OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-17-02 November 2016

MANAGEMENT OF BROOKHAVEN NATIONAL LABORATORY'S CYBERSECURITY PROGRAM

Department of Energy
Washington, DC 20585

November 15, 2016

MEMORANDUM FOR THE SECRETARY

FROM: Rickey R. Hass
Acting Inspector General

SUBJECT: INFORMATION: Audit Report on the "Management of Brookhaven National Laboratory's Cybersecurity Program"

BACKGROUND

Brookhaven National Laboratory (Brookhaven) is a multipurpose research institution funded primarily by the Department of Energy and operated by Brookhaven Science Associates. Brookhaven employs almost 3,000 individuals and hosts over 4,000 visiting researchers each year. To support its research mission, Brookhaven makes extensive use of information technology resources for scientific and business computing related to high-speed network infrastructure, data management, and Web applications. As a management and operating contractor, Brookhaven is responsible for meeting various Federal cybersecurity requirements. The challenges related to cybersecurity management have become even more important with recent cybersecurity incidents in the Federal Government and the compromised sensitive information of millions of individuals. Furthermore, the range of cyber threat actors, methods of attack, targeted systems, and victims continue to expand.

Our recent report on *The Department of Energy's Cybersecurity Risk Management Framework* (DOE-OIG-16-02, November 2015) noted that while the Department had made progress toward reducing the likelihood of compromise to its information systems and data, additional effort was needed to ensure that it identified risks and adequately secured systems and information. The report stated that several sites, including Brookhaven, had not fully implemented an effective cybersecurity continuous monitoring process. We initiated this audit to determine whether Brookhaven effectively managed its cybersecurity program.

RESULTS OF AUDIT

Brookhaven had not implemented a fully effective cybersecurity program. We identified weaknesses related to vulnerability and configuration management, physical and logical access controls, security planning and assessments, and contingency planning and data retention. Specifically, we found that:

- Brookhaven was not fully effective at implementing vulnerability and configuration management controls and processes. For instance, our vulnerability scanning, along with

manual testing of the Brookhaven network, identified 243 unique vulnerabilities on workstations, servers, and Web applications, including 224 (92 percent) vulnerabilities that were high or medium risk as categorized within the National Vulnerability Database sponsored by the Department of Homeland Security. These vulnerabilities included end-of-life software applications and database management tools no longer supported by the vendor as well as outdated operating systems and virus scanner definitions. We also identified configuration management weaknesses, including numerous expired exceptions to allow network traffic through the site's firewall.

- Brookhaven had not always maintained adequate physical or logical access controls over its information and systems. We identified weaknesses related to ensuring appropriate physical access controls over the laboratory's data center. In addition, opportunities for improvement existed related to granting logical access to the site's network. Furthermore, while Brookhaven had made progress, it had not fully utilized Personal Identity Verification cards to support multifactor authentication to access certain systems, as required by the Office of Management and Budget.

- Brookhaven had not conducted security planning and assessment activities in accordance with Federal requirements. Even though the National Institute of Standards and Technology's *Security and Privacy Controls for Federal Information Systems and Organizations* provided updated Federal cybersecurity guidance in 2013, Brookhaven officials still had not implemented many enhanced security controls related to access, security awareness and training, and contingency planning. In addition, Brookhaven had not included all self-identified weaknesses in its plan of action and milestones (POA&M) process. POA&Ms are an important tool to assist management in identifying, prioritizing, and tracking remediation of known cybersecurity weaknesses.

- Brookhaven had not developed adequate contingency planning procedures to ensure that it could recover essential functions in the event of a significant disruption. Although Brookhaven had established a continuity of operations plan to provide guidance for the continuation of essential functions in the event of an emergency, we found that officials had not developed a Business Impact Analysis to determine its mission and business essential functions. Moreover, in some instances Brookhaven had not documented or updated individual contingency plans for some of its information systems.

The identified weaknesses occurred, in part, because Brookhaven officials had not fully implemented applicable requirements related to cybersecurity. For example, Brookhaven officials had not adhered to all Federal and site-specific policies and procedures designed to address many of the areas of weakness noted during our review, including vulnerability management and access controls. We also found that Brookhaven Site Office and laboratory officials had not always effectively monitored the cybersecurity program. For instance, Brookhaven Site Office officials had not ensured that the site contractor met all Federal and contract requirements related to cybersecurity. We also noted that Brookhaven contractor officials had not adequately monitored their cybersecurity program to ensure that they corrected vulnerabilities in a timely manner.

Notably, subsequent to our prior report on *The Department of Energy's Cybersecurity Risk Management Framework*, the Brookhaven Site Office developed a continuous monitoring plan designed to monitor Brookhaven's systems, networks, and cybersecurity processes. However, weaknesses associated with implementing controls reduced the effectiveness of this plan and, without further improvements, Brookhaven's information and systems may be at a higher than necessary risk of compromise. Therefore, we have made recommendations that, if fully implemented, should improve management of Brookhaven's cybersecurity program.

