New Jersey Office of the State Auditor Update

Dan Altobelli, CPA, CISA, CEH

Managing Auditor

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

About the Office of the State Auditor

- The State Auditor is a constitutional officer appointed and confirmed by a joint session of the Legislature.
- Office is administratively located within the Office of Legislative Services(OLS), a non-partisan office established to assist the Legislature in their mission.
- The office consists of approximately 92 professionals and four administrative staff.
- Reports are public and directed to the Governor, Senate President, Speaker of the Assembly and the Executive Director of OLS.

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

About the Office of the State Auditor

- Established as the Legislative watchdog over the other branches of government, authorities, commissions, and other legislatively mandated entities.
- Established in a manner critical to independence as compared to other audit organizations in the state. (In fact and appearance)
- All reporting is in compliance with *GAS* (GAO yellow book).

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Mission

- To provide independent, unbiased, timely, and relevant information to the Legislature, agency management, and the citizens of New Jersey which can be used to improve the operations and accountability of public entities.
- Reporting includes recommendations on how to improve the workings of government and how to strengthen agency internal controls.

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Types of Audits Performed

- We are authorized to conduct post-audits of all transactions and accounts kept by or for all agencies of State Government.
- We are authorized to conduct performance audits of any program or entity that receives state funds (follow *GAS*).
- We are authorized to perform forensic audits of any school district which has a year-end general fund deficit and one of several reporting criteria indicated in the enabling legislation.

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Types of Audits Performed

- We perform:
  - Financial statement opinion audits
  - Performance Audits
    - Internal control effectiveness
    - Program effectiveness, economy, and efficiency
    - Program compliance
  - Forensic audits of school districts

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Types of Audits Performed

- We perform:
  - Financial statement opinion audits
  - Performance Audits
    - Internal control effectiveness
    - Program effectiveness, economy, and efficiency
    - Program compliance
  - Forensic audits of school districts

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

How Are We Doing?

- Last 10 years:
  - Average of 26 reports each calendar year
  - Potential cost savings and revenue enhancements averaging $166 million annually
  - This works out to approximately $1.25 million per auditor per year.
- In addition, we have noted a significant number of internal control improvements which have no doubt added to the efficiency and effectiveness of State operations which were not measurable in dollars.

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

How Are We Doing?

- Legislation requires us to perform annual compliance reviews of recently published audit reports.
- In December of each year, we assess compliance with our recommendations for all audits published in the preceding fiscal year. We also follow up on all non-compliant or partially compliant items from the previous year's compliance report.
- Fiscal Year 2018 review found that 71% of our recommendations were fully or partially complied with.
- For the 2-year period (including FY2017 carry over items) – 84% compliance.

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Ethical Hacking

- Information Security
- Standards and Criteria
- Ethical Hacking Process at the OSA
- Major Finding Areas
- Reporting the Results
- Where are we going with this?

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Information Security

- What is the purpose of information security?
  - It's all about loss.

- The state collects and maintains a LARGE amount of data
  - Personally Identifiable Information (PII)
  - Confidential Information

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Information Security

- Public entities are charged with protecting their information assets from unauthorized disclosure, modification, or loss

- How does the State do it?
  - New Jersey State Government departments and agencies act as the custodians of extensive information holdings and rely upon information systems for fiscal, policy, and program delivery initiatives. Consequently, security measures must be implemented to guard against unauthorized access to, alteration, disclosure, or destruction of information and information systems, and safeguards must be implemented to offset possible threats.

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Standards and Criteria

- Executive Branch SISM
- NIST 800-53r4
- NIST Cybersecurity Framework
- CIS Top 20
- PCI-DSS
- HIPPA
- FISMA
- FISCAM

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Ethical Hacking at the OSA

- What is “ethical” hacking?
- How do we do it?
- How is it different?
- Performance Audits of Information Security

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

OSA Ethical Hacking Process

Prior to the Engagement Letter (shhh!)

1. Initial Planning
   - Factors to consider (laws, regulations)
   - Basic details of the “hack”
2. Reconnaissance
   - “Blind” search for information
   - Social Engineering, surveillance, theft

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

OSA Ethical Hacking Process

After the Engagement Letter

1. Audit Planning
   - Gain an understanding from the auditee
   - Document controls in place
   - Enumeration of IT environment
2. Vulnerability Identification
   - Automated scanning tools
   - General Controls testing
3. “Exploitation”
4. Reporting

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Major Finding Areas

- Patch Management
- Insecure Configuration
- Poor Coding Practices
- Logical Access Controls
- People?

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Reporting the Results

Prioritized and Categorized Results

Public Report

Confidential Management Letter

Auditee Response

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

The Future

Expand into social engineering tests

Smaller scopes covering more agencies

Continuous audit process

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR

Questions

"I would rather have questions that can't be answered, than answers that cannot be questioned." – Richard Feynman

Dan Altobelli
daltobelli@njleg.org
609-847-3470
www.njleg.state.nj.us/legislativepub/auditreports.asp

New Jersey Legislature
Office of LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR