U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Audit Report

Management of Naval Reactors' Cyber Security Program

DOE/IG-0884

April 2013

Department of Energy
Washington, DC 20585

April 12, 2013

MEMORANDUM FOR THE SECRETARY

Greg Friedman

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of Naval Reactors' Cyber Security Program"

INTRODUCTION AND OBJECTIVE

The Naval Reactors Program (Naval Reactors), an organization within the National Nuclear Security Administration, provides the military with safe and reliable nuclear propulsion plants to power warships and submarines. Naval Reactors maintains responsibility for activities supporting the United States Naval fleet nuclear propulsion systems, including research and design, operations and maintenance and the ultimate disposition of the nuclear propulsion plants. Both the Department of Energy and the Department of Navy fund Naval Reactors. To fulfill its mission, Naval Reactors utilizes numerous information systems that reside on both classified and unclassified networks. It is imperative that the systems are protected against cyber security threats, regardless of classification, given the sensitive nature of the Naval Reactors mission and its impact on the naval fleet.

Previous Office of Inspector General reviews of Naval Reactors related to our *Federal Information Security Management Act of 2002* evaluations identified certain security weaknesses related to access controls and contingency planning. While the program had taken action to address weaknesses identified during our prior reviews, cyber security processes should continue to evolve to address threats that are becoming more sophisticated and frequent. As noted in a U.S. Government Accountability Office report on *Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems* (GAO-11-463T, March 2011), cyber security threats are originating from a wide variety of sources, including foreign nations and disgruntled or former employees. We initiated this audit to determine whether the Naval Reactors Program had effectively managed its cyber security program.

RESULTS OF AUDIT

Naval Reactors had made a number of enhancements to its cyber security program over the past several years. However, we identified weaknesses related to vulnerability management, access controls, incident response and security awareness training that could negatively affect its security posture. In particular:

- Naval Reactors' vulnerability management controls and processes were not fully effective in applying security patches for all desktop and network applications. For example, although the program had taken action to correct the vast majority of vulnerabilities identified during scans performed in July 2011, our current review disclosed 335 high and medium risk vulnerabilities. Naval Reactors officials were unable to provide us with information regarding the age of the identified weaknesses due to the lack of an adequate corrective action tracking mechanism.

- Controls over access to information and systems at Naval Reactors were not always operating effectively. Specifically, system access had not been revoked for terminated and/or separated employees within timeframes established by Naval Reactors' security policies. In addition, officials were not always able to provide documentation supporting the approval of individuals' access to information systems.

- Our review identified that a confirmed cyber security incident involving malicious code located on the unclassified network in January 2012 was not reported to the Department's Joint Cyber Security Coordination Center, as required. Reporting all instances of successful infection or persistent attempts at infection by malicious code is a key aspect of ensuring the effectiveness of the Department's incident handling capabilities, including sharing information concerning common vulnerabilities and threats within the organization.

- Although Naval Reactors had established a cyber security awareness training program, its implementation was not always effective. For instance, we determined that the Naval Reactors Laboratory Field Office had not conducted annual cyber security training in Fiscal Year 2011 for any of its almost 200 Federal employees. In addition, we noted that contractor employees did not always complete the required security training within the established due dates.

The weaknesses identified occurred, in part, because Naval Reactors had not ensured that necessary cyber security controls were fully implemented. Specifically, officials had not fully developed and/or implemented policies and procedures related to vulnerability management, access controls, incident response and cyber security training. For example, officials stated that an enterprise-wide vulnerability management policy outlining specific criteria for the treatment of all third-party vulnerabilities did not exist. In addition, Naval Reactors had not always effectively utilized Plans of Action and Milestones to track, prioritize and remediate cyber security weaknesses.

To its credit, Naval Reactors had taken a number of actions to strengthen its cyber security program in recent years. However, absent a fully effective cyber security program, information systems and data remain at a higher than necessary risk of compromise. As such, we made several recommendations that, if fully implemented, should help the program address the weaknesses identified. Due to security considerations, information on specific weaknesses and information systems has been omitted from this report. Naval Reactors officials were provided with detailed information regarding respective weaknesses identified.