MANAGEMENT RESPONSE

Management concurred with the recommendations and provided initial corrective actions to address the issues identified in the report. Management commented that it had implemented a defense-in-depth cybersecurity posture and a layered set of controls to mitigate risk. Management's comments and our response are summarized and discussed in the body of the report. Management's formal comments are included in Appendix 3.

Attachment

cc: Deputy Secretary
Under Secretary for Science and Energy
Chief of Staff
Chief Information Officer

MANAGEMENT OF BROOKHAVEN NATIONAL LABORATORY'S CYBERSECURITY PROGRAM

TABLE OF CONTENTS

Audit Report

Appendices

MANAGEMENT OF BROOKHAVEN NATIONAL LABORATORY'S CYBERSECURITY PROGRAM

DETAILS OF FINDING

The *Federal Information Security Modernization Act of 2014* (FISMA) requires each Federal agency to develop, document, and implement an enterprise-wide cybersecurity program to protect systems and data that support the operations and assets of an agency, including those provided or managed by contractors. To facilitate satisfying the requirements, the National Institute of Standards and Technology (NIST) developed mandatory guidance for categorizing and protecting Federal information and systems according to risk levels. At the time of our review, NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, contained minimum-security requirements that Federal agencies were to implement by April 2014. Brookhaven National Laboratory (Brookhaven) officials stated that they were not required to follow the provisions of NIST SP 800-53, Revision 4, because they were not included in Department of Energy orders or in the site's contract. However, Brookhaven is required to follow FISMA, which states that all agencies are required to adhere to current NIST guidance. As previously reported by the Office of Inspector General, sites that do not adhere to the requirements of revised NIST publications within 1 year of the release date may not be formally considering many newer controls in a timely manner. Department directives also set forth cybersecurity requirements and responsibilities and direct Department elements and site/facility management contractors to establish a Risk Management Approach that is consistent with NIST guidance.

Brookhaven officials stated that the site had implemented a defense-in-depth cyber security posture that provides a layered set of controls to mitigate risks, including items such as network segmentation, real-time system logging, multiple firewalls, and intrusion detection systems. However, despite these positive actions, we determined that Brookhaven had not implemented a fully effective unclassified cybersecurity program. Our review of Brookhaven's design and implementation of cybersecurity controls for five moderate risk unclassified information systems identified various cybersecurity weaknesses related to vulnerability and configuration management, access controls, security planning and assessments, and contingency planning and data retention.

Vulnerability and Configuration Management

We identified numerous vulnerability and configuration management weaknesses during our testing at Brookhaven. In particular, our internal and external vulnerability scans, along with manual testing of the Brookhaven network infrastructure, identified 243 unique vulnerabilities on a sample of workstations, servers, and Web applications, including 224 (92 percent) vulnerabilities that were determined to be high or medium risk as categorized in the National Vulnerability Database maintained by the Department of Homeland Security. Specifically, we found:

- Brookhaven had not remediated numerous high and medium risk vulnerabilities on servers and workstations within 30 days, as required by its policy. In one instance, a

vulnerability existed that could have been exploited by an attacker to obtain sensitive credential information, execute an arbitrary or malicious code on the site's information systems, or cause a denial of service attack.[1]

- The site's network still had several software applications and database management tools installed that the vendor no longer supported because end-of-life had been reached. When a product reaches its end-of-life and is no longer supported by the vendor, the vendor does not release new security patches for the product, increasing the risk of compromise. In one instance, site officials used a database management tool that the vendor had not supported since July 2010. Brookhaven also continued to use an operating system that the vendor had not supported since February 2012. Contrary to Brookhaven's network management policy, unsupported operating systems were not removed, segmented from the Brookhaven campus network, or documented within the site's firewall policy. Instead, systems continued to operate in the unsecure environment exposing them to a significantly higher risk of compromise. Subsequent to our testing, officials took action to upgrade software and were actively planning to remediate the remaining weaknesses.

- One application stored user authentication information in an unsecure manner on the network, making the authentication information accessible to any Web server on the same network. Under certain conditions, such as a malicious actor controlling the other Web servers, this insecure setting could have increased the risk of unauthorized users accessing or modifying sensitive information in Web applications. Brookhaven officials indicated that they addressed this vulnerability by taking corrective actions to isolate the application servers.

- Several Brookhaven servers and a workstation contained outdated virus scanner definitions, including one instance where virus definitions were more than 8 months old. By failing to update virus scanner definitions in a timely manner, Brookhaven may not be adequately protecting systems and data from recently identified threats. Officials responded that the vulnerabilities only existed on a few computers in our sample of systems; however, even a limited number of outdated scanners could increase the risk of intrusion by reducing Brookhaven's ability to detect and report malware installed on servers and workstations.

