January 15, 2015

MEMORANDUM TO: Those on the Attached List

FROM: Mark A. Satorius ***/RA/***
Executive Director for Operations

SUBJECT: FISCAL YEAR 2015 CYBERSECURITY RISK MANAGEMENT ACTIVITIES

First, I want to express my appreciation for your efforts in managing activities to continuously improve the agency's cybersecurity posture. The Nuclear Regulatory Commission (NRC) did make progress enhancing its cybersecurity posture in Fiscal Year (FY) 2014; however, like other federal institutions, NRC experienced an increased level of attack attempts and computer security incidents in comparison to FY 2013. Evidence of increased attack activity directed toward the NRC is shown in the 18 percent increase from 293 computer security incidents in FY 2013 to 346 incidents that we reported to the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team in FY 2014. I also wish to acknowledge the seriousness of what Federal agencies, including the NRC, are facing. For example, in 2014, a number of other Federal agencies were impacted by cybersecurity incidents resulting in major disruptions to their operations and necessitating costly remediation efforts.

The purpose of the cybersecurity risk management activities described herein is to identify, control, and continuously reduce the cybersecurity operating risk to the NRC mission. Our understanding of NRC's operating environment (current and evolving), the information we maintain, and the technologies connected to it allow us to make balanced, risk informed decisions and focus our resources on the most important things. On that very point, reflecting on the discussions at the most recent Senior Leadership Meeting, and feedback received by the Project AIM team, I ask that you work with the Computer Security Office over the coming months to re-examine the processes and practices used to comply with the Federal Information Security Management Act. These activities, and the process and practice improvements we make, provide benefits to the NRC that improve mission efficiency and effectiveness in our use of information technology and information systems as well as improve office and region preparedness to proactively and authoritatively respond to ongoing internal and external independent audits or evaluations.

It is essential that all NRC Office Directors, Regional Administrators and System Owners continue to fully engage in performing the FY 2015 Risk Management Activities. These activities are necessary to minimize the cybersecurity risk and reduce their potential negative impacts to the NRC mission, and are outlined in the enclosed "Cybersecurity Risk Management Activities Instructions for Fiscal Year 2015."

CONTACT: Thomas Rich, CSO
301-415-6596

During FY 2014, the agency continued efforts to improve its cybersecurity risk posture by developing a Cybersecurity Risk Dashboard (CRDB). This multiyear project supports the agency's mission by identifying and quantifying the cybersecurity risk posture of the agency, increasing the communication and awareness of risk, informing and prioritizing cybersecurity and business line investments, and facilitating efforts to balance security controls and mission risk. The dashboard displays many of the cybersecurity risk management activities discussed in the enclosure to this memorandum. The plan for FY 2015 is to expand the CRDB by providing summary displays for additional offices, refining the metrics and risk scoring, and supporting Quarterly Risk Management briefings with the Deputy Executive Directors for Operations, who also serve as the NRC's Designated Approving Authority. In addition, for FY 2015, the Computer Security Office (CSO) is refining the system authorization process and improving the system used to manage Plan of Action and Milestones (POA&M).

As you are aware, cyber risk management activities must be included in your annual Operating Plan with appropriate funding. In addition, evidence of completion of these activities is provided to the Inspector General as part of the annual independent evaluation of the Federal Information Security Management Act. To enable an agency-wide perspective of cybersecurity risk the CSO provides periodic updates on the completion of these activities to the Designated Approving Authority.

The enclosure provides detailed instructions on the required activities, including instructions for making the specified documentation available to CSO. CSO contract vehicles are available to offices and regions to support these cybersecurity risk management activities. If you desire to use this support, please ensure sufficient resources and schedule are available by coordinating requirements with your designated Cyber Security Program Support Services Contracting Officer's Representative.

Enclosure:
As stated

cc: D. Ash, DEDCM
M. Weber, DEDMRT
M. Johnson, DEDR

During FY 2014, the agency continued efforts to improve its cybersecurity risk posture by developing a Cybersecurity Risk Dashboard (CRDB). This multiyear project supports the agency's mission by identifying and quantifying the cybersecurity risk posture of the agency, increasing the communication and awareness of risk, informing and prioritizing cybersecurity and business line investments, and facilitating efforts to balance security controls and mission risk. The dashboard displays many of the cybersecurity risk management activities discussed in the enclosure to this memorandum. The plan for FY 2015 is to expand the CRDB by providing summary displays for additional offices, refining the metrics and risk scoring, and supporting Quarterly Risk Management briefings with the Deputy Executive Directors for Operations, who also serve as the NRC's Designated Approving Authority. In addition, for FY 2015, the Computer Security Office (CSO) is refining the system authorization process and improving the system used to manage Plan of Action and Milestones (POA&M).

