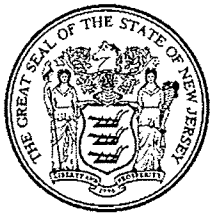

New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

New Jersey Office of Homeland Security and Preparedness

July 1, 2013 to October 30, 2015

Stephen M. Eells
State Auditor

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

PERI A. HOROWITZ
Executive Director
(609) 847-3901

OFFICE OF THE STATE AUDITOR
(609) 847-3470
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

GREGORY PICA
Assistant State Auditor

JOHN J. TERMYNA
Assistant State Auditor

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Vincent Prieto
Speaker of the General Assembly

Ms. Peri A. Horowitz
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the New Jersey Office of Homeland Security and Preparedness for the period of July 1, 2013 to October 30, 2015. If you would like a personal briefing, please call me at (609) 847-3470.

Stephen M. Eells
State Auditor
May 18, 2016

Table of Contents

Scope

We have completed an audit of the New Jersey Office of Homeland Security and Preparedness (OHSP) for the period July 1, 2013 to October 30, 2015. We did not review the data within the State Asset Database, Operation Management System, and the Suspicious Activity Report System due to security clearance issues. Our audit included financial activities accounted for in the state's General Fund.

Expenditures of the OHSP during our audit period were $175.4 million including reimbursements to sub-grantees. Revenues for the same period were $139.5 million in state-match monies and drawdowns of federal grants. Per Governor Jon S. Corzine's Executive Order #5, OHSP was created as a cabinet-level office to administer, coordinate, lead, and supervise New Jersey's counter-terrorism and preparedness efforts. The goal of this office is to coordinate emergency response efforts across all levels of government, law enforcement, emergency management, non-profit organizations, other jurisdictions, and the private sector, and to protect the people of New Jersey.

Objectives

The objectives of our audit were to determine whether financial transactions were related to the OHSP's programs, were reasonable, and were recorded properly in the accounting systems. Additional objectives were to determine the effectiveness of monitoring sub-grantee compliance and the adequacy of information technology (IT) general controls pertaining to the OHSP's significant IT systems. We also tested for resolution of the significant conditions noted in our prior report dated August 20, 2009.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

In preparation for our testing, we studied legislation, the administrative code, circular letters promulgated by the Department of the Treasury, and policies of the OHSP. Provisions we considered significant were documented and compliance with those requirements was verified by interview, observation, and through our testing of financial transactions. We also read the budget messages, reviewed financial and program activity trends, and interviewed OHSP personnel to obtain an understanding of the programs and the internal controls.

Statistical and non-statistical sampling approaches were used. Our samples of financial transactions were designed to provide conclusions on our audit objectives, as well as internal controls and compliance. Sample populations were sorted and transactions were judgmentally or randomly selected for testing.

To ascertain the status of findings included in our prior report, we identified corrective action, if any, taken by the office and walked through the system to determine if the corrective action was effective.

Conclusions

We found that the financial transactions included in our testing were related to the OHSP's programs, were reasonable, and were recorded properly in the accounting systems. We also found effective compliance of sub-grantee monitoring and adequate information technology general controls pertaining to the OSHP's significant IT systems. In making these determinations, we noted certain control weaknesses regarding a professional service contract, sub-grantee compliance with grant agreements, and information technology general controls meriting management's attention. We found that the OHSP had resolved the significant issues noted in our prior audit report.

We also made an observation concerning the Critical Infrastructure Protection Bureau.

Grant Management System

An agreement without enforceable deadlines caused increased project costs.

OHSP currently uses the Grant Tracking System (GTS) to track homeland security grant funding from the awarding of the grant to the grant reimbursement to the sub-grantee. In 2012, OHSP management determined the need for a new system to replace the old GTS which was created in 2005. This new Grant Management System would be a web-based system that would allow the office to timely review and manage grants and remedy the shortcomings of GTS.

The state's Office of Information Technology (OIT) approved the one-year project for June 1, 2012 to May 31, 2013 for $396,000 or 3,650 hours. The OHSP hired two hourly programmers for the project from a consulting firm listed on the state's IT professional service contract at an approved hourly rate. After multiple extensions on the original purchase order, resources spent on the project reached 8,044 hours totaling $861,000. Now, however, to finish the project by June 30, 2016, OHSP issued another purchase order for an additional $177,000. If completed, total costs and hours would be $1,161,000 and 9,781, respectively.