As noted in prior Office of Inspector General reports, failure to apply patches and remediate vulnerabilities promptly could result in unauthorized access to systems and information, as well as loss or disruption of critical operations. Even when Brookhaven was aware of existing vulnerabilities, we noted that documentation justifying risk acceptance for known vulnerabilities or weaknesses contained insufficient detail. For example, documentation for one vulnerability did not include any formal acceptance of risk or discussion of mitigating controls. Similarly, officials accepted the risk of another particular vulnerability but disclosed that they did not fully

[1] A denial-of-service attack occurs when an attacker attempts to prevent legitimate users from accessing information or services. By targeting computers and network connections, an attacker may be able to prevent users from accessing email, Web sites, or other services that rely on the affected computers.

understand the vulnerability or its impact. Lack of detailed information regarding vulnerabilities and the rationale for accepting the risk limits the ability of officials from Brookhaven and the Brookhaven Site Office to make educated risk acceptance decisions.

We also determined that Brookhaven had not always ensured that firewalls were appropriately configured to protect the site's network. Firewalls separate networks with differing security requirements, such as the Internet from an internal network that houses servers with sensitive data. As noted in NIST SP 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, a firewall should block all inbound and outbound traffic not expressly permitted by the firewall policy to decrease the risk of attack and reduce the volume of traffic on an organization's network. At Brookhaven, we identified 207 firewall exceptions that were expired but remained open. Several of these exceptions had been expired for more than a year. In addition, we found that five of the control variances were for separated employees no longer employed by Brookhaven.

In addition, although required to protect the confidentiality and integrity of information stored on digital media, Brookhaven did not always encrypt transported media. According to Brookhaven officials, the laboratory does not encrypt backup tapes that are transported offsite. As noted by NIST, many threats exist that could lead to the compromise of confidential information stored on removable storage media such as backup tapes. We also found that Brookhaven had not encrypted sensitive data at rest for any of the applications reviewed, including one that stored personally identifiable information such as names, addresses, and social security numbers. As previously noted on in our special report on *The Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013), the encryption of data at rest is an industry best practice that should be considered to maintain the confidentiality and integrity of information.

Access Controls

We identified several weaknesses related to implementing physical and logical access controls at Brookhaven. In particular, Brookhaven had not taken the necessary steps to ensure there were physical access controls at its data centers. For instance, we identified seven individuals that had separated from the laboratory but still maintained access to the data centers, including one individual that separated from Brookhaven approximately a year ago. We are particularly concerned about this issue because site officials brought to our attention their concerns that physical access privileges were not always promptly removed, including access for guests visiting the site.

In addition, officials had not ensured that they secured all data center equipment, including servers, in locked wiring closets or locked cabinets. Industry guidance notes that unrestricted physical access to an organization's secure areas, equipment, or materials containing sensitive data may make it easier to compromise systems by allowing a malicious insider to access the equipment. Therefore, an organization's physical security controls are often just as important as its technical or logical access controls. The vulnerabilities we identified related to tracking data center access may have further exacerbated the impact of other identified weaknesses related to access controls.

We also found that Brookhaven had not always appropriately granted logical access to networks and systems. In particular, we identified weaknesses in the approval process for granting logical access to the laboratory's network. According to Brookhaven's policy, an individual must sign a computer use agreement and complete annual cybersecurity training prior to gaining access to the network. However, we determined that of the 93 accounts sampled, 4 individuals maintained access to their account even though they did not complete the annual training requirement. Because we statistically selected our sample from approximately 5,200 active accounts, we believe that the actual number of discrepancies may be significantly higher.

Furthermore, while Brookhaven utilized multifactor authentication using tokens to remotely access networks or applications, it did not use Personal Identity Verification (PIV) cards. At the time of our review, Brookhaven had initiated implementing PIV authentication requirements related to the Office of Management and Budget's (OMB) Cybersecurity Sprint initiative, which are to be implemented by the end of fiscal year 2016. Although Brookhaven may not meet the goals of the Cybersecurity Sprint initiative by the deadline, officials noted that they continue to work with the Department's Office of the Chief Information Officer to implement using PIV credentials. Other Office of Inspector General ongoing reviews have identified similar issues.

Security Planning and Assessment

Contractor officials had not implemented controls included in NIST SP 800-53, Revision 4, issued in April 2013. NIST's guide on *Security and Privacy Controls for Federal Information Systems and Organizations* added 295 controls and control enhancements to improve security of Federal information systems. According to Federal requirements, Brookhaven should have implemented the enhanced controls no later than 1 year after publication of the new guidance. However, at the time of our review, officials had implemented few of the enhanced controls on the systems reviewed. Notably, officials were considering the new requirements and had developed an assessment plan, which they were working to implement. However, a Brookhaven official responsible for assessing controls noted that the process of enhancing security controls would take approximately 18 months to implement. While we commend Brookhaven officials for their efforts at the time of our review, we note that the anticipated completion date is more than 2½ years past the original due date. Therefore, implementing additional controls and enhancements for areas such as access controls, security awareness and training, and contingency planning was delayed and resulted in a higher than necessary risk for the systems reviewed.

