

April 13, 2016

MEMORANDUM TO: Frederick D. Brown, Acting Chief Information Officer
Office of the Chief Information Officer

FROM: Marissa G. Bailey, Director */RA/ S. Coffin for*
Division of Preparedness and Response
Office of Nuclear Security and Incident Response

SUBJECT: IMPLEMENTATION OF RECOMMENDATIONS FROM THE INCIDENT
RESPONSE STANDARDIZATION PROJECT

In April of 2015, Robert Lewis commissioned the Incident Response Standardization Project (IRSP) to explore options which would improve the effectiveness and efficiency of information technology (IT) assets which support the agency's incident response program. This effort has been completed, and the Working Group and Steering Committee recommendations have been provided to me by memorandum dated November 24, 2015, (ML15328A277). I endorse the following recommendations from the IRSP Executive Steering Committee.

Recommendation 1: Expand the Incident Response Oversight Committee (IROC) to include the Chief of the Operations Branch, and explicitly define the IROC's authority to establish and maintain standards for use of communication and IT assets for IRP implementation in the IROC Charter. To ensure alignment on major programmatic items, the IROC should be guided by the Director, NSIR/DPR that has decision-making authority for setting program direction. The IROC charter will be revised to incorporate this recommendation in its entirety. The new charter should be in place by mid 2016.

Recommendation 2: Explore the use of Government Furnished Equipment in the IRCs for immediate cost savings. NSIR will evaluate the cost and potential benefits of purchasing vs. leasing equipment as part of the next HOC workstation refresh in 2017. The new Operations Center Information Management System (OCIMS) support contract, which will be in force at the end of March 2016 includes options to increase the flexibility of the contract vehicle. NSIR is also monitoring the efforts of OCIO and ADM to negotiate a new IT Infrastructure Services and Support contract vehicle. In the interim, NSIR is working to virtualize the 27 physical servers which support the incident response program, using hardware provided by OCIO, in an effort to reduce operating costs and improve efficiency. The transition of the servers to the virtualized platform should be completed by the end of CY 2016. Further virtualization of physical systems will be explored in ongoing budget years to the extent that it is practical.

Recommendation 3: Establish a formal change control process, for procurement, servicing, and use of IT and communication assets. NSIR intends to implement a change management process, similar to the one currently used by OCIO, to ensure that changes to the IT infrastructure supporting the Incident Response Program are coordinated and managed correctly. This process will include elements to assess, prioritize fund, implement, and track changes to incident response facilities and IT and communications assets. The change management process will be implemented by mid 2016.

Recommendation 4: Establish a single Authority to Operate (ATO) for all Incident Response facilities. NSIR will coordinate this effort with the Information Security Directorate. The Information Security Directorate of OCIO will have the lead for this effort. NSIR will work with OCIO/ISD to develop and implement an integrated ATO to support all incident response equipment. OCIO/ISD is already working with the regional offices to develop a generic ATO for each of the regions. NSIR intends to leverage this ongoing work to merge portions of these ATOs with the existing one supporting the HOC.

Recommendation 5: Perform a full Business Process Improvement (BPI) review of the Incident Response Program (IRP) to evaluate the need for regional Incident Response Centers and the merits of phasing them out. The results of the BPI would be used to define the IRP functional design, responder roles and responsibilities and to prescribe the facility design, responder tools and their intended use. NSIR/DPR will perform an in-depth evaluation of the current Incident Response Program. This evaluation will utilize assets from within NSIR and should be completed in late 2017. Insights gleaned from the evaluation will be used to inform staffing and facility requirement decisions for the HOC and the Regional Incident Response Centers during outgoing budget years.

CONTACT: Bernard W. Stapleton, NSIR/DPR
(301) 287-3532

Recommendation 4: Establish a single Authority to Operate (ATO) for all Incident Response facilities. NSIR will coordinate this effort with the Information Security Directorate. The Information Security Directorate of OCIO will have the lead for this effort. NSIR will work with OCIO/ISD to develop and implement an integrated ATO to support all incident response equipment. OCIO/ISD is already working with the regional offices to develop a generic ATO for each of the regions. NSIR intends to leverage this ongoing work to merge portions of these ATOs with the existing one supporting the HOC.

Recommendation 5: Perform a full Business Process Improvement (BPI) review of the Incident Response Program (IRP) to evaluate the need for regional Incident Response Centers and the merits of phasing them out. The results of the BPI would be used to define the IRP functional design, responder roles and responsibilities and to prescribe the facility design, responder tools and their intended use. NSIR/DPR will perform an in-depth evaluation of the current Incident Response Program. This evaluation will utilize assets from within NSIR and should be completed in late 2017. Insights gleaned from the evaluation will be used to inform staffing and facility requirement decisions for the HOC and the Regional Incident Response Centers during outgoing budget years.

CONTACT: Bernard W. Stapleton, NSIR/DPR
(301) 287-3532

Distribution:

B. Stapleton/NSIR
R. Stransky/NSIR
S. Coffin/NSIR
F. Brown/OCIO

ADAMS Accession Nos.: ML16084A686

Office	NSIR/DPR	NSIR/DPR	NSIR/DPR
Name	R. Stransky	B. Stapleton	S. Coffin
Date	03/30/16	04/06/16	04/06/16

OFFICIAL RECORD COPY