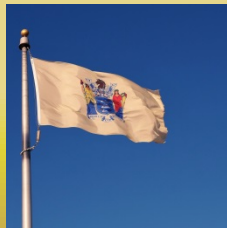
Reporting of Confidential/Sensitive Information

Insert cool (but professional) logo here

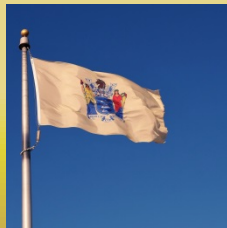
Dan Altobelli
Principal Auditor
New Jersey Office of the State Auditor
January 31, 2019



Background

Information Technology Audit Unit:

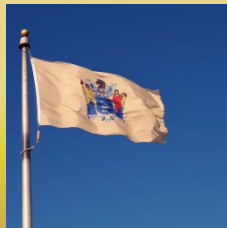
- Founded in 1998 by Frank Bowker and co.
- First audit report was on state's readiness for Y2K
- Provides data retrieval and support for audits
- 1 manager (currently vacant) (fingers crossed!)
- 6 Audit Staff
- 2 Data Retrieval Staff



Background

IT is everywhere:

- IT-specific audits
  - Application and general controls, vulnerability assessments, IT security reviews, project management, governance
- Financial Audit (CAFR)
  - Audit of controls over the New Jersey Comprehensive Financial System
- Integrated Audit
  - Started training in 2009 for financial and performance staff on how to address business process and general controls



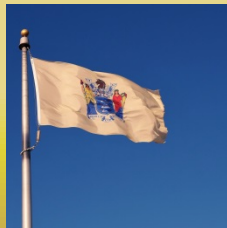
Statutory Information

52:24-6 Reports to the Legislature and Governor

- Report in writing the findings of any audit

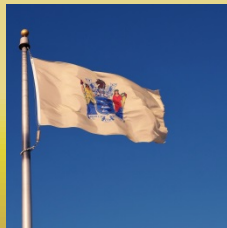
52:24-4 Duties, responsibilities of the State Auditor

- …provide the State Auditor with prompt access to all records necessary for the State Auditor to perform the duties of the State Auditor , notwithstanding any statutory or regulatory requirements of confidentiality with regard to the records , for the purpose of carrying out the provisions of this chapter. The State Auditor shall not disclose a confidential record provided by an accounting agency, or authority, entity, or grantee, except as may be necessary for the State Auditor to fulfill any constitutional or statutory responsibilities. Working papers prepared by the State Auditor shall be confidential and shall not be considered government records under P.L.1963, c.73 (C.47:1A-1 et seq.).



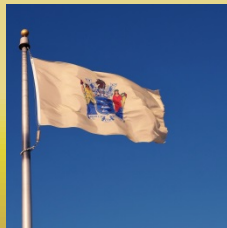
Reporting of Confidential/Sensitive Information

The story of the little audit report that just couldn't see the light of day…



Reporting of Confidential/Sensitive Information

- Public Reports and Management Letters
  - Items Reported Under Separate Cover
  - Confidential Management Letter with Issues
  - Distribution of these Items
  - Availability to the Legislature
  - Importance of Confidentiality
  - Assessing Compliance
  - Issues and Areas for Improvement



Reporting of Confidential/Sensitive Information

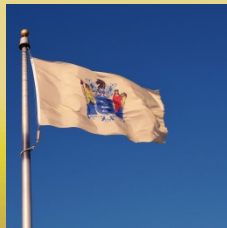
- Items Reported Under Separate Cover
  - Our audit disclosed reportable conditions deemed confidential in nature. These conditions were communicated in a confidential management letter provided to agency management only. The findings and recommendations contained in the management letter are subject to the Office of the State Auditor's compliance process as required by N.J.S.A. 52:24-4.

Reporting of Confidential/Sensitive Information

- Confidential Management Letter with Issues
  - Even in the confidential management letter, we typically do not provide detail to the host/user level
  - X of Y user accounts tested did not have a password meeting the state's complexity requirements
  - X of Y servers tested were missing critical operating system patches that leave them vulnerable to compromise.
  - Detailed testing results given to audit liaison during the engagement.

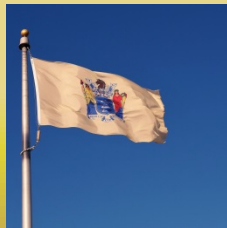
Reporting of Confidential/Sensitive Information

- Distribution of these Items
  - Public report to Legislature and public
  - Management Letter to agency commissioner only
    - They can distribute as necessary internally, but it's on them
- Availability to the Legislature
  - Request a personal briefing with the State Auditor
    - Would still only cover results and root causes in the management letter – no technical specifics
    - Legislators have never requested a briefing for this reason



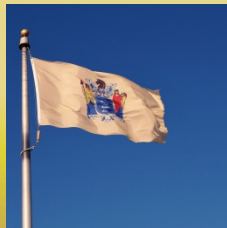
Reporting of Confidential/Sensitive Information

- Importance of Confidentiality
  - Yellow Book to exercise discretion when choosing to withhold information from the public
  - Stressed throughout the audit process with the auditee
    - Discussion of report and management letter at entrance
    - Distinction between where findings are going at informal exit
      - » Auditee opportunity to discuss
    - Provide only numbered paper copies of report and management letter before the formal exit, which are collected at the end of the meeting.
    - Final management letter provided only in paper format.



Reporting of Confidential/Sensitive Information

- Assessing Compliance
  - Statute says that compliance is on report items
    - Items reported under separate cover
  - Challenge of reporting compliance on confidential items
    - Working on a way to show that compliance work has been done without giving out any information on the original issues
  - Compliance report is not public, so that is not an issue.



Reporting of Confidential/Sensitive Information

- Issues and Areas for Improvement
  - Aforementioned compliance assessment
  - Integrated audit findings
  - Getting the issues in the hands of the Legislature
    - No committee that deals with Information Technology
  - Hearings are all public and recorded
    - Would have to do a confidential session
  - Educating the members of this committee
    - Don't "politicize" and expose
    - What happens if you are the source of a leak?