HOUSE COMMITTEE ON

INFORMATION MANAGEMENT AND TECHNOLOGY

March 1, 2005 Hearing Room 357

1:00 P.M. Tape 20 - 22

MEMBERS PRESENT: **Rep. John Dallum, Chair**

Rep. Jerry Krummel, Vice-Chair

Rep. Brad Witt

MEMBERS EXCUSED: **Rep. Kelley Wirth, Vice-Chair**

Rep. Chuck Burley

STAFF PRESENT: **Dallas Weyand, Committee Administrator**

Louann Rahmig, Committee Assistant

MEASURES/ISSUES HEARD:

Information Technology Security and Audits – Informational Meeting

These minutes are in compliance with Senate and House Rules. Only text enclosed in quotation marks reports a speaker's exact words. For complete contents, please refer to the tapes.

TAPE/#	Speaker	Comments

TAPE 20, A

004	Chair Dallum	Calls the meeting to order at 1:00 p.m. Announces that presentations will be limited to 20 minutes each. Opens an informational meeting on information technology security and audits.

INFORMATION TECHNOLOGY SECURITY AND AUDITS – INFORMATIONAL MEETING

017	Chuck Hibner	Deputy, Secretary of State Audits Division. Presents overview of the division's responsibilities, which include information technology (IT), financial and performance audits.
045	Hibner	Explains that staff are obtaining certified information systems audit certifications. Describes the division's annual audit plan, from which projects are selected based on risk analyses.
068	Hibner	Advises that audit findings are publicly released with recommendations, except when the information would put the system at risk.
080	Neal Weatherspoon	Oregon Secretary of State Audits Division. Provides more detail on the IT audit process.
111	Weatherspoon	Points out that the standards have changed for the way business is conducted by auditors.
125	Weatherspoon	Informs that the division performs reviews of systems with statewide implications, such as the payroll system, public employees' retirement system and data archives center. Indicates that increasing public access poses great risk.
132	Weatherspoon	Advises that the division classifies itself as an external auditor independent from the agencies audited and describes the standards used for financial and performance audits.
178	Weatherspoon	Continues by expressing concerns with controls associated with day to day integrity and the cost of system development.
208	Weatherspoon	Comments on disaster recovery and contingency planning. Advises that the division has performed IT audits on several state agencies and the university system. Invites members to review the division's web site for audit reports.

254	Linda Haglund	Deputy State Treasurer. Provides overview of the office's responsibilities, all of which are IT dependent. Gives statistics on annual transactions. Advises that Treasury keeps track of all the state, local government, municipality, county and school district debt in an overlapping debt program.
297	Haglund	Continues by describing the investment holdings that are tracked.
320	Haglund	Describes agency security. Explains that internal audit staff does an annual risk assessment, and IT staff are dedicated to watching the network fulltime to identify attempts to access their system.
345	Haglund	Continues with information on their network, which has a strong perimeter to prevent outsiders from accessing the system. Refers to a recent state-driven penetration test and the fact that the firewall held up to the attack attempt.
370	Haglund	Believes that the best testing is done by a third party to avoid manipulation by internal staff or collusion with other agencies.
420	Haglund	Describes a recent penetration test and review of physical security by a third-party from the Department of Administrative Services (DAS) approved list of vendors.

TAPE 21, A

048	Haglund	Continues with explanation of test which looked at the physical location of systems, access controls and practices of sensitive information. Stresses the importance of using a highly qualified vendor that would not cause system failure during testing.
058	Haglund	Closes with comments that at Treasury security over financial transactions and information is critical.
067	Rep. Krummel	Asks about the handling of local and state government outstanding debt.
073	Haglund	Replies that Treasury does not handle payment of local government debt but tracks overlapping debt issuances. Explains that they manage all of the state's debt from centralized issuance and contracts for the fiscal agent, the mechanism by which bond coupon payments are paid.