MANAGEMENT REACTION

Management generally concurred with the report's recommendations and indicated that corrective actions had been taken or were planned to address the issues identified. Management stated that it was committed to enhancing the Naval Reactors cyber security program and planned to incorporate the report's recommendations into future improvements, as appropriate. Management expressed concern with several conclusions in the report. Management's comments and our responses to its expressed concerns are summarized in the body of the report. Management's formal comments are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary
Acting Under Secretary of Nuclear Security
Chief of Staff

REPORT ON MANAGEMENT OF NAVAL REACTORS' CYBER SECURITY PROGRAM

TABLE OF CONTENTS

Cyber Security Management

Appendices

MANAGEMENT OF NAVAL REACTORS' CYBER SECURITY PROGRAM

CYBER SECURITY MANAGEMENT

The Naval Reactors Program (Naval Reactors) had taken a number of actions to improve its cyber security posture in recent years. For instance, Naval Reactors worked to centralize its certification and accreditation process by using a commercial-off-the-shelf software product to enhance efficiency. Officials also worked to improve security operations over the classified and unclassified network infrastructure. While these are positive actions, our review of the Naval Reactors cyber security program identified various control weaknesses over unclassified and classified information systems related to vulnerability management, access controls, incident management and cyber security awareness training.

Vulnerability Management

Naval Reactors' implementation of vulnerability management controls and processes was not fully effective in applying security patches for third-party applications. In particular, in July 2011, Naval Reactors proactively worked with testers from the National Nuclear Security Administration's (NNSA) Information Assurance Response Center (NIARC) to conduct an in-depth vulnerability scan of its classified information systems and network. During the scan, NIARC identified approximately 9,000 high and medium risk vulnerabilities. To its credit, Naval Reactors had taken action to remediate the vast majority of the identified vulnerabilities as of the time of our review. However, in responding to our preliminary report, Naval Reactors rescanned its systems and identified 335 high and medium risk vulnerabilities. While we commend the program for significantly reducing the number of vulnerabilities, a Naval Reactors official noted that a subset of the 335 vulnerabilities included 9 high risk weaknesses originally identified by the 2011 NIARC scans. The official commented, however, that the program was unable to determine how many of the medium risk vulnerabilities remained from the NIARC scan.

Despite making progress in the remediation of identified vulnerabilities, the Naval Reactors official noted that the program was still attempting to formalize a process for effectively tracking the progress of corrective actions taken to remediate identified vulnerabilities. As noted by the National Institute of Standards and Technology (NIST), an effective vulnerability management system can reduce the amount of time and resources spent responding to vulnerabilities and exploitation of those weaknesses. Furthermore, proactive management of system vulnerabilities can reduce or eliminate the potential for exploitation and involves considerably less time and effort than responding after an event has occurred.

Access Controls

Our review determined that controls over access to information systems at Naval Reactors were not always operating effectively. In particular, access to information systems for terminated/separated employees had not been revoked within timeframes established by the program. While the Naval Reactors Cyber Security Program Plan required that network passwords be disabled within 24 hours when a user's access privileges are revoked, 19 of 53 (36 percent) terminated/separated employees did not have their access revoked within the required timeframe. One former employee's account remained active for 103 days after separation from Naval Reactors. A key control for protecting information technology systems and the information that resides on them is to implement effective, logical and physical access controls that help prevent unauthorized modification, loss or disclosure of information.

We also identified weaknesses over the approval process for granting system access to new employees. According to Naval Reactors' policy, a newly hired individual must complete *Consent to Access National Nuclear Security Administration Computers and NNPP Net Email and Information Systems Responsibility Agreement* forms prior to gaining access to the network. However, our sample of 90 new hires found that 3 individuals were missing the required approval forms. In addition, although Naval Reactors required access forms for users who were not Bechtel Plant Machinery Inc. (BPMI) employees to access individual systems, Naval Reactors was unable to provide documentation to support access approval for 6 of 10 non-BPMI employees that were sampled.

Incident Response

Our review of incident response and reporting practices at Naval Reactors identified that a confirmed cyber security incident involving the unclassified network in January 2012 had not been reported to the Department of Energy's (Department) Joint Cyber Security Coordination Center (JC3). Specifically, an exploit of malicious code was identified by NIARC through routine scans of the network perimeter and was referred to Naval Reactors for further investigation. While officials confirmed the malicious code incident, they issued a negative report to JC3 during the month it occurred stating that there were no incidents to report. As noted by JC3 reporting requirements, "all instances of successful infection or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms" must be reported within 4 hours of the confirmation of the event. In comments on our report, management stated that the incident was not reported because officials did not believe the attack was successful. While we did not identify indications that exploitation of systems and information had occurred, we did note that malware was successfully installed on a Naval Reactors unclassified system and, therefore, should have been reported in accordance with Department guidelines. According to the Office of Management and Budget, a key aspect of having a fully effective incident handling capability is sharing information concerning common vulnerabilities and threats within the organization.

Security Awareness Training

Although Naval Reactors had established a cyber security awareness training program, its implementation was not always effective. Specifically, the Naval Reactors Laboratory Field Office had not conducted annual cyber security training in Fiscal Year 2011 for any of its almost 200 Federal employees. As noted by the U.S. Department of Homeland Security, the most common vector for an intruder to gain unauthorized access to sensitive information is through phishing attacks, many of which can be prevented by effective user training. A phishing attack is a social engineering technique in which cyber attackers utilize email as a method to deliver malicious code in attached files or by diverting a user to a fake webpage, providing a gateway to the information that resides on the user's information system or network. One way to help minimize risk to both the program and the user is to ensure that an adequate security awareness training program is provided for all Naval Reactors employees.

There were also many instances in which Naval Reactors contractors had not completed security training in a timely manner. Specifically, as noted in the following table, employees at four Naval Reactors facilities – BPMI, Knolls Atomic Power Laboratory (KAPL), Bettis Atomic Laboratory (Bettis) and the Naval Reactors Facility (NRF) – were delinquent in completing annual cyber security training within the required timeframes.

Site	Total Delinquent	Total Population	Percentage Delinquent
BPMI	**52**	**891**	**6%**
KAPL	**2,946**	**3,067**	**96%**
Bettis	**773**	**2,572**	**30%**
NRF	**35**	**1,212**	**3%**
Totals	**3,806**	**7,742**	**49%**

To their credit, certain entities had taken action subsequent to our review. However, in one instance, 310 of 3,067 (10 percent) KAPL employees had yet to complete training requirements as of June 2012.

Implementation of Cyber Security Controls

The issues identified occurred, in part, because Naval Reactors had not ensured that the necessary cyber security requirements were fully implemented. In particular, Naval Reactors had not fully developed and/or implemented policies and procedures related to vulnerability management, access controls, incident response and cyber security training. In addition, Naval Reactors had not always effectively utilized Plans of Action and Milestones (POA&M) to track, prioritize and remediate cyber security weaknesses.

Policies and Procedures

We found that, in many cases, policies and procedures were not fully developed or not effectively implemented to ensure that cyber security weaknesses were corrected. In particular, the vulnerability management weaknesses identified occurred, in part, because Naval Reactors lacked adequate policies and procedures for patching vulnerabilities in third-party software applications. For example, although the Naval Reactors' vulnerability management process was specific to the application of patches highlighted in bulletins issued by JC3, an enterprise-wide vulnerability management policy outlining specific criteria for the treatment of all third-party vulnerabilities did not exist. Officials told us that efforts to draft an enterprise-wide policy had recently begun, but the efforts were not complete at the time of our review. In addition to the lack of policies and procedures, officials commented that certain patches had not been implemented due to potential operational impacts, availability of patches from vendors and the configuration of desktop systems. As noted by NIST Special Publication 800-40v2, *Creating a Patch and Vulnerability Management Program*, the development of a formal plan that outlines how to prioritize and remediate identified vulnerabilities in a timely manner is critical to maintaining the operational availability, confidentiality and integrity of information systems.

We found that while Naval Reactors had developed policies and procedures related to managing access controls, these policies and procedures were not always effectively implemented. For example, Naval Reactors did not centrally manage its access control records, which contributed to missing system access approvals and delays in revoking access for terminated/separated employees. In many instances, paper copies of approvals were filed in binders throughout multiple Naval Reactors facilities. In addition, an enterprise-wide system or process was not utilized to revoke logical access of terminated/separated employees; rather, each individual site utilized different processes. Furthermore, one of the Naval Reactors employees responsible for the termination/separation of employees was unaware of the procedure to revoke access within 24 hours of termination/separation.