We also identified weaknesses related to how officials assessed security for Brookhaven's information systems. For example, we found that there was a lack of independence between the individuals assessing the effectiveness of security controls and those responsible for implementing the controls. At Brookhaven, cybersecurity officials were responsible for both implementing and testing controls, which is contrary to Federal guidelines requiring that an independent reviewer evaluate security controls. To their credit, Brookhaven officials informed us that the laboratory's Internal Audit group had planned an audit to test specific NIST SP 800-53 controls for the moderate risk systems. In addition, Brookhaven had not always submitted self-identified weaknesses as part of its plan of action and milestones (POA&M) process. Our review of five system security plans for moderate risk systems found

20 instances where Brookhaven identified cybersecurity control weaknesses but did not formally include these weaknesses in the POA&M process so that the Brookhaven Site Office and Office of Science officials could review them. Furthermore, we noted that 11 of these weaknesses affected multiple systems and included deficiencies in controls related to logical access, incident response, configuration management, and contingency planning. As noted in OMB's *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, POA&Ms are an important management tool to assist in identifying, assessing, prioritizing, and monitoring remediation activities for known cybersecurity weaknesses.

Contingency Planning and Data Retention

Brookhaven had not developed and/or implemented adequate contingency planning and data retention processes for the information systems reviewed. Although officials established a Continuity of Operations Plan that provided guidance for the continuation of essential functions in the event of an emergency, we found that Brookhaven had not developed or had not updated its contingency plans for the systems reviewed, including networks and business applications used by most individuals at the site. Officials also had not performed a Business Impact Analysis to determine which systems were essential to the mission and business functions of the site. Similarly, the contingency plans should have included procedures for the assessment and recovery of a system following a disruption and should have provided key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, and detailed recovery procedures. In addition, our review found that even though system security planning documentation indicated that Brookhaven maintained an alternative processing site at the Princeton Plasma Physics Laboratory, this was no longer the case. The lack of an alternative processing site could affect Brookhaven's ability to recover and perform system operations for an extended period.

During our review, we also noted that Brookhaven had not ensured that its audit logging capabilities were fully operational. Specifically, officials commented that the site's archival process for recording security information was not working for certain logs, resulting in a loss of 6 months' of log information. Brookhaven officials also stated that there was only a limited risk of being unable to obtain forensics for specific log data that had aged out of online logging systems. However, NIST SP 800-92, *Guide to Computer Security Log Management*, noted:

> "Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems."

Security Control Implementation and Monitoring

The identified weaknesses occurred, in part, because Brookhaven had not always implemented applicable Federal, Department, and site level requirements related to cybersecurity. For example, Brookhaven officials had not implemented applicable requirements to address many of

the areas of weakness noted during our review, including vulnerability management and access controls. Although Brookhaven officials stated they had developed a formal monitoring and oversight plan and maintained monthly meetings to discuss the cybersecurity program, officials had not always effectively monitored the cybersecurity program to ensure that Brookhaven implemented Federal and contract requirements related to cybersecurity.

Security Control Implementation

Although Brookhaven had established policies to remediate security vulnerabilities in a timely manner, we found that many of the vulnerability management weaknesses occurred because officials had not implemented the policies and procedures. For instance, one application weakness that the site identified in March 2014 still had not been remediated at the time of our testing – more than 16 months from when it was originally identified. Cybersecurity officials noted that, while they were responsible for conducting vulnerability testing, they did not always have the authority to remediate the identified vulnerability, and responsible officials, such as system owners, did not always promptly correct vulnerabilities. In addition, officials did not always implement policy to ensure that they removed or isolated software no longer supported by the vendor. Even when they identified vulnerabilities, officials did not implement an effective process for documenting the acceptance of related risks. Although required by Brookhaven policy, officials did not always provide an explanation for weaknesses that they identified as "false positives"[2] or explain why they could not remediate certain vulnerabilities or employ compensating controls to mitigate weaknesses. This practice was contrary to NIST guidance on *Managing Information Security Risk Organization, Mission, and Information System View*, which stated that a risk response should identify, evaluate, and implement an appropriate course of action to accept, avoid, mitigate, share, or transfer risk.

Similarly, Brookhaven's ineffective enforcement of its own policy allowed expired firewall variances to provide unnecessary access to the laboratory's information technology infrastructure. In particular, officials did not always review variances to firewall configuration changes associated with controlling network traffic flow (both inbound and outbound). According to site policy, officials should have reviewed exceptions to the network traffic flow annually and removed any exceptions that no longer had an explicit mission or business need. Brookhaven officials stated that the additional risk regarding firewall variances was limited because of processes currently in place. However, subsequent to our review of the firewall exceptions, officials indicated that they would be reviewing variances and revoking access, where appropriate. In addition, they also took action to improve the process of reviewing firewall variances to restrict the number of exceptions that were expired or to assign exceptions properly.

Contrary to site policies and procedures for logical access to networks and systems, Brookhaven officials had not conducted the necessary reviews to ensure that all employees with network access completed the required annual cybersecurity training. In addition, we noted that automated scripts for monitoring completed training were not operating in all instances. As noted in a recent Government Accountability Office report, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs* (GAO-15-714,

[2] A "false positive" is an incorrectly identified vulnerability encountered as part of technical vulnerability testing.

