Mr. Chair and members of the Committee!

I'm here to present an overview of the IT Security Audit work our office does.

I will briefly summarize what we have done in the past, and then outline the changes we've made to describe the current process we are following. I will conclude with a few new things we are incorporating as we are starting our audits for 2015.

Our division has done IT security audits since September 2000 and the process has evolved over that time. In the early years, our audits were carried out by one staff person, and more targeted in nature. For example, a 2003 audit focused on certain aspects of an agency's security posture, such as password or anti-virus controls and the agency's disaster recovery planning efforts. In 2005, the team grew a bit. The two auditors reviewed how well agencies adhered to best practices in access controls as well as data and general controls, in addition to other areas such as incident response and physical security.

By June of 2010, our office had lost our main IT auditor, as well as the Post Auditor and other managers to retirement. In an effort to revitalize the IT audit function, the new Post Auditor received direction from the Post Audit Committee to run IT security audits based on a 3-year compliance/control audit cycle. Once the team was assembled, staff audited up to 10 agencies in each of calendar years 2011, 2012, and 2013. These audits covered more aspects of IT security, ranging from password control, to IT security awareness training and reviews of agency's computer inventory. The December 2013 report brought the 3-year compliance and control audit cycle to a close.

As part of the CURRENT triennial plan (2014-2016), we started out with an audit on statewide information about the types, volume and variety of sensitive data that agencies maintain. We are using information from that audit, as well as other information, to apply a risk-based process in selecting agencies to be audited during this 2014-2016 audit cycle.

Attachment 2
JCIT 2-18-15

I'd like to cover how our work has CHANGED. These changes were made partly based on feedback from the audited agencies, and partly because our audit function and personnel has grown in sophistication:

- **We have streamlined our IT security audit work to cover more ground**. Whereas before we concentrated our work on select IT security areas, we now audit all major IT security areas. At each agency, we evaluate roughly 100 different items, most of which are based on policies promulgated through the Information Technology Executive Council. Additionally we evaluate agency's adherence to a handful of best practices we think are important, but are not part of the statewide ITEC requirements. We evaluate many of these requirements at the agency-wide level. Additionally, we also evaluate specific IT security controls for ONE of the agency's system applications that hold sensitive information. By changing our internal review processes and work products, we are able to do more work in less time.

- **We have curtailed the writing and reporting process.** Because our audit reports are confidential and limited in distribution, we decided to spend less time in editing the report. This results in a much more technical report, and saves considerable effort while accomplishing the same goal, which is for the agency to know and remediate its IT security weaknesses.

- **We divided our work at the agency into distinct phases.** This helps create structure and explains expectations. Here's a general run-down of these phases:
    1. *Self-assessment Phase*: In this first phase, the agency completes a self-assessment to document whether THEY believe they are in compliance with the requirements and best practices we are testing. Agencies generally have 2-3 weeks to fill out the survey. It also allows them to clearly understand the items we are measuring. As part of the survey, we indicate whether the items are an ITEC requirement or an LPA selected

best practice. As I mentioned before, most of them are based directly on ITEC policies.

2. *Interview Phase:* This interview, typically conducted with the agency's IT staff, helps us learn about the agency's IT function.
3. *Onsite work:* In this third and most important phase, we are at the agency (generally for 5 days). We generally review policies and procedures, training files for employees, and review computer settings. We also look at other documentation such as COOP plans, risk assessments, or website vulnerability scans the agency has available. Based on that work, we determine whether the agency is in compliance with ITEC requirements and best practices. During this phase, we also run a scan of the agency's workstations and select servers. The scan tells us whether the agency has adequately patched those machines to prevent known vulnerabilities.
4. *Evaluation and Synthesis:* After our week-long onsite visit, we document, discuss and synthesize the findings internally. For each finding, we determine what level of severity we think the problem presents, generally based on impact and likelihood. A critical risk finding is a vulnerability that creates an imminent threat for data loss. On the other side of the spectrum, technical findings are weaknesses in the agency's documentation or security process that are unlikely to lead to present or future vulnerabilities.
5. *Finalization of Audit*: During this phase, we hold an exit conference with the agency, produce a draft report and request feedback from the agency. Lastly, the final report, including the agency's action plans and official response is presented to the Legislative Post Audit Committee in an executive session.

We have conducted 7 agency audits in 2014, and plan to conduct 12 audits in 2015. The general process I'm describing hasn't changed from 2014 to 2015.

However, the ITEC standards **were revised** in November 2014. Consequently, we reviewed and created a new list of requirements we wanted to audit against, based on these new standards. As before, we have added a few best practices. Again, we ended up with roughly 100 items to audit, across 15 IT security areas. In our new list of items we decided to audit, we identified just a few of them that are truly new (they were not present in the previous ITEC version). Because agencies have until July 2016 to come into full compliance, failing those requirements will not carry the same weight as failing requirements that have existed previously.

During 2015, we will also offer social engineering testing to agencies under audit. Social engineering tests more closely mimic the types of breach attempts that agency staff might actually encounter, and thus provide agencies with a more realistic picture of their vulnerabilities, with no additional cost to them. This is the only optional component of our work. Social engineering tests can include looking in trash bins for sensitive information, calling staff to see if they'd give up confidential information such as their password, or e-mailing to see if staff would click on unfamiliar links that – if sent by a real hacker – could contain malicious code.

That's a summary of where we've been and where we hope to go. And with that, I will stand for any questions you may have.