Counsel

Jody C. Martin, Director, Office of Commission  
Appellate Adjudication

Cherish K. Johnson, Chief Financial Officer

Robert J. Feitel, Inspector General

Nader L. Mamish, Director, Office of International Programs

Eugene Dacus, Director, Office of Congressional Affairs

David A. Castelveter, Director, Office of Public Affairs

Brooke P. Clark, Secretary of the Commission

Daniel H. Dorman, Executive Director for Operations

Cathy Haney, Deputy Executive Director for Materials,  
Waste, Research, State, Tribal, Compliance, Administration,  
and Human Capital Programs, OEDO

Darrell Roberts, Deputy Executive Director for Reactor  
and Preparedness Programs, OEDO

Marissa Bailey, Assistant for Operations, OEDO

Jennifer M. Golder, Director, Office of Administration

David J. Nelson, Chief Information Officer

Mark Lombard, Director, Office of Enforcement

Tracy T. Higgs, Acting Director, Office of Investigations

Mary A. Lamary, Chief Human Capital Officer

John Lubinski, Director, Office of Nuclear Material Safety  
and Safeguards

Andrea Veil, Acting Director, Office of Nuclear Reactor  
Regulation

Raymond V. Furstenau, Director, Office of Nuclear Regulatory  
Research

Vonna L. Ordaz, Director, Office of Small Business and Civil  
Rights

Mirela Gavrilas, Director, Office of Nuclear Security  
and Incident Response

David C. Lew, Regional Administrator, Region I

Laura A. Dudes, Regional Administrator Region II

John B. Giessner, Regional Administrator, Region III

Scott A. Morris, Regional Administrator, Region IV

**E-Mail Mail Stops**

RidsACRS\_MailCTR Resource

RidsAslbpManagement Resource

RidsOgcMailCenter Resource

RidsOcaaMailCenter Resource

RidsOcfoMailCenter Resource

RidsOigMailCenter Resource

RidsOipMailCenter Resource

RidsOcaMailCenter Resource

RidsOpaMail Resource

RidsSecyMailCenter Resource

RidsEdoMailCenter Resource

RidsEdoMailCenter Resource

RidsEdoMailCenter Resource

RidsEdoMailCenter Resource

RidsAdmMailCenter Resource

RidsOCIO Resource

RidsOeMailCenter Resource

RidsOiMailCenter Resource

RidsOchcoMailCenter Resource

RidsNmssOd Resource

RidsNrrOd Resource **(I)**

RidsNrrMailCenter Resource **(A)**

RidsResOd Resource **(I)**

RidsResPmdaMail Resource **(A)**

RidsSbcrMailCenter Resource

RidsNsirOd Resource **(I)**

RidsNsirMailCenter Resource **(A)**

RidsRgn1MailCenter Resource

RidsRgn2MailCenter Resource

RidsRgn3MailCenter Resource

RidsRgn4MailCenter Resource