September 2015), providing training is critical to securing information and systems because people are one of the weakest links when securing systems and networks. To their credit, Brookhaven officials conducted an internal assessment subsequent to our review to identify and provide cybersecurity training to the individuals who did not meet the annual requirement. In addition, officials informed us that they were in the process of modifying account lock procedures for users who had not met all of the training requirements for account access. Furthermore, officials did not adequately implement policies related to granting and revoking physical access to restricted areas. Although policies and procedures required that designated approvers review access lists quarterly and remove access upon termination of employment, we found that officials had not taken the appropriate action to revoke access. We also found that Brookhaven's human resources personnel did not adequately coordinate with badging office personnel to revoke access privileges, as appropriate.

We determined that Brookhaven had not fully implemented Federal contingency planning requirements. Specifically, NIST required the organization to develop a contingency plan for information systems that identifies essential missions and business functions. Federal guidance also noted that conducting a Business Impact Analysis is a key step in the contingency planning process because it assists an organization in determining mission or business processes, recovery criticality, and recovery priorities for systems. In addition, although NIST required establishing an alternative processing site for moderate risk systems, officials no longer maintained such a site for any of the systems reviewed because they did not believe that they were legally required to do so. Furthermore, officials had not ensured that they were maintaining audit records for all systems as required by NIST. Although officials made changes to the site's logging capabilities, they had not tested the changes to ensure that the capabilities continued to function as necessary.

Monitoring and Oversight

Brookhaven and Brookhaven Site Office officials had not always effectively monitored the cybersecurity program to ensure that they were implementing Federal and contract requirements related to cybersecurity. In particular, Brookhaven had not fully implemented a continuous monitoring program to ensure effective information security. In addition, Brookhaven officials had not ensured that individuals corrected vulnerabilities in a timely manner as well as tracked and prioritized weaknesses for remediation. Furthermore, Brookhaven Site Office personnel had not ensured that the management and operating contractor met the requirements of the site-level contract, including implementing updated cybersecurity requirements.

We determined that Brookhaven had not fully established an effective continuous monitoring process in accordance with Federal requirements. Specifically, NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, required that all security controls implemented at the system level be assessed for effectiveness in accordance with Federal requirements and individual system security plans. Consistent with our prior report on *The Department of Energy's Cybersecurity Risk Management Framework* (DOE-OIG-16-02, November 2015), we found that Brookhaven had not thoroughly tested the effectiveness of security controls on various systems reviewed. As a result, many of the weaknesses identified during our review existed, at least in part, because of the lack of an

effective continuous monitoring process. An effective continuous monitoring process should help officials maintain an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

We found that Brookhaven officials had not established a process to monitor effectively the age of vulnerabilities, which could have helped them prioritize corrective actions, as appropriate. Without this type of analysis, Brookhaven could not effectively monitor enforcement of its patch management policy, which required revocation of access to systems if vulnerabilities remained uncorrected after 30 days of patch availability. In addition, officials had not effectively utilized POA&Ms to track, prioritize, and remediate cybersecurity weaknesses. According to the Office of Science's Program Cyber Security Plan, organizations should include in a POA&M any weakness, deficiency, or vulnerability identified by assessments internal or external to the organization or information system being assessed or as part of the continuous monitoring strategy. Department guidance also noted that organizations should prepare a POA&M for weaknesses identified during the risk management process. We noted that tracking only a limited number of POA&M items could limit the site's ability to effectively prioritize and correct all identified weaknesses in a timely manner.

Brookhaven Site Office officials had not ensured that contractors met the cybersecurity requirements of the site level contract. Specifically, Brookhaven officials commented that they delayed implementing NIST SP 800-53, Revision 4, because existing Department directives and the Office of Science's Program Cyber Security Plan did not require the use of NIST SP 800-53 Revision 4. However, NIST's *Minimum Security Requirements for Federal Information and Information Systems* notes that Federal agencies must meet the minimum security controls in accordance with NIST SP 800-53, as amended. Furthermore, Brookhaven's contract indicated that the process described in the contract should not affect the application of otherwise applicable laws and regulations, including Department directives.

Impact and Path Forward

Without improvements that fully implement cybersecurity policies and procedures, Brookhaven's information and systems will continue to be at a higher-than-necessary risk of compromise, loss, or modification. For instance, without an effective vulnerability management program and sufficient controls over its network traffic, Brookhaven increases its risk of malicious attacks that could allow attackers the ability to compromise systems and information. In addition, the lack of enforcement of logical and physical access controls increases the risk of unauthorized access to systems and information. Furthermore, the weaknesses identified related to contingency planning may hinder Brookhaven's ability to complete essential mission functions in the event of a significant disruption.

In addition, without adequate performance monitoring and oversight, Brookhaven may not adequately address cybersecurity risks in a timely and effective manner. Improving the POA&M process could facilitate management's understanding of the cybersecurity risks at Brookhaven and help prioritize investments to ensure adequate protection of data and information systems. Furthermore, without an effective continuous monitoring process, the Authorizing Official may continue to lack the necessary situational awareness to operate information systems on an

ongoing basis. Based on the weaknesses identified during our review, we believe that additional action is necessary to help strengthen controls over Brookhaven's unclassified information systems.

