Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL
INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2012
Technology Governance
(OIG-13-A-03)

Status of Recommendation

Recommendation 7:   Provide refresher training to all staff responsible for implementing NRC's Plan of Action and Milestones (POA&M) process.

Agency Response Dated
October 31, 2013:   In an effort to integrate the POA&M process into the U.S. Nuclear Regulatory Commission (NRC) Enterprise Risk Management (ERM) program, the Computer Security Office (CSO) is focusing on risk management activities that change the focus from the current system-by-system approach to an enterprise system portfolio view. That allows for the prioritization of POA&M items across systems and better utilization of resources. This will require changes to the current POA&M process. CSO anticipates completing the necessary updates to the process by the end of the second quarter of fiscal year (FY) 2014 and will provide the training by the end of the fourth quarter of FY2014.

Original Target Completion Date: September 30, 2013
Revised Target Completion Date: September 30, 2014

OIG Analysis: The proposed action meets the intent of the recommendation. This recommendation will be closed when the Office of the Inspector General (OIG) receives verification that the refresher training has been provided.

Status: CSO continues to review the POA&M training/briefing materials. Upon CSO approval of these materials, CSO will begin scheduling training sessions. CSO now expects training to occur during FY2015. This delay is attributable to a 40% staffing level in the team responsible for this effort. However, CSO has continued its efforts to acquire the needed staff, which is nearing completion. As a result, CSO will continue to work toward completing the refresher training required to close this audit recommendation.

Current Target Completion Date: December 15, 2015

Point of Contact: Kathy Lyons-Burke, 301-415-6595

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL
INFORMATION SECUIRTY MANAGEMENT ACT FOR FISCAL YEAR 2012
Technology Governance
(OIG-13-A-03)

Status of Recommendation

Recommendation 8:   Configure the agency's automated POA&M tool to do the
following: (i) prevent scheduled completion dates from being
changed, (ii) prevent weaknesses from being created without a
scheduled completion date or weakness source, (iii) prevent
weaknesses from being closed without specifying an actual date
closed, (iv) prevent users from entering actual completion dates in
the future, (v) prevent users from entering an actual completion
date when the status is not closed, and (vi) automatically change
the weakness status from on track to delayed once the scheduled
completion date has passed.

Agency Response Dated
October 31, 2013:   CSO has coordinated with the vendor to implement these
configuration recommendations. Our analysis determined that these
items do not work as designed, and vendor modifications are required
as a result of the functionality of the current POA&M tool. The NRC
submitted change requests to the vendor to implement the identified
modifications. In the current version of the tool, the vendor corrected
deficiencies identified in Recommendations 8(iii), 8(iv), and 8(v).
Modifications to address findings in Recommendations 8(i), 8(ii),
and 8(vi) are still under review by the vendor, with no target date
for correcting these findings. The current target completion date
remains valid.

Original Target Completion Date: September 30, 2013
Revised Target Completion Date: September 30, 2014

OIG Analysis: The proposed action meets the intent of the recommendation.
This recommendation will be closed when OIG receives
verification that the agency's POA&M tool has been configured as
discussed in the recommendation.

Status: CSO has coordinated with the vendor to implement these
recommendations, but the staff has determined that these items do
not function as designed. As a result, the NRC requires additional
vendor modifications to ensure that the current POA&M tool is
properly configured to fulfill the stated recommendations, and the
NRC has submitted related change requests to the vendor.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL
INFORMATION SECUIRTY MANAGEMENT ACT FOR FISCAL YEAR 2012
Technology Governance
(OIG-13-A-03)

Status of Recommendation

The vendor has developed a new version of the POA&M tool,
which is currently under evaluation and testing in the Centralized
Testing Facility (CTF). In the interim, the National Institutes for
Standards and Technology (NIST) finalized Revision 4 of Special
Publication 800-53, "Security and Privacy Controls for Federal
Information Systems and Organizations." The current version of
the vendor's tool will allow the NRC to conform to the latest format
requirements. Additional time in the CTF and in production testing
will be required to finalize these changes.

Current Target Completion Date: December 15, 2015

Point of Contact: Kathy Lyons-Burke, 301-415-6595

Recommendation 10:   Update IT environment contingency plan to update contingency
planning procedures specific to NRC remote locations that are not
up-to-date. Specifically, update the list of IT environment servers
supporting NRC remote locations that are referenced in Appendix
H of the IT environment contingency plan and update the
contingency plans for NRC remote locations that are attached to
the IT environment contingency plan.

**Agency Response Dated
October 31, 2013:**   Subsequent to the status update provided on July 19, 2013, the
Office of Information Services (OIS) determined that where
Information Technology (IT) components are not currently
included within an existing IT system boundary, each NRC remote
office (Regions I–IV and the Technical Training Center (TTC))
should consolidate such components into a single IT system for
the given remote office. Toward that end, the remote offices are
currently preparing Federal Information Safety Management Act
(FISMA)-compliant Authority to Operate (ATO) documentation for
these systems, and this documentation will include updated
contingency procedures that will be added to Appendix H of the
Information Technology Infrastructure (ITI) Contingency Plan as
soon as they become available. However, OIS anticipates the
need to extend the target completion date for this
recommendation to allow for completion of the ATO process.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL
INFORMATION SECUIRTY MANAGEMENT ACT FOR FISCAL YEAR 2012
Technology Governance
(OIG-13-A-03)

Status of Recommendation

Original Target Completion Date: September 30, 2013
Revised Target Completion Date: August 30, 2014

OIG Analysis:

The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS has updated the appropriate system contingency plans.