We also determined that cyber security incidents were not always reported in a timely manner because Naval Reactors' Incident Response Policy contained a different interpretation from JC3 of what constituted a malicious code incident. Specifically, we noted that the Naval Reactors policy stated that malicious code incidents were to be reported to JC3 when "successful large network site-wide infection or persistent attempts at infection by malicious code occurred." This deviated from the JC3 reporting guidelines, however, which noted that "all instances of successful infection" should be reported. We also found that Naval Reactors lacked a fully automated system to track cyber security incidents and noted instances in which the current procedures allowed the use of duplicative tracking numbers and the incorrect classification of an incident. For example, while Naval Reactors classified one malicious code incident we reviewed as "closed," our evaluation of the incident report found that the status was recorded as "open."

Furthermore, we found inadequate implementation of changes to cyber security awareness training procedures. Specifically, although the site transitioned to training employees using an online service, Naval Reactors Federal employees did not have the necessary application licenses needed to access the training material. The contractor responsible for establishing the training was unaware of this issue until we brought it to their attention. Subsequently, site officials initiated a process to ensure that all Federal employees receive the required cyber security training. In addition, we noted that Naval Reactors had not consistently terminated access for those contractor individuals who had not completed training within the established training deadlines as required by site procedures.

Plan of Action and Milestones

Naval Reactors had not always effectively utilized POA&Ms to track, prioritize and remediate cyber security weaknesses. In particular, although Naval Reactors had a process in place to develop POA&Ms, the process did not fully meet the requirements set forth by NNSA Policy (NAP) 14.1C, *NNSA Baseline Cyber Security Program*, for tracking, documenting and correcting program and system level findings. For example, the weaknesses identified during the NIARC vulnerability scan were not captured in a POA&M, even though NAP 14.1C required that "findings" identified through such activities are captured in a POA&M. Rather, Naval Reactors only required weaknesses identified through the certification and accreditation process to be entered into the POA&M. As noted by the Office of Management and Budget, a POA&M reflects the enterprise security needs of an agency and provides a roadmap for continuous security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool for agency officials.

Improvements for Naval Reactors Cyber Security Program

Absent an effective enterprise-wide vulnerability management process, Naval Reactors' applications that are missing security patches for known vulnerabilities are at risk for computer viruses and other malicious attacks that could allow attackers the ability to compromise systems and information. In addition, without effective account management practices, the weaknesses noted may increase the risk of malicious or unauthorized access to the unclassified and classified networks, systems and related applications. Furthermore, inadequate development and implementation of incident response policies and procedures may increase the risk that the Department will not have a comprehensive view of specific threats to its information systems. Also, improving the POA&M process could facilitate management's understanding of the cyber security risks within Naval Reactors and help prioritize investments to ensure adequate protection of data and information systems.

RECOMMENDATIONS

To help Naval Reactors address the challenges in developing a mature and effective information security program, we recommend that the Administrator, National Nuclear Security Administration, direct the Naval Reactors Laboratory Field Office to:

1. Establish an effective enterprise-wide vulnerability management program, including development and implementation of policies and procedures for both the classified and unclassified networks;

2. Centralize the management of user accounts to include a repository for system access approvals, as well as ensure that the granting and revocation of access is in accordance with Naval Reactors policy;

3. Properly align Naval Reactors incident reporting guidance with JC3 reporting requirements to help ensure

all cyber security incidents are properly reported, as required;

4. Strengthen policies and procedures related to POA&Ms to ensure that all identified cyber security weaknesses are tracked, prioritized and remediated in a timely manner; and

5. Implement policies and procedures to ensure that cyber security awareness training is completed in a timely manner.

MANAGEMENT REACTION

Management generally concurred with the report's recommendations and indicated that corrective actions had been taken or were planned to address the issues identified. Management stated that it was committed to enhancing the Naval Reactors cyber security program and planned to incorporate the report's recommendations into future improvements, as appropriate. Management commented that the program proactively worked with NNSA to conduct vulnerability scans and immediately began to remediate identified weaknesses. In addition, management stated that it continues to work towards finalizing policies and procedures supporting the vulnerability management program and strengthening procedures related to access controls. Furthermore, management considered its actions related to incident reporting and managing POA&Ms to be consistent with Department requirements. Management also stated that users' training is now current, and planned modifications to tracking systems will improve retrieval of training records.