RECOMMENDATIONS

To help improve management of Brookhaven's information security program, we recommend the Manager, Brookhaven Site Office, direct Brookhaven to:

1. Develop and implement site-level vulnerability and configuration management policies and procedures, as needed, to ensure system vulnerabilities are remediated and verified in a timely manner and that controls over network traffic are operating in a secure manner;

2. Ensure that logical and physical access controls are in place and operating effectively, including ensuring that all users complete cybersecurity awareness training prior to obtaining access to information systems and controlling physical access to restricted areas, as appropriate;

3. Enhance contingency planning and data retention processes to include conducting a Business Impact Analysis that identifies all essential mission and business functions, develops the necessary contingency plans, and ensures that all logging capabilities and archival processes are fully functional;

4. Implement fully effective policies and procedures related to POA&Ms to ensure that all identified cybersecurity weaknesses are tracked, prioritized, and remediated in a timely manner; and

5. Ensure that Brookhaven implements the most recent Federal cybersecurity requirements.

MANAGEMENT RESPONSE

Management concurred with the recommendations and provided initial corrective actions to address the issues identified in the report. For example, in response to our recommendation regarding vulnerability and configuration management weaknesses, management committed to developing and reviewing metrics to monitor controls at Brookhaven as part of its continuous monitoring process. In addition, management committed to conducting business impact assessments to identify and prioritize critical business components that, as noted in our report, is a critical aspect of contingency planning. Management also committed to reviewing both Department and Federal guidance on a regular basis to ensure that the most recent cybersecurity requirements are addressed.

While management fully concurred with our recommendations, its formal response noted additional concerns regarding the report. In particular, while management agreed that additional work is necessary to ensure that system vulnerabilities are detected and remediated in a timely manner, management did not agree that the report reflected its defense-in-depth cybersecurity posture. Specifically, management stated that before the audit could detect system vulnerabilities, Brookhaven personnel had disabled mitigating defenses to allow system scanning to take place. Management also commented that Brookhaven followed existing Department requirements, which reflected a specific version of Federal guidance at the time of our review. In addition, management did not agree with several statements regarding oversight of Brookhaven's cybersecurity program.

Management's comments are included in Appendix 3.

AUDITOR COMMENTS

Management's comments and planned corrective actions were responsive to our recommendations. As noted in the report, we acknowledge Brookhaven's use of a defense-in-depth cybersecurity posture, which provides a layered set of controls to mitigate risks, including items such as network segmentation, real-time system logging, multiple firewalls, and intrusion detection systems. However, despite the defense-in-depth strategy, our review determined that additional action is necessary to improve Brookhaven's security posture. While we agree that the Office of Science guidance reflects outdated Federal cybersecurity requirements, we found that Brookhaven's contract noted that it must adhere to all applicable Federal requirements. We agree that Brookhaven personnel had disabled mitigating defenses, allowing access to the network that might otherwise be denied. However, although Brookhaven provided us access, vulnerabilities still existed and there was no guarantee that the protections that had been disabled for us would be fully effective in protecting against external threats.

In addition, as noted in several previous reviews, the Office of Science had not updated its Program Cyber Security Plan since June 2010 to reflect new cybersecurity risks and changes to Federal or Department policy. While we have a long-standing recommendation in this area, the Office of Science officials have yet to update the Program Cyber Security Plan, potentially affecting the security posture of its program and sites. Furthermore, while management did not

agree with all oversight comments regarding the handling of POA&Ms, we found that Brookhaven was not adhering to established policy to ensure the effective use of POA&Ms to track, prioritize, and remediate all known cybersecurity weaknesses.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

To determine whether Brookhaven National Laboratory (Brookhaven) effectively managed its cybersecurity program.

Scope

The audit was performed between July 2015 and November 2016 at Brookhaven in Upton, New York. The audit included internal and external vulnerability scanning conducted by KPMG LLP (KPMG) on behalf of the Office of Inspector General (OIG). KPMG conducted external testing of unclassified networks and systems as an outsider without any elevated privileges. KPMG conducted internal scanning as an authenticated user (a user with a valid username and password) and reported on vulnerabilities that an insider or a remote attacker could exploit. Both internal and external scans took into consideration compensating controls. Furthermore, Brookhaven whitelisted KPMG scanners to allow and expedite the scanning of systems. Whitelisting is used to grant network access that might otherwise be denied. Testwork did not attempt to determine whether an actual attack had exploited vulnerabilities or circumvented existing controls. The audit was conducted under OIG project number A15TG027.

Methodology

To accomplish our objective, we:

- Reviewed applicable laws and regulations, including those pertaining to information and cybersecurity;
- Reviewed applicable standards and guidance issued by the Department of Energy, including the Office of Science;
- 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 (Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*);
- Reviewed prior reports issued by the Office of Inspector General and the Government Accountability Office;
- Used a statistically selected sample of 93 Brookhaven network accounts to determine whether users met the requirements for Brookhaven network access (active employee/guest, completed annual cyber training, signed computer use agreement);
- Held discussions with Brookhaven Site Office and contractor personnel; and

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

For our statistically selected sample of 93 Brookhaven network accounts, we used a 99 percent confidence rate, a precision level of plus or minus 5 percent, and an expected error rate of zero to determine the sample size. We used statistical sampling to enable us to project the sample results across the entire population of Brookhaven network accounts. However, we anticipated having zero errors, as Brookhaven should not have granted an individual access to the domain if they did not meet the criteria. We identified errors that limited our ability to project our sample results across the population.