Status:

The Regional offices and TTC continue to work with CSO to complete their FISMA documentation for an updated ATO. Once the Regional offices have completed their ATO, their updated contingency plans will be added to Appendix H of the ITI Contingency Plan document. As anticipated, the target completion date for this recommendation needs to be extended to allow for the completion of the ATO process.

Current Target Completion Date: August 30, 2015

Point of Contact:

Michael Williams, 301-287-0660

Recommendation 11:

Update the IT environment contingency plan to include contingency procedures for the IT environment and other IT components supporting the one NRC remote location for which these procedures are missing.

Agency Response Dated October 31, 2013:

Subsequent to the status update provided on July 19, 2013, OIS determined that where IT components are not currently included within an existing IT system boundary, the TTC should consolidate such components into a single IT system. Toward that end, the TTC is currently preparing FISMA-compliant ATO documentation for this system, and this documentation will include updated contingency procedures that will be added to Appendix H of the ITI Contingency Plan as soon as they become available. However, OIS anticipates the need to extend the target completion date for this recommendation to allow for completion of the ATO process.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL
INFORMATION SECUIRTY MANAGEMENT ACT FOR FISCAL YEAR 2012
Technology Governance
(OIG-13-A-03)

Status of Recommendation

Original Target Completion Date: September 30, 2013
Revised Target Completion Date: August 30, 2014

OIG Analysis:
The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS has updated the IT environment contingency plan to include contingency procedures for the IT environment and other IT components supporting the one NRC remote location for which these procedures are missing.

Status:
The Regional offices and TTC continue to work with CSO to complete their FISMA documentation for an updated ATO. Once the Regional offices have completed their ATO, their updated contingency plans will be added to Appendix H of the ITI Contingency Plan document. As anticipated, the target completion date for this recommendation needs to be extended to allow for the completion of the ATO process.

Current Target Completion Date: August 30, 2015

Point of Contact:
Michael Williams, 301-287-0660

Recommendation 12:
Update the COOPs (Continuity of Operations Plans) for NRC remote locations that are referenced in Appendix G of the IT environment contingency plan to include current IT environment configurations at NRC remote locations and to address situations where the IT environment at those locations is unavailable for any reason.

Agency Response Dated October 31, 2013:
Subsequent to the status update provided on July 19, 2013, OIS determined that where IT components are not currently included within an existing IT system boundary, each NRC remote office (Regions I–IV and the TTC) should consolidate such components into a single IT system for the given remote office. Toward that end, the remote offices are currently preparing FISMA-compliant ATO documentation for these systems, and this documentation will include updated COOPs that will be added to Appendix G of the ITI Contingency Plan as soon as they become available.

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL
INFORMATION SECUIRTY MANAGEMENT ACT FOR FISCAL YEAR 2012
Technology Governance
(OIG-13-A-03)

Status of Recommendation

However, OIS anticipates the need to extend the target completion date for this recommendation to allow for completion of the ATO process.

Original Target Completion Date: September 30, 2013
Revised Target Completion Date: August 30, 2014

OIG Analysis:	The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that OIS updated the COOPs for NRC remote locations that are referenced in Appendix G of the IT environment contingency plan to include current IT environment configurations at NRC remote locations and to address situations where the IT environment at those locations is unavailable for any reason.
Status:	CSO continues to review the POA&M training and briefing materials. Upon CSO approval of these materials, CSO will begin scheduling training sessions. Staff expects to schedule training for FY2014 and FY2015. The Regional offices and TTC continue to work with the CSO to complete their FISMA documentation for an updated ATO. Once the Regional offices have completed their ATO, the updated contingency plans will be added to Appendix G of the ITI Contingency Plan document. As anticipated, the target completion date for this recommendation needs to be extended to allow for the completion of the ATO process.

Current Target Completion Date: August 30, 2015

Point of Contact:	Michael Williams, 301-287-0660
Recommendation 13:	Develop a COOP for the IT environment and other IT components supporting the one NRC remote location that does not have a COOP.
Agency Response Dated October 31, 2013:	Subsequent to the status update provided on July 19, 2013, OIS determined that where IT components are not currently included within an existing IT system boundary, the TTC should consolidate such components into a single IT system. Toward that end, the

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL
INFORMATION SECUIRTY MANAGEMENT ACT FOR FISCAL YEAR 2012
Technology Governance
(OIG-13-A-03)

Status of Recommendation

TTC is currently preparing FISMA-compliant ATO documentation
for this system, and this documentation will include an updated
COOP that will be added to Appendix G of the ITI Contingency
Plan as soon as it becomes available. However, OIS anticipates
the need to extend the target completion date for this
recommendation to allow for completion of the ATO process.

Original Target Completion Date: September 30, 2013
Revised Target Completion Date: August 30, 2014

OIG Analysis: The proposed action meets the intent of the recommendation.
This recommendation will be closed when OIG receives
verification that OIS developed a COOP for the IT environment
and other IT components supporting the one NRC remote location
that does not have a COOP.

Status: The Regional offices and TTC continue to work with CSO to
complete their FISMA documentation for an updated ATO. Once
the Regional offices have completed their ATO, their updated
contingency plans will be added to Appendix G of the ITI
Contingency Plan document. As anticipated, the target
completion date for this recommendation needs to be extended to
allow for the completion of the ATO process.

Current Target Completion Date: August 30, 2015

Point of Contact: Michael Williams, 301-287-0660