The contract agreement did not clearly define the scope of the project, associated costs, and delivery dates. Therefore, OHSP management did not have an effective process to control costs and ensure timely completion of the project. New Jersey Department of the Treasury Circular Letter 14-07-DPP/OMB/OIT states, "The requesting agency has primary responsibility for obtaining maximum value from its Professional Service contracts and to ensure that all deliverables are satisfactorily provided according to agreed upon schedule." In addition, Federal Regulations 44 CFR 13.36 Procurement b.10 states that grantees and sub-grantees will use time and material type contracts only if the contract includes a ceiling price that the contractor exceeds at its own risk.

We also noted the consultants' billable hours were not always accurately supported by daily sign in/out sheets. We observed the consultants did not always fill out these sheets, or their sign-in time did not always reflect their actual arrival time.

Recommendation

We recommend, for future projects, that OHSP management utilize contract agreements with clearly defined scopes, enforceable deadlines, and cost ceilings.

Sub-Grantee Noncompliance with Grant Agreement

Monitoring of sub-grantee compliance should be strengthened.

The Office of Homeland Security and Preparedness, the grantee, is the State Administrative Agency for various federal grant programs. Per the Grant Tracking System from July 1, 2013 to August 10, 2015, OHSP reimbursed sub-grantees $20.4 million for qualified expenditures relating to the equipment, exercise, or training categories. We judgmentally sampled five counties with grant reimbursements totaling $8.3 million from the above categories for our field visits. We randomly selected 111 purchase orders from 13 sub-grantees. These 13 sub-grantees were comprised of county agencies, colleges, non-profit organizations, and a hospital.

Per the grant agreement, individual equipment items with an original cost of at least $1,000 and an expected useful life of three years or more must be maintained on an equipment inventory system. In addition, sub-grantees who receive funding from OHSP shall ensure that all vendors they intend to do business with are not listed as an excluded entity on the federal System for Award Management or a debarred agency on New Jersey's Consolidated Debarment Report. Sub-recipients shall retain a copy of the search results with the procurement documents. This process ensures that vendors are in good standing status when goods or services are purchased.

We noted the sub-grantees did not fully comply with grant agreements on maintaining debarment documents and equipment management when procuring goods and services from vendors.

We noted the following exceptions.

- Our sample included 99 purchases from non-state contract vendors and noted 23 incidents where sub-grantees did not maintain records documenting the verification of vendors to either the federal or state debarment databases. However, we noted no debarred vendors in our testing.

- Our sample included 16 equipment items, each with an acquisition cost over $1,000 and expected useful lives of three years or more. We noted seven instances when items were not found in the equipment inventory system and five instances where the sub-grantees did not have an equipment inventory system. We physically located all items tested.

In addition, we found four security systems ranging in cost from $9,300 to $43,000 that were procured without competitive bidding.

Recommendation

We recommend OHSP management strengthen its monitoring procedures for sub-grantees to include a review of debarment and equipment records. In addition, Department of the Treasury regulations should be followed in regards to competitive bidding.

»➤«

Information Technology

State Asset Database (SADB)

Compliance with SADB's policies and timely monitoring of SADB access activities would enhance the protection of security data regarding the state's critical infrastructure.

SADB is a web-based tool created in 2012 to be used by OHSP and designated local government staffs. The database stores site specific data on facilities that meet the New Jersey Critical Infrastructure Criteria Matrix. When the criteria are met, the assets are classified as Critical Infrastructure Key Resource (CIKR). The national, state, local, or special interest assets include systems or physical assets that are so vital to the state that the incapacitation or destruction of such would create a debilitating impact on the economy, life safety, or security of New Jersey citizens.

Per OHSP's policy, to gain access to the SADB's state and national asset access level, an individual must meet the following requirements.

- Access requests must be on a need-to-know basis and properly approved.
- Complete the annual Protected Critical Infrastructure Information (PCII) training and maintain current certification on file with the system administrator.
- Complete a one-time Chemical-terrorism Vulnerability Information (CVI) training and maintain the certification on file with the system administrator.

Our review disclosed the following noncompliance exceptions.