AUDITOR COMMENTS

Management's planned corrective actions are responsive to our recommendations. As to the areas in which management expressed concerns, we determined that although management stated that the handling of the cyber security incident noted in our report was in accordance with Department requirements, we found that malware was installed successfully on an unclassified system and, therefore, should have been reported to JC3. In addition, while management stated that Naval Reactors' implementation and reporting of POA&Ms was consistent with NNSA requirements, we noted that officials did not include all program and system-level findings in the POA&M in accordance with NNSA policy. Management's comments are included in their entirety in Appendix 3.

Appendix 1

OBJECTIVE

To determine whether the Naval Reactors Program (Naval Reactors) effectively managed its cyber security program.

SCOPE

The audit was performed between March 2012 and April 2013 at the Naval Reactors Laboratory Field Office and the Bechtel Marine Propulsion Corporation in West Mifflin, Pennsylvania. We also obtained information from other Naval Reactors facilities, as necessary. The audit was limited to the review of Naval Reactors' cyber security activities. At the request of Naval Reactors officials, we did not conduct vulnerability scanning on the network, but instead relied upon scans conducted by National Nuclear Security Administration Information Assurance Response Center (NIARC) and Naval Reactors personnel.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and regulations, including those pertaining to information and cyber security;

- Reviewed applicable standards and guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology (NIST) for the planning and management of system and information security such as Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems;* and, NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*;

- Obtained and analyzed documentation from Naval Reactors related to the planning, development and management of cyber security related functions such as cyber security plans, Plans of Action and Milestones and budget information;

- Assessed controls over network operations and systems to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources;

- Reviewed prior reports issued by the Office of Inspector General and the Government Accountability Office; and

- Held discussions with officials from the Naval Reactors Laboratory Field Office and site support contractors.

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, we assessed significant internal controls and Naval Reactors' implementation of the *GPRA Modernization Act of 2010* and determined that it had not established performance measures for its cyber security efforts. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We did not solely rely on computer-processed data to satisfy our objective. However, we validated the results of the scans performed by NIARC and Naval Reactors personnel over various networks and drives by confirming the weaknesses disclosed with responsible on-site personnel. In addition, we confirmed the validity of other data, when appropriate, by reviewing supporting source documents.

Management waived an exit conference.

RELATED REPORTS

Office of Inspector General Reports

- Audit Report on *Follow-up Audit of the Department's Cyber Security Incident Management Program* (DOE/IG-0878, December 2012). Although certain actions had been taken in response to our prior Cyber Security Incident Management Program report listed below, we identified several issues that limited the efficiency and effectiveness of the Department of Energy's (Department) cyber security incident management program and adversely impacted the ability of law enforcement to investigate incidents. For instance, we noted that the Department and the National Nuclear Security Administration continued to operate independent, partially duplicative cyber security incident management capabilities at an annual cost of more than $30 million. The issues identified were due, in part, to the lack of a unified, Department-wide cyber security incident management strategy.

- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2012* (DOE/IG-0877, November 2012). The evaluation determined that 16 previously identified weaknesses remained uncorrected, including 4 from Fiscal Year (FY) 2010. In addition, during the review, it was noted that an additional 22 cyber security weaknesses were identified at various locations for FY 2012. The identified weaknesses were related to access controls, vulnerability management, system integrity of web applications, planning for continuity of operations and change control management. The weaknesses identified occurred, in part, because Department elements had not ensured that cyber security requirements were fully developed and implemented. In addition, programs and sites had not always effectively monitored performance to ensure that appropriate controls were in place. Without improvements to its unclassified cyber security program, including implementation of effective continuous monitoring practices and adopting processes to ensure security controls are in place and operating as intended, there is an increased risk of compromise and/or loss, modification and non-availability of the Department's systems and the information.

- Special Report on *Management Challenges at the Department of Energy* (DOE/IG-0874, October 2012). Based on the work performed during FY 2012 and other risk assessment tools, the Office of Inspector General identified nine areas, including cyber security, which remained as management challenges for FY 2013. While positive strides had been made in a number of areas, many of the Department's most significant management challenges were not amenable to immediate resolution.