As you are aware, cyber risk management activities must be included in your annual Operating Plan with appropriate funding. In addition, evidence of completion of these activities is provided to the Inspector General as part of the annual independent evaluation of the Federal Information Security Management Act. To enable an agency-wide perspective of cybersecurity risk the CSO provides periodic updates on the completion of these activities to the Designated Approving Authority.

The enclosure provides detailed instructions on the required activities, including instructions for making the specified documentation available to CSO. CSO contract vehicles are available to offices and regions to support these cybersecurity risk management activities. If you desire to use this support, please ensure sufficient resources and schedule are available by coordinating requirements with your designated Cyber Security Program Support Services Contracting Officer's Representative.

Enclosure:
As stated

cc: D. Ash, DEDCM
M. Weber, DEDMRT
M. Johnson, DEDR

DISTRIBUTION:
KBrock, OEDO
CCorley, OEDO
JPetsch, CSO
All ISSOs
ISSO branch chiefs

ADAMS Accession No.: ML14302A400 (Memo) ML14302A346 (Pkg)ML14302A382 (Encl.)

OFFICE	CSO	CSO	CSO	CSO	OEDO	OEDO
NAME	ASage	KLyons-Burke	TGraham	TRich/Jon Feibus for	DAsh	MSatorius
DATE	11/21/14	11/24/14	12/5/14	12/5/14	1/13/15	1/15/15

MEMORANDUM TO THOSE ON THE ATTACHED LIST DATED: January 15, 2015
SUBJECT: FISCAL YEAR 2015 CYBERSECURITY RISK MANAGEMENT ACTIVITIES

	E-Mail Mail Stops
Edwin M. Hackett, Executive Director, Advisory Committee on Reactor Safeguards	RidsAcrsAcnw_MailCTR Resource
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel	RidsAslbpManagement Resource
Margaret M. Doane, General Counsel	RidsOgcMailCenter Resource
Brooke D. Poole, Director, Office of Commission Appellate Adjudication	RidsOcaaMailCenter Resource
Maureen E. Wylie, Chief Financial Officer	RidsOcfoMailCenter Resource
Hubert T. Bell, Inspector General	RidsOigMailCenter Resource
Nader L. Mamish, Director, Office of International Programs	RidsOipMailCenter Resource
Eugene Dacus, Acting Director, Office of Congressional Affairs	RidsOcaMailCenter Resource
Eliot B. Brenner, Director, Office of Public Affairs	RidsOpaMail Resource
Annette Vietti-Cook, Secretary of the Commission	RidsSecyMailCenter Resource RidsSecyCorrespondenceMCTR Resource
Melanie A. Galloway, Assistant for Operations, OEDO	RidsEdoMailCenter Resource
Cynthia A. Carpenter, Director, Office of Administration	RidsAdmMailCenter Resource
Thomas W. Rich, Director, Computer Security Office	RidsCsoMailCenter Resource
Patricia K. Holahan, Director, Office of Enforcement	RidsOeMailCenter Resource
Cheryl L. McCrary, Director, Office of Investigations	RidsOiMailCenter Resource
James P. Flanagan, Director, Office of Information Services	RidsOis Resource
Miriam L. Cohen, Chief Human Capital Officer	RidsHrMailCenter Resource
Glenn M. Tracy, Director, Office of New Reactors	RidsNroOd Resource **(I)** RidsNroMailCenter Resource **(A)**
Catherine Haney, Director, Office of Nuclear Material Safety and Safeguards	RidsNmssOd Resource
William M. Dean, Director, Office of Nuclear Reactor Regulation	RidsNrrOd Resource **(I)** RidsNrrMailCenter Resource **(A)**
Brian W. Sheron, Director, Office of Nuclear Regulatory Research	RidsResOd Resource **(I)** RidsResPmdaMail Resource **(A)**
Vonna Ordaz, Director, Office of Small Business and Civil and Rights	RidsSbcrMailCenter Resource
James T. Wiggins, Director, Office of Nuclear Security and Incident Response	RidsNsirOd Resource **(I)** RidsNsirMailCenter Resource **(A)**
Daniel Dorman, Regional Administrator, Region I	RidsRgn1MailCenter Resource
Victor M. McCree, Regional Administrator, Region II	RidsRgn2MailCenter Resource
Cynthia D. Pederson, Regional Administrator, Region III	RidsRgn3MailCenter Resource
Marc L. Dapas, Regional Administrator, Region IV	RidsRgn4MailCenterResource