- OHSP management did not utilize and maintain the access request forms on file to document that access privileges were properly reviewed and approved based on needs and job functions of requested individuals.
- Of the 61 individuals with SADB's state and national asset access level, we noted 8 did not have PCII training, 2 did not renew their annual certifications, and one did not have CVI training.

We also reviewed SADB's activity logs and noted that 22 users with access had no activity for more than one year. In addition, we noted the system does not require external users to change their passwords on a scheduled basis. OHSP's Network & Computer User Manual states, "Passwords shall be changed on a regular rotational basis; a system generated reminder will prompt users at least every 90 days to change their passwords." However, this policy only applies to internal users.

Noncompliance to internal policy and weak IT general controls on logical access increases the risk of improper access of critical data.

Recommendation

We recommend that OHSP management adhere to its policies and provide system access on a need basis only. These privileges should be reviewed periodically to ensure need is still warranted. In addition, OHSP management should implement a system prompt to require the changing of the passwords for external users every 90 days.

Operation Management System (OMS)

A written comprehensive policy is needed to protect confidential data in the OMS.

Operation Management System (OMS) is a web-based application that was created in 2007. The system is utilized by the Analysis Bureau and the Operation Bureau within the Division of Intelligence. OMS is structured into different modules for different levels of access capabilities. The four main modules in the application are for storing information relating to: intelligence, informant contacts, employee background checks, and information on sector specific businesses. Currently, there are 126 users of this system comprised of OHSP investigators and analysts, and 92 external users (guests) from the FBI, Coast Guard, State Police, and Port Authority, as well as OHSP's interns.

Access privileges were granted to users without documentation of the approval process. Our review disclosed that the 92 guests erroneously had access to the intelligence module. Those access privileges were immediately removed upon our notification to OHSP management. Adequate documentation of the user groups and access privileges based on job responsibilities would lower the risk of unauthorized access to the system.

Our review also disclosed that an OHSP intern that separated from OHSP in 2010 did not have their access privilege removed. The privilege was removed upon our notification to OHSP management. Untimely removal of access privilege may lead to unauthorized access and use of the sensitive data.

Our review of OMS activity logs as of October 21, 2015 disclosed that 57 users had not accessed the system in over two years. Users should be periodically reviewed and evaluated for current activity to ensure access privileges are required.

In addition, we noted the system does not require external users to change their passwords on a scheduled basis. OHSP's Network & Computer User Manual states, "Passwords shall be changed on a regular rotational basis; a system generated reminder will prompt users at least every 90 days to change their passwords." However, this policy only applies to internal users.

OHSP management did not establish a written policy to properly administer and document access privileges based on job responsibilities. Federal industry best practices for information systems recommend that an entity should implement effective authorization controls that include, at a minimum, the principle of least privilege and user accounts should be appropriately controlled. In addition, inactive accounts and accounts for separated individuals are to be disabled and removed timely.

Recommendation

We recommend that OHSP management develop comprehensive policies, implement necessary controls, and document the review and approval process to ensure that access privileges are only granted based on job responsibilities. OHSP management should also timely review system activity logs to identify and evaluate inactive accounts for timely removals. In addition, OHSP management should implement a system prompt to require external users to change their passwords every 90 days.

»➤◂«

Business Continuity and Data Recovery

The OHSP Information Technology Bureau has not tested its business continuity plan.

OHSP has one business continuity plan for all its systems but it has not been tested. OHSP should comply with their Disaster Recovery Manual by performing periodic testing exercises in order to thoroughly train recovery personnel and ensure the strategies and actions accurately reflect current business recovery requirements. Industry best practices require periodic testing of the business continuity plan to ensure adequate controls are in place and functioning properly to minimize the loss of data if a disruption were to occur. Testing is also important because it measures the feasibility of the plan and identifies any modifications that may be required because of noted weaknesses.

Recommendation

We recommend OHSP management periodically test the business continuity plan as stated in the OHSP Disaster Recovery Plan.

»➤◂«

Observation

Critical Infrastructure Protection Bureau

Effective procedures are needed to better protect state Critical Infrastructure Key Resources.