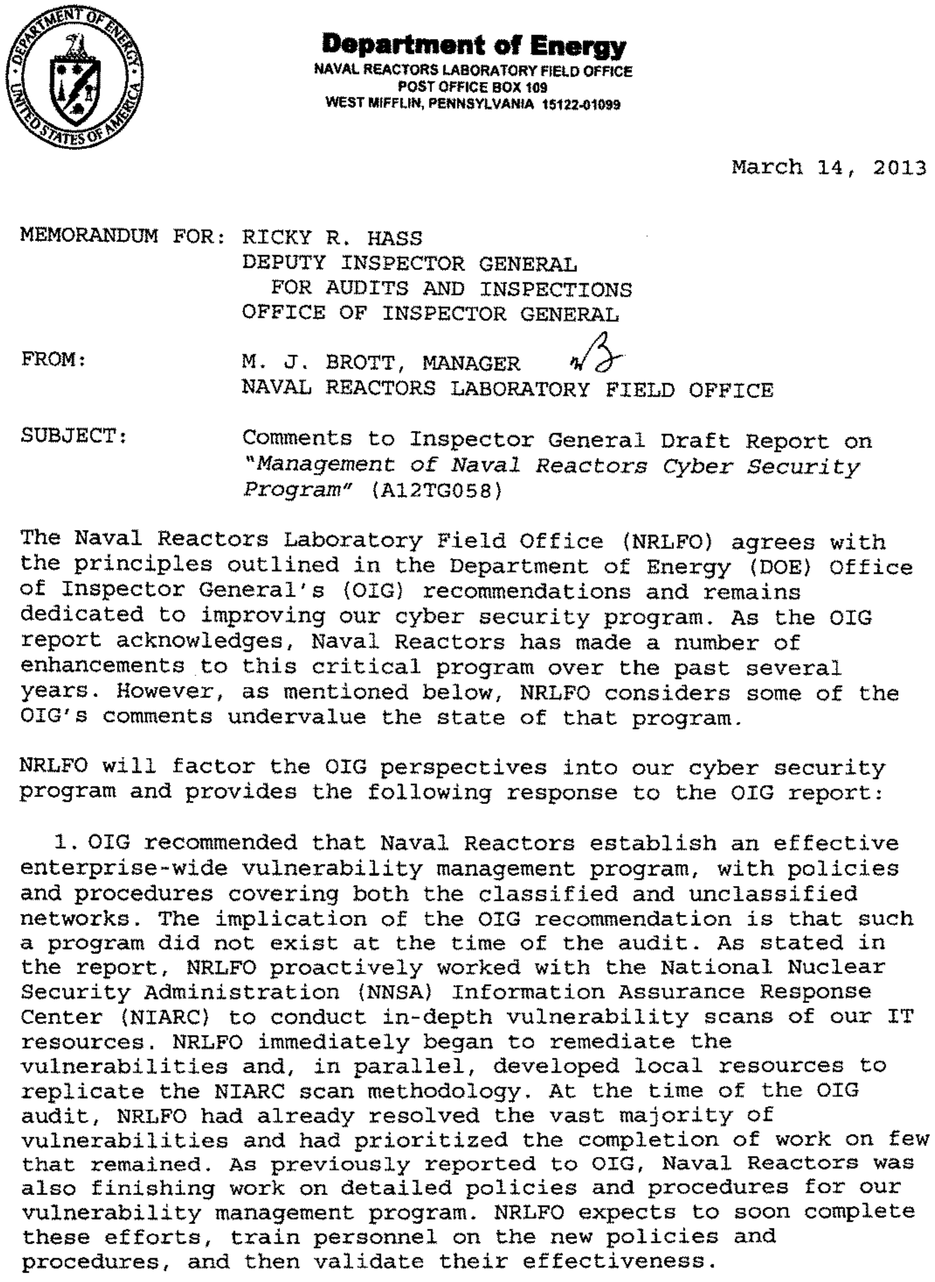
- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2011* (DOE/IG-0856, October 2011). The review determined that although the Department had taken steps over the past years to address previously identified cyber security weaknesses, additional efforts were needed to enhance its unclassified cyber security program. Weaknesses were identified in the areas of access controls, vulnerability management, business continuity/disaster recovery, change control management and annual cyber security refresher training. The weaknesses identified occurred, in part, because Departmental elements had not ensured that cyber security requirements included all necessary elements and were properly implemented. Furthermore, program elements also did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place. Without improvements to its unclassified cyber security program, such as consistent risk management practices and adopting processes to ensure security controls are appropriately developed, implemented and monitored, there is an increased risk of compromise and/or loss, modification and non-availability of the Department's systems and information.