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 the Department's implementation of the *GPRA Modernization Act of 2010* and determined that it had established performance measures related to cybersecurity. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our audit objective.

An exit conference was held with management on November 3, 2016.

RELATED REPORTS

Office of Inspector General Reports

- Audit Report on *The Department of Energy's Cybersecurity Risk Management Framework* (November 2015, DOE-OIG-16-02). The review determined that the Department of Energy (Department) had made progress toward implementing an unclassified cybersecurity risk management framework designed to reduce the likelihood of compromise to its information systems and data. However, we found that additional effort is needed to ensure that operating system risks are identified and systems and information are adequately secured. For example, programs and sites had not always properly categorized the risk to systems or implemented appropriate security controls. Although certain controls had been established, officials had not always thoroughly and independently assessed or monitored such controls to ensure they were effective. Furthermore, programs and sites had not ensured that authorizing officials responsible for accepting system risk were fully aware of the risks, weaknesses, and vulnerabilities to the information systems under their purview. The weaknesses identified existed, in part, because Federal requirements for securing information systems had not been fully implemented, and the Department had not established sufficient oversight and communication to support its cybersecurity risk management program. In addition, Federal officials had not provided adequate oversight to ensure that effective risk management practices had been implemented. Moreover, Department management had not always ensured that risk tolerances were established and communicated to field elements as required to help ensure the implementation of an effective risk management program.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program - 2015* (November 2015, DOE-OIG-16-01). This evaluation determined that the Department, including the National Nuclear Security Administration, had taken a number of positive steps over the past year to address previously identified cybersecurity weaknesses related to its unclassified cybersecurity program. While these actions were positive, our current evaluation found that the types of deficiencies identified in prior years continued to persist, such as issues related to security reporting, vulnerability management, system integrity of Web applications, and account management. The weaknesses identified occurred, in part, because the Department had not ensured that policies and procedures were fully developed and implemented to meet all necessary cybersecurity requirements. In addition, the Department had not always implemented an effective performance monitoring and risk management program. Furthermore, we noted that risk management processes at the locations reviewed were not always effective to identify and remediate cybersecurity weaknesses.

- Special Report on *Management Challenges at the Department of Energy - Fiscal Year 2016* (November 2015, OIG-SR-16-01). Based on the work performed during fiscal year 2015 the Office of Inspector General identified seven areas, including cybersecurity, that

remained management challenges for fiscal year 2016. It was included on the list because of the inherent risks, the identification of continuing cybersecurity weaknesses, and the sensitivity of much of the Department's work.

- Special Report on *The Department of Energy's July 2013 Cyber Security Breach* (December 2013, DOE/IG-0900). The July 2013 incident resulted in the exfiltration of a variety of personally identifiable information on over 104,000 individuals. Our review identified a number of technical and management issues that contributed to an environment in which this breach was possible. Compliance and technical problems included the frequent use of complete Social Security numbers as identifiers; the permission of direct internet access to a highly sensitive system without adequate security controls; the lack of assurance that required security planning and testing activities were conducted; and the failure to assign the appropriate level of urgency to replace end-of-life systems. We also identified numerous contributing factors related to inadequate management processes. These issues created an environment in which the cybersecurity weaknesses we observed could go undetected or uncorrected. While we did not identify a single point of failure that led to the breach, the combination of the technical and managerial problems that we observed set the stage for individuals with malicious intent to access the system with what appeared to be relative ease.

Government Accountability Office Report

- Government Accountability Office (GAO) Report on *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs* (GAO-15-714, September 2015). GAO found persistent weaknesses in protecting information and information systems at 24 Federal agencies, which illustrates the challenges Federal agencies face in effectively applying information security policies and practices. These deficiencies place critical information and information systems used to support the operations, assets, and personnel of Federal agencies at risk, and can impair agencies' efforts to fully implement effective information security programs. In prior reports, GAO and Inspectors General have made hundreds of recommendations to agencies to address deficiencies in information security controls and weaknesses in their programs, but many of these recommendations remain unimplemented.

MANAGEMENT COMMENTS

Department of Energy
Brookhaven Site Office
P.O. Box 5000
Upton, New York 11973

SEP 2 8 2016

MEMORANDUM FOR RICKEY R. HASS, ACTING INSPECTOR GENERAL
OFFICE OF INSPECTOR GENERAL
U.S. DEPARTMENT OF ENERGY

FROM: FRANK J. CRESCENZO, MANAGER
OFFICE OF SCIENCE
BROOKHAVEN SITE OFICE

SUBJECT: DRAFT REPORT ON BROOKHAVEN NATIONAL LABORATORY'S (BNL'S) CYBER SECURITY PROGRAM

Thank you for the opportunity to review and comment on the subject draft report. This was a comprehensive assessment of Brookhaven National Laboratory's (BNL's) cyber security policies and protections that identified weaknesses which the site office is committed to addressing. This feedback will help the Department of Energy (DOE) further their goal of protecting BNL's information systems from increasingly dangerous cyber threats and enabling world-class facilities and multi-disciplinary science programs.