The mission of the Critical Infrastructure Protection Bureau is to ensure the protection, preparedness, and resiliency of New Jersey Critical Infrastructure Key Resources (CIKR). One of its six core functions is to perform Site Assessment Visits (SAVs) on the physical security of qualified CIKR in New Jersey. Identified security gaps and recommendations are provided to the owners or operators of the facilities and the reports are uploaded into OHSP's restricted access State Assets Database (SADB). We did not have access to SADB and were not able to view the reports to ascertain the significance of any security gaps that were identified in the SAVs. Currently, there is no written policy to prioritize how many sites should be selected for the assessments. As of April 30, 2015, the bureau had identified 773 state level critical assets of which approximately 90 percent are privately owned. From 2006 to October 2015, the combined total of all SAVs performed by OHSP's staff and local government agencies totaled 101. In addition, we were informed by OHSP that the office does not have the enforcing authority to require improvements or corrections on identified security gaps. However, New Jersey Statutes Annotated C.App.A:9-73 allows the Attorney General to institute an action or proceeding in the Superior Court for equitable and other relief, which the court shall order if necessary to preserve, protect, or sustain the public safety or well-being.

P.L. 2001, Chapter 246 states that the Infrastructure Advisory Committee shall act as a liaison to private industry throughout the state and establish ongoing communication between private industry and any other private entity, and state and local officials regarding domestic preparedness and the respective roles and responsibilities of the public and private sectors. Our review of the minutes for the quarterly meetings of the Infrastructure Advisory Committee in calendar year 2015 made no mention of any security gap discussions.

The national and state's CIKR are significant assets with great impact to the security of the state, the state's economic security, public health, and public safety. Performing sufficient SAVs, sharing identified risks to key members of specific industries, and enforcing the resolution on security gaps would ensure better protection of critical infrastructures in the state. Facility owners and operators of both the private and public sectors have responsibilities to protect not just their critical assets, but also the affected citizens of New Jersey.

CHRIS CHRISTIE
GOVERNOR

KIM GUADAGNO
LT. GOVERNOR

State of New Jersey
Office of Homeland Security and Preparedness
PO Box 091
TRENTON, NJ 08625-0091

CHRIS RODRIGUEZ
DIRECTOR

May 13, 2016

Mr. Gregory Pica, Assistant State Auditor
Office of Legislative Services
Office of the State Auditor
125 South Warren Street
PO Box 067
Trenton, NJ 08625-0067

Mr. Pica:

Enclosed is the New Jersey Office of Homeland Security and Preparedness response to the NJ State Audit findings conducted from July 1, 2013 to October 30, 2015 by your office.

Please include this document with your release of the audit to the Governor and the Legislature.

Sincerely,

Jared M. Maples
Director of Administration

Enclosure

c: Dr. Christopher Rodriguez, Director
Mr. Steven Gutkin, Deputy Director
Mr. Dennis Quinn, Chief of Staff

State of New Jersey
Office of Homeland Security and Preparedness

Audit Findings & Response
July 1, 2013 – October 30, 2015

Office of Legislative Services
Office of the State Auditor

Grant Management System

Finding

An agreement without enforceable deadlines caused increased project costs.

OHSP currently uses the Grant Tracking System (GTS) to track homeland security grant funding from the awarding of the grant to the grant reimbursement to the sub-grantee. In 2012, OHSP management determined the need for a new system to replace the old GTS which was created in 2005. This new Grant Management System would be a web-based system that would allow the office to timely review and manage grants and remedy the shortcomings of GTS.

The state's Office of Information Technology (OIT) approved the one-year project for June 1, 2012 to May 31, 2013 for $396,000 or 3,650 hours. The OHSP hired two hourly programmers for the project from a consulting firm listed on the state's IT professional service contract at an approved hourly rate. After multiple extensions on the original purchase order, resources spent on the project reached 8,044 hours totaling $861,000. Now, however, to finish the project by June 30, 2016, OHSP issued another purchase order for an additional $177,000. If completed, total costs and hours would be $1,161,000 and 9,781, respectively.

The contract agreement did not clearly define the scope of the project, associated costs, and delivery dates. Therefore, OHSP management did not have an effective process to control costs and ensure timely completion of the project. New Jersey Department of the Treasury Circular Letter 14-07-DPP/OMB/OIT states, "The requesting agency has primary responsibility for obtaining maximum value from its Professional Service contracts and to ensure that all deliverables are satisfactorily provided according to agreed upon schedule." In addition, Federal Regulations 44 CFR 13.36 Procurement b.10 states that grantees and sub-grantees will use time and material type contracts only if the contract includes a ceiling price that the contractor exceeds at its own risk.