083	Rep. Krummel	Inquires at what level the state-sponsored attack was stopped.
089	Haglund	Responds that the attack did not penetrate the initial firewall.
094	Rep. Krummel	Asks about the provisions for systems being patched to continue a high level of security.
105	Haglund	Answers that there are two internal audit staff plus one fulltime network monitor. Explains further that the individual who monitors the network is responsible for staying current on all releases, and an automated system has been implemented for installation of patches.
128	Rep. Krummel	Asks if Treasury is consolidating into the data center, and if so, would some of the security issues be resolved.
133	Haglund	Replies that Treasury is not part of the initial consolidation and does not know if there are any unique aspects of Treasury's functions that would need to be addressed.
142	Chair Dallum	Inquires how often a new third party vendor would be sought.
150	Haglund	Responds, every time if adequate skill sets were available.
153	Chair Dallum	Asks if Treasury would put out for bid.
157	Haglund	Answers, that is correct.
158	Chair Dallum	Inquires if the outside evaluation is completely independent of any other state agency.
159	Haglund	Responds, that is correct.
160	Chair Dallum	Inquires if there is an advantage to using an outside agency.
161	Haglund	Answers that Treasury's objective is to have a robust test and to use the most experienced resources to perform it.
171	Chair Dallum	Asks if the Secretary of State audits Treasury.

172	Haglund	Replies, yes.
174	Chair Dallum	Seeks clarification that Treasury uses an internal ongoing audit, a Secretary of State audit and an outside audit, which provides three different looks at the office.
179	Haglund	Answers, yes.
190	Theresa Masse	Head of Cyber Security, DAS. Refers to written information titled *Protecting Confidential State Information Assets* **(EXHIBIT A)**. Describes how security has been handled in the past, which was very agency-centric **(EXHIBIT A, Page 1)**. Explains that DAS had a vulnerability assessment in 2004.
224	Masse	Continues that a decentralized approach lacks an objective assessment of risk exposure and does not allow adequate priority and resource allocation **(EXHIBIT A, Page 2)**.
239	Masse	Refers to the current model **(EXHIBIT A, Page 3)**. Advises that the vulnerability assessment has created a sense of urgency. Explains the Immediate Action Plan (IAP).
258	Masse	Advises that agency directors are involved with several committees to implement the IAP.
276	Masse	Continues by explaining the enterprise security planning process **(EXHIBIT A, Page 4)**.
289	Masse	Outlines the hybrid model for the future **(EXHIBIT A, Page 5)**.
309	Masse	Discusses coordination of security programs with federal and local governments and business partners to maximize efficiency.
319	Masse	Provides examples of coordination **(EXHIBIT A, Page 6)**.
337	Masse	Refers to the future model **(EXHIBIT A, Page 7)**. Points out that coordination with Homeland Security and the Oregon State Police is necessary.
348	Don Fleming	State Chief Information Officer, DAS. Discusses immediate areas of concern **(EXHIBIT A, Page 8)**. States the implementation of the

		Computing and Networking Infrastructure Consolidation (CNIC) project will decrease the "weakest link" issue, which is the decentralized agency approach to security. Believes statutory authority, administrative rules and changes to the business model will be required to ensure a secure infrastructure.
371	Fleming	Continues with information on areas of assessment and monitoring **(EXHIBIT A, Page 9)**.
409	Fleming	Expresses that multiple vulnerability assessments are not cost-effective and can be potentially harmful.
427	Fleming	Explains that the suggested approach is to utilize highly competent third-party vendors, who are most current on attack scenarios and vulnerabilities, to perform assessments on a centralized basis.

TAPE 20, B

007	Fleming	Continues that dissemination of information would be on a "need to know" basis. Cites an example of an "attack" on a research laboratory and subsequent vulnerability assessment.
034	Fleming	Discusses incident response **(EXHIBIT A, Page 10)**. Believes a team of highly trained experts must be created that will have extraordinary authorities to respond to an attack. Outlines the types of authorities needed to be effective.
077	Fleming	Continues with audit issue remediation **(EXHIBIT A, Page 11)**. Discusses agency responses to audit report findings. Suggests making remediation plans mandatory, including follow-up to see that the plan was implemented and effective in eliminating the findings.
109	Fleming	Refers to house rules **(EXHIBIT A, Page 12)**. States that through a collaborative effort, rules must be established and followed. Cites some examples.
143	Fleming	Concludes that the existing problems are self inflicted and must be managed more effectively. Expresses concern about uncoordinated, multiple organizations conducting vulnerability assessments, as they can be dangerous and disruptive.
177	Greg Hutchins	Quality Plus Engineering. Describes his company, which does risk management assessments for federal and private clients. Begins a