The DOE Brookhaven Site Office (BHSO) agrees that additional work is needed to ensure that system vulnerabilities are detected and remediated in a timely manner, or mitigated to reduce the risk of an exploit. This is an ongoing effort to stay abreast of the increasing number of operating system and third party applications that require patching or updating to address security vulnerabilities. While we agree that some of these vulnerabilities exist, the report does not describe BNL's defense-in-depth cyber security posture that implements a layered set of controls to mitigate risks. Before the audit team was able to detect system vulnerabilities, laboratory personnel disabled those mitigating defenses to allow system scanning to take place. During normal operations, computer scans of BNL's network or anomalous behavior are routinely blocked from access to prevent this type of behavior. The scanners used for this report to perform credentialed scans are part of BNL's whitelisted vulnerability scanners, which provide much more detailed information than could be readily obtained by an attacker. During the external scans for this report, the computers were immediately blocked by BNL's cyber defenses, and once they were allowed to proceed, detected no significant vulnerabilities. BNL has robust perimeter defenses, network segmentation and intrusion detection systems to further mitigate the risk of attacks.

Brookhaven Science Associates (BSA) implements requirements included in their Management and Operating Contract. For the Cyber Security Program, these requirements include DOE Order 205.1B, which references the DOE Office of Science (SC) Program Cyber Security Plan (PCSP). At the time of this report, the PCSP specifically requires NIST SP 800-53 Revision 3 as the version for designing and implementing security controls. Based upon the aforementioned information and the oversight plan provided to the Office of Inspector General,

BHSO does not agree with several statements regarding oversight included in the report such as "Brookhaven Site Office officials had not ensured that contractors met the cyber security requirements of the site level contract." Additionally, BHSO does not agree with the statement that "a Federal oversight official provided direction to Brookhaven that did not require Brookhaven to track all weaknesses through remediation in a POAMs". Instead, the issue discussed was considered an internal program enhancement not involving significant risk, wherein internal processes were considered appropriate to track the status of the enhancement.

Below please find my Management Response to each recommendation with some specific actions provided in the attachment. BSA has committed to providing a more detailed Corrective Action Plan by October 30, 2016 and is in the process of updating security controls to NIST SP 800-53 Revision 4.

RECOMMENDATIONS:

1. Develop and implement site-level vulnerability and configuration management policies and procedures, as needed, to ensure system vulnerabilities are remediated and verified in a timely manner, and that controls over network traffic are operating in a secure manner.

2. Ensure that logical and physical access controls are in place and operating effectively, including ensuring that all users complete cyber security awareness training prior to obtaining access to information systems, and controlling physical access to restricted areas, as appropriate.

3. Enhance contingency planning and data retention processes to include conducting a Business Impact Analysis that identifies all essential mission and business functions, develops the necessary contingency plans, and ensures that all logging capabilities and archival processes are fully functional.

4. Implement fully effective policies and procedures related to Plans of Actions and Milestones (POAMs) to ensure that all identified cyber security weaknesses are tracked, prioritized, and remediated in a timely manner.

5. Ensure that Brookhaven implements the most recent Federal cyber security requirements.

MANAGEMENT RESPONSE:

The Brookhaven Site Office concurs with the recommendations and will direct BSA, the management and operating contractor at BNL, to:

1. Develop and implement site-level vulnerability and configuration management policies and procedures, as needed, to ensure system vulnerabilities are remediated and verified in a timely manner, and that controls over network traffic are operating in a secure manner.

   Estimated Completion Date: December 31, 2017

SEP 2 8 2016

2. Ensure that logical and physical access controls are in place and operating effectively, including ensuring that all users complete cyber security awareness training prior to obtaining access to information systems, and controlling physical access to restricted areas, as appropriate.

   Estimated Completion Date: March 31, 2017

3. Enhance contingency planning and data retention processes to include conducting a Business Impact Analysis that identifies all essential mission and business functions, develops the necessary contingency plans, and ensures that all logging capabilities and archival processes are fully functional.

   Estimated Completion Date: December 31, 2017

4. Implement fully effective policies and procedures related to POAMs to ensure that all identified cyber security weaknesses are tracked, prioritized, and remediated in a timely manner.

   Estimated Completion Date: December 31, 2016

5. Implement the most recent Federal cyber security requirements.

   Estimated Completion Date: December 31, 2016

If you have any questions please contact Kim Nekulak, of my staff, at (631) 344-7439.

Enclosure:
As Stated

cc w/enclosure:

J. Venneri, SC-41.1
S. Weekley, SC-CH
G. Smeets, SC-CH
F. Healy, SC-CH
N. Masincupp, SC-OR
E. Landini, SC-BHSO
J. Loh, SC-BHSO

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

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