We also noted the consultants' billable hours were not always accurately supported by daily sign in/out sheets. We observed the consultants did not always fill out these sheets, or their sign-in time did not always reflect their actual arrival time.

Recommendation

We recommend for future projects that OHSP management utilize contract agreements with clearly defined scopes, enforceable deadlines, and cost ceilings.

Response

The OHSP Information Technology Bureau (IT) recognizes the recommendation and will continue to adhere to statutory and regulatory requirements of the US Department of Homeland Security, NJ Treasury Division of Purchase and Property, and NJ Office of Information Technology, as appropriate, to clearly define the scope, enforceable deadlines, and cost ceilings for contract agreements in all applicable projects.

Sub-Grantee Noncompliance with Grant Agreement

Finding

Monitoring of sub-grantee compliance should be strengthened.

The Office of Homeland Security and Preparedness (OHSP), the grantee, is the State Administrative Agency for various federal grant programs. Per the Grant Tracking System from July 1, 2013 to August 10, 2015, OHSP reimbursed sub-grantees $20.4 million for qualified expenditures relating to the equipment, exercise, or training categories. We judgmentally sampled five counties with grant reimbursements totaling $8.3 million from the above categories for our field visits. We randomly selected 111 purchase orders from 13 sub-grantees. These 13 sub-grantees were comprised of county agencies, colleges, non-profit organizations, and a hospital.

Per the grant agreement, individual equipment items with an original cost of at least $1,000 and an expected useful life of three years or more must be maintained on an equipment inventory system. In addition, sub-grantees who receive funding from OHSP shall ensure that all vendors they intend to do business with are not listed as an excluded entity on the federal System for Award Management or a debarred agency on New Jersey's Consolidated Debarment Report. Sub-recipients shall retain a copy of the search results with the procurement documents. This process ensures that vendors are in good standing status when goods or services are purchased.

We noted the sub-grantees did not fully, comply with grant agreements on maintaining debarment documents and equipment management when procuring goods and services from vendors.

We noted the following exceptions.

- Our sample included 99 purchases from non-state contract vendors and noted 23 incidents where sub-grantees did not maintain records documenting the verification of vendors to either the federal or state debarment databases. However, we noted no debarred vendors in our testing.

- Our sample included 16 equipment items, each with an acquisition cost over $1,000 and expected useful lives of three years or more. We noted seven instances when items were not found in the equipment inventory system and five instances where the sub-grantees did not have an equipment inventory system. We physically located all items tested.

In addition, we found four security systems ranging in cost from $9,300 to $43,000 that were procured without competitive bidding.

Recommendation

We recommend OHSP management strengthen its monitoring procedures for sub-grantees to include a review of debarment and equipment records. In addition, Department of the Treasury regulations should be followed in regards to competitive bidding.

Response

Instances where sub-grantees failed to maintain records documenting the verification of vendors to either the federal or state debarment databases.

During each semi-annual Monitor Review, the Grants Management Bureau (GMB) staff will verify that all homeland security funded sub-grantees and purchases have been reviewed against federal and state vendor debarment and suspension lists. Furthermore, sub-grantees will be instructed to retain a screen shot of each vendor debarment check for compliance and auditing purposes. The results will be captured by the GMB staff in the Grant Liaison Monitor Review Report.

In addition, the GMB plans to roll out the new Grant Management System (GMS) replacing the Grant Tracking System in the near future. A section of the new GMS will require the sub-grantee to affirm that a federal and state vendor debarment check was conducted for each vendor providing HSGP or NSGP funded goods or services.

Instances where sub-grantees failed to properly inventory equipment or do not have an inventory system.

The GMB staff has and will continue with its Monitor Review efforts to include a compliance check with respect to inventory requirements and inventory systems. The Monitor Review reports currently have a section specific to inventory requirements. This section will be modified to include specific inventory requirements (for example, Inventory Sample Collected and Attached) for inclusion within the Monitor Review Report.

Instances where sub-grantees failed to follow the Department of the Treasury Regulations regarding the competitive bidding process.

The GMB will use a risk assessment process to identify any potential at-risk sub-grantees to ensure that all procurement transactions are conducted in a manner providing full and open competition in accordance with applicable State and federal requirements. Entities identified as "at-risk" will be subject to additional audit monitoring as needed. In addition, the GMB staff will incorporate within its Monitor Review efforts a random sampling of procurements to evaluate compliance. A section of the Monitor Review report will be revised to include examination of competitive bidding documents. Finally, GMB will incorporate additional curriculum into any sub-grantee award workshops.