- Audit Report on *The Department's Cyber Security Incident Management Program* (DOE/IG-0787, January 2008). Program elements and facility contractors established and operated as many as eight independent cyber security intrusion and analysis organizations whose missions and functions were partially duplicative and not well coordinated. Sites could also choose whether to participate in network monitoring activities performed by the organizations. Furthermore, the Department had not adequately addressed related issues through policy changes, despite identifying and acknowledging weaknesses in its cyber security incident management and response program.

U.S. Government Accountability Office Report

- Report on *Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems* (GAO-11-463T, March 2011).

MANAGEMENT COMMENTS



Department of Energy
NAVAL REACTORS LABORATORY FIELD OFFICE
POST OFFICE BOX 109
WEST MIFFLIN, PENNSYLVANIA 15122-01099

March 14, 2013

MEMORANDUM FOR: RICKY R. HASS
DEPUTY INSPECTOR GENERAL
FOR AUDITS AND INSPECTIONS
OFFICE OF INSPECTOR GENERAL

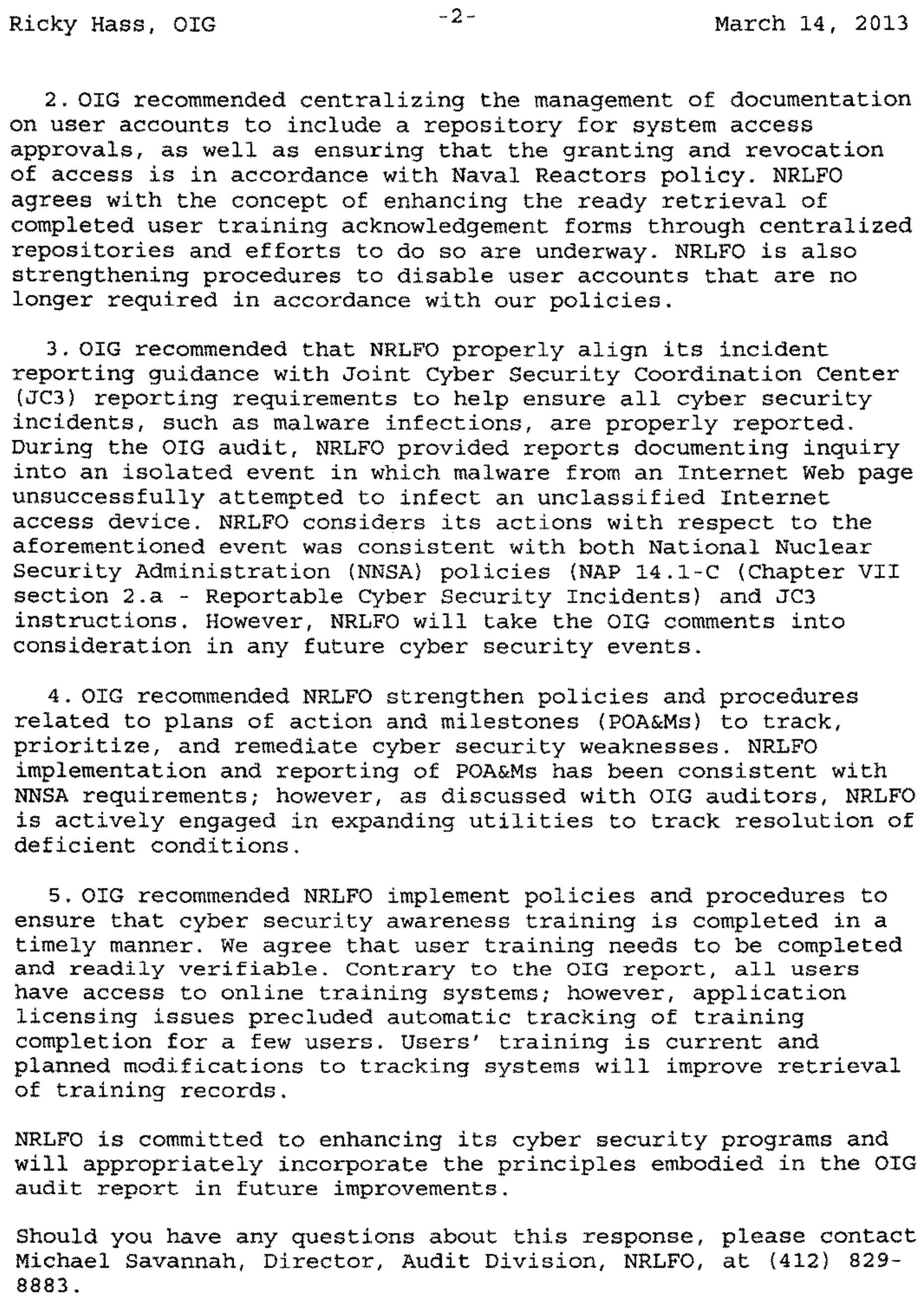
FROM: M. J. BROTT, MANAGER
NAVAL REACTORS LABORATORY FIELD OFFICE

SUBJECT: Comments to Inspector General Draft Report on *"Management of Naval Reactors Cyber Security Program"* (A12TG058)

The Naval Reactors Laboratory Field Office (NRLFO) agrees with the principles outlined in the Department of Energy (DOE) Office of Inspector General's (OIG) recommendations and remains dedicated to improving our cyber security program. As the OIG report acknowledges, Naval Reactors has made a number of enhancements to this critical program over the past several years. However, as mentioned below, NRLFO considers some of the OIG's comments undervalue the state of that program.

NRLFO will factor the OIG perspectives into our cyber security program and provides the following response to the OIG report:

1. OIG recommended that Naval Reactors establish an effective enterprise-wide vulnerability management program, with policies and procedures covering both the classified and unclassified networks. The implication of the OIG recommendation is that such a program did not exist at the time of the audit. As stated in the report, NRLFO proactively worked with the National Nuclear Security Administration (NNSA) Information Assurance Response Center (NIARC) to conduct in-depth vulnerability scans of our IT resources. NRLFO immediately began to remediate the vulnerabilities and, in parallel, developed local resources to replicate the NIARC scan methodology. At the time of the OIG audit, NRLFO had already resolved the vast majority of vulnerabilities and had prioritized the completion of work on few that remained. As previously reported to OIG, Naval Reactors was also finishing work on detailed policies and procedures for our vulnerability management program. NRLFO expects to soon complete these efforts, train personnel on the new policies and procedures, and then validate their effectiveness.