		PowerPoint presentation titled *Oregon Cyber Security* and provides a hard copy **(EXHIBIT B)**.
202	Hutchins	Points out the differences between east and west coast mind sets, and that the federal government believes cyber security is a homeland security issue.
245	Hutchins	Discusses hacking.
257	Hutchins	Quotes from *CIO Magazine* **(EXHIBIT B, Page 3)**.
275	Hutchins	Continues by discussing what is at stake for Oregon and dissemination of unwanted information **(EXHIBIT B, Page 4)**.
302	Hutchins	Points out that the threshold of "due care" has changed between pre-9/11 and post-9/11.
337	Hutchins	Defines "due care" **(EXHIBIT B, Page 5)**.
374	Hutchins	Cites credentials needed to meet higher standard of "due care."

TAPE 21, B

010	Hutchins	Outlines professional proficiency of accountants and engineers **(EXHIBIT B, Page 6)**.
022	Hutchins	Discusses Certified Information Systems Auditor requirements **(EXHIBIT B, Page 7)**.
033	Hutchins	Defines half life of knowledge.
047	Hutchins	Summarizes what Oregon should do.
075	Chair Dallum	Asks if Quality Plus Engineering is on the state-approved vendor list.
076	Hutchins	Replies, yes.
78	Chair Dallum	Inquires if the company has done any audits for the state on IT security.

079	Hutchins	Responds, no, but has done an eco-evaluation assessment.
082	Rep. Witt	Asks how we can expect to keep up.
089	Hutchins	Believes it is important to move from a collaborative environment to a control system environment, as it is necessary for someone to be accountable.
103	Rep. Witt	Agrees that there is the appearance of great need for a security system to run security for the state.
108	Hutchins	States that the way business is done will change in the next five years.
114	Rep. Witt	Asks if internal security systems need to be parallel systems, similar to the type used in a casino.
11 8	Hutchins	Responds that there needs to be redundancies.
126	Chair Dallum	Summarizes testimony from DAS and Treasury regarding authority to shut down systems, seize, isolate and inoculate, using a combination of internal staff and a third party. Asks if that is the type of redundancy needed.
139	Hutchins	Responds that operational controls are needed, not auditing controls.
144	Chair Dallum	Restates Treasury's process which provides internal daily monitoring, the Secretary of State's level of security and a periodic third-party assessment. Asks if that system is redundant enough.
162	Hutchins	Responds, should be.
165	Rep. Krummel	Asks if Quality Plus Engineering has a Certified Information System Security Professional (CISSP) employee.
167	Hutchins	Answers, no.
171	Rep. Krummel	Believes that a CISSP has the level of understanding of information security that is important. States that it is not uncommon for an engineer to have CISSP credentials.

185	Rep. Witt	Asks for a description of the management controls needed to be engineered into the security system that may not now be there.
192	Hutchins	Replies culture of controls and culture of due diligence. Indicates there is no sense of accountability, which is the toughest challenge in any type of security.
207	Rep. Krummel	Asks if the Secretary of State Audits Division staff who perform information systems audits have CISSP credentials.
220	Hibner	Responds that Mr. Weatherspoon does and the division is developing those credentials.
240	Rep. Krummel	Asks Mr. Weatherspoon if he has an engineering degree as well as the CISSP.
244	Weatherspoon	Replies, no, and cites credentials, training and background experience.
279	Weatherspoon	Continues that no one at the Audits Division has engineering knowledge and contract for it if needed.
288	Rep. Krummel	Inquires if an engineer with software background and a security systems professional certification would be included in an agency security system or cyber security system audit.
310	Weatherspoon	Responds that the level of expertise needed would be in proportion to the level of audit so may need to contract out.
340	Rep. Krummel	Seeks clarification