Information Technology

Finding

State Asset Database (SADB)

Compliance with SADB's policies and timely monitoring of SADB access activities would enhance the protection of security data regarding the state's critical infrastructure.

SADB is a web-based tool created in 2012 to be used by OHSP and designated local government staffs. The database stores site specific data on facilities that meet the New Jersey Critical Infrastructure Criteria Matrix. When the criteria are met, the assets are classified as Critical Infrastructure Key Resource (CIKR). The national, state, local, or special interest assets include systems or physical assets that are so vital to the state that the incapacitation or destruction of such would create a debilitating impact on the economy, life safety, or security of New Jersey citizens.

Per OHSP's policy, to gain access to the SADB's state and national asset access level, an individual must meet the following requirements.

- Access requests must be on a need-to-know basis and properly approved.
- Complete the annual Protected Critical Infrastructure Information (PCII) training and maintain current certification on file with the system administrator.
- Complete a one-time Chemical-terrorism Vulnerability Information (CVI) training and maintain the certification on file with the system administrator.

Our review disclosed the following noncompliance exceptions.

- OHSP management did not utilize and maintain the access request forms on file to document that access privileges were properly reviewed and approved based on needs and job functions of requested individuals.
- Of the 61 individuals with SADB's state and national asset access level, we noted 8 did not have PCII training, 2 did not renew their annual certifications, and one did not have CVI training.

We also reviewed SADB's activity logs and noted that 22 users with access had no activity for more than one year. In addition, we noted the system does not require external users to change their passwords on a scheduled basis. OHSP's Network & Computer User Manual states, "Passwords shall be changed on a regular rotational basis; a system generated reminder will prompt users at least every 90 days to change their passwords." However, this policy only applies to internal users.

Noncompliance to internal policy and weak IT general controls on logical access increases the risk of improper access of critical data.

Recommendation

We recommend that OHSP management adhere to its policies and provide system access on a need basis only. These privileges should be reviewed periodically to ensure need is still warranted. In addition, OHSP management should implement a system prompt to require the changing of the passwords for external users every 90 days.

Response

All persons nominated for access to SADB are required to have a need-to-know and a right-to-know to have access to the database. Before access is granted, each user must hold a valid certification for Protected Critical Infrastructure Information (PCII) and Chemical-terrorism Vulnerability Information (CVI).

OHSP IT has re-aligned the procedure for employee separation activities to include disabling accounts in SADB. Furthermore, OHSP IT will work with the Infrastructure Protection and Training Bureau (IPT) to review users that have not logged in within the past year and create a database to track the certifications held by the users (PCII and CVI). When the certification is within one month of expiration, the SADB administrator will be notified and again within one week of expiration. Following those notifications, the account will be disabled when the certification expires. Finally, the SADB login processing will be updated to require users to follow the current OHSP password guidelines.

Finding

Operation Management System (OMS)

A written comprehensive policy is needed to protect confidential data in the OMS.

Operation Management System (OMS) is a web-based application that was created in 2007. The system is utilized by the Analysis Bureau and the Operation Bureau within the Division of Intelligence. OMS is structured into different modules for different levels of access capabilities. The four main modules in the application are for storing information relating to: intelligence, informant contacts, employee background checks, and information on sector specific businesses. Currently, there are 126 users of this system comprised of OHSP investigators and analysts, and 92 external users (guests) from the FBI, Coast Guard, State Police, and Port Authority, as well as OHSP's interns.

Access privileges were granted to users without documentation of the approval process. Our review disclosed that the 92 guests erroneously had access to the intelligence module. Those access privileges were immediately removed upon our notification to OHSP management. Adequate documentation of the user groups and access privileges based on job responsibilities would lower the risk of unauthorized access to the system.

Our review also disclosed that an OHSP intern that separated from OHSP in 2010 did not have their access privilege removed. The privilege was removed upon our notification to OHSP management. Untimely removal of access privilege may lead to unauthorized access and use of the sensitive data.

Our review of OMS activity logs as of October 21, 2015 disclosed that 57 users had not accessed the system in over two years. Users should be periodically reviewed and evaluated for current activity to ensure access privileges are required.