2. OIG recommended centralizing the management of documentation on user accounts to include a repository for system access approvals, as well as ensuring that the granting and revocation of access is in accordance with Naval Reactors policy. NRLFO agrees with the concept of enhancing the ready retrieval of completed user training acknowledgement forms through centralized repositories and efforts to do so are underway. NRLFO is also strengthening procedures to disable user accounts that are no longer required in accordance with our policies.

3. OIG recommended that NRLFO properly align its incident reporting guidance with Joint Cyber Security Coordination Center (JC3) reporting requirements to help ensure all cyber security incidents, such as malware infections, are properly reported. During the OIG audit, NRLFO provided reports documenting inquiry into an isolated event in which malware from an Internet Web page unsuccessfully attempted to infect an unclassified Internet access device. NRLFO considers its actions with respect to the aforementioned event was consistent with both National Nuclear Security Administration (NNSA) policies (NAP 14.1-C (Chapter VII section 2.a - Reportable Cyber Security Incidents) and JC3 instructions. However, NRLFO will take the OIG comments into consideration in any future cyber security events.

4. OIG recommended NRLFO strengthen policies and procedures related to plans of action and milestones (POA&Ms) to track, prioritize, and remediate cyber security weaknesses. NRLFO implementation and reporting of POA&Ms has been consistent with NNSA requirements; however, as discussed with OIG auditors, NRLFO is actively engaged in expanding utilities to track resolution of deficient conditions.

5. OIG recommended NRLFO implement policies and procedures to ensure that cyber security awareness training is completed in a timely manner. We agree that user training needs to be completed and readily verifiable. Contrary to the OIG report, all users have access to online training systems; however, application licensing issues precluded automatic tracking of training completion for a few users. Users' training is current and planned modifications to tracking systems will improve retrieval of training records.

NRLFO is committed to enhancing its cyber security programs and will appropriately incorporate the principles embodied in the OIG audit report in future improvements.

Should you have any questions about this response, please contact Michael Savannah, Director, Audit Division, NRLFO, at (412) 829-8883.

IG Report No. DOE/IG-0884

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report that would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name ______________________________ Date ________________________________

Telephone __________________________ Organization __________________________

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact our office at (202) 253-2162.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://energy.gov/ig

Your comments would be appreciated and can be provided on the Customer Response Form.