In addition, we noted the system does not require external users to change their passwords on a scheduled basis. OHSP's Network & Computer User Manual states, "Passwords shall be changed on a regular rotational basis; a system generated reminder will prompt users at least every 90 days to change their passwords." However, this policy only applies to internal users.

OHSP management did not establish a written policy to properly administer and document access privileges based on job responsibilities. Federal industry best practices for information systems recommend that an entity should implement effective authorization controls that include, at a minimum, the principle of least privilege and user accounts should be appropriately controlled. In addition, inactive accounts and accounts for separated individuals are to be disabled and removed timely.

Recommendation

We recommend that OHSP management develop comprehensive policies, implement necessary controls, and document the review and approval process to ensure that access privileges are only granted based on job responsibilities. OHSP management should also timely review system activity logs to identify and evaluate inactive accounts for timely removals. In addition, OHSP management should implement a system prompt to require external users to change their passwords every 90 days.

Response

All persons nominated for access to OMS are required to have a need-to-know and a right-to-know to have access to the database based upon their respective job responsibilities.

OHSP IT has re-aligned the procedure for employee separation activities to include disabling accounts in OMS. Additionally, OHSP IT will work with the Investigations Bureau to review those users that have not logged in within the past year and determine if their accounts should be disabled or closed. Finally, the OMS login processing will be updated to require users to follow the current OHSP password guidelines.

Finding

Business Continuity and Data Recovery

The OHSP Information Technology Bureau has not tested its business continuity plan.

OHSP has one business continuity plan for all its systems but it has not been tested. OHSP should comply with their Disaster Recovery Manual by performing periodic testing exercises in order to thoroughly train recovery personnel and ensure the strategies and actions accurately reflect current business recovery requirements. Industry best practices require periodic testing of the business continuity plan to ensure adequate controls are in place and functioning properly to minimize the loss of data if a disruption were to occur. Testing is also important because it measures the feasibility of the plan and identifies any modifications that may be required because of noted weaknesses.

Recommendation

We recommend OHSP management periodically test the business continuity plan as stated in the OHSP Disaster Recovery Plan.

Response

OHSP IT will conduct annual testing of all IT infrastructure at primary and backup locations and align these priorities with OHSP's Continuity of Operations Plan (COOP), last updated in April 2016.

Observation

Critical Infrastructure Protection Bureau

Effective procedures are needed to better protect state Critical Infrastructure Key Resources.

The mission of the Critical Infrastructure Protection Bureau is to ensure the protection, preparedness, and resiliency of New Jersey Critical Infrastructure Key Resources (CIKR). One of its six core functions is to perform Site Assessment Visits (SAVs) on the physical security of qualified CIKR in New Jersey. Identified security gaps and recommendations are provided to the owners or operators of the facilities and the reports are uploaded into OHSP's restricted access State Assets Database (SADB). We did not have access to SADB and were not able to view the reports to ascertain the significance of any security gaps that were identified in the SAVs. Currently, there is no written policy to prioritize how many sites should be selected for the assessments. As of April 30, 2015, the bureau had identified 773 state level critical assets of which approximately 90 percent are privately owned. From 2006 to October 2015, the combined total of all SAVs performed by OHSP s staff and local government agencies totaled 101. In addition, we were informed by OHSP that the office does not have the enforcing authority to require improvements or corrections on identified security gaps. However New Jersey Statutes Annotated C.App.A:9-73 allows the Attorney General to institute an action or proceeding in the Superior Court for equitable and other relief which the Court shall order if necessary to preserve; protect, or sustain the public safety or well-being.

P.L. 2001, Chapter 246 states that the Infrastructure Advisory Committee shall act as a liaison to private industry throughout the state and establish ongoing communication between private industry and any other private entity, and state and local officials regarding domestic preparedness and the respective roles and responsibilities of the public and private sectors. Our review of the minutes for the quarterly meetings of the Infrastructure Advisory Committee in calendar year 2015 made no mention of any security gap discussions.

The national and state's CIKR are significant assets with great impact to the security of the state, the state's economic security, public health, and public safety. Performing sufficient SAVs, sharing identified risks to key members of specific industries, and enforcing the resolution on security gaps would ensure better protection of critical infrastructures in the state. Facility owners and operators of both the private and public sectors have responsibilities to protect not just their critical assets, but also the affected citizens of New Jersey.

Response

The Critical Infrastructure Protection Bureau's (CIPB) mission is to ensure the protection, preparedness, and resiliency of New Jersey's Critical Infrastructure and Key Resources (CIKR), which include both public assets and privately owned infrastructure resources. The CIBP, now renamed the Infrastructure Protection and Training Bureau (IPT), collaborates with the US Department of Homeland Security (US DHS), sector specific State agencies including the New Jersey Board of Public Utilities (NJBPU), New Jersey Department of Environmental Protection (NJDEP), and the New Jersey Department of Health, and CIKR owners and operators, to take proactive steps to manage risk, strengthen facility security, and improve resilience.

To fulfill its mission, the IPT directs its activities through six core functions:

1. Staff assignments to each of the 16 critical infrastructure sectors identified by Presidential Policy Directive 21.
2. Infrastructure Advisory Committee (IAC) coordination.
3. State Asset Database (SADB) management and maintenance.
4. Vulnerability and risk assessments through Site Assessment Visits (SAV), Rapid Survey Tool (RST), and other US DHS toolsets.
5. Private Sector Exercise Program.
6. Private Sector Coordination Desk operations at the State Emergency Operations Center.

In addition, the IPT's strategic focus is guided by: (1) threat and vulnerability assessments; (2) the National Infrastructure Protection Plan (NIPP); (3) the New Jersey Domestic Security Preparedness Act; (4) Title 6 of the Code of Federal Regulations requirements for the handling of critical infrastructure information; (5) national and international reporting trends; (6) suspicious activity reports regarding terrorism threats; and (7) business requirements of the public and private sectors.

The New Jersey Domestic Security Preparedness Act (Act), N.J.S.A. App. A:9-64 et seq., established the IAC as a "liaison to private industry throughout the State [. . .] [and] a resource to the [Domestic Security Preparedness Task Force]. . . ." N.J.SA. App. A:9-70. The IAC acts as an advisory body to the Domestic Security Preparedness Task Force (Task Force) "with respect to domestic preparedness issues facing private industry and other private entities." N.J.S.A. App. A:9-70. In doing so, the IAC, in coordination with the IPT, assists the Task Force in helping to understand the unique risk profiles and vulnerabilities of each of the critical infrastructure sectors across the State.

Additionally, the Act grants authority to the Task Force to adopt "domestic security and preparedness standards, guidelines and protocols" in order to "preserve, protect and sustain the critical assets of the State's infrastructure" as applicable to public and private entities. N.J.S.A. App. A:9-69(a). In support of this mandate, the IAC reviews standards, guidelines, and protocols considered by the Task Force. N.J.S.A. App. A:9-69(a). Through the Act and the provisions of Executive Order #5 (Corzine), the Task Force has required certain state critical infrastructure facilities to provide it and OHSP with documentation that identified risks and vulnerability assessments and other required security information. These reports created a baseline for OHSP, the IPT, and the Task Force to evaluate the security posture of those critical

infrastructure facilities.

IPT is currently in the process of working with representative working groups from each of the 16 critical infrastructure sectors and their subsectors as defined by Presidential Policy Directive 21 to update security focused best practices for each sector. Upon completion, the updated best practices will be disseminated to critical infrastructure facilities throughout the State. These best practices will identify security and resiliency measures to address gaps in security, including physical security enhancements, cyber security protocols, and resiliency recommendations. The recommendations align with other regulatory requirements unique to each specific sector, including the North American Electric Reliability Corporation, Federal Energy Regulatory Commission, National Institute of Standards for Technology, Chemical Facility Anti-Terrorism Standards, Nuclear Regulatory Commission, NJBPU, and NJDEP. Sector best practices will also be reviewed for approval by the Task Force and then implemented by the specific State agency or private entity as applicable.

Recognizing the effect of the State's critical infrastructure on the stability of New Jersey's economy, public health, and safety, OHSP regularly assesses its strategic focus and operations based on the continually changing threat environment. These reviews inform the priorities identified in the IPT's six core functions, which guide IPT's implementation for the protection of critical infrastructure and key resources. Overall, the public and private sector partnership approach as envisioned in the Act has resulted in a collaborative working environment between those sectors that combats threats to the State's critical infrastructure and key resources and enhances New Jersey's overall domestic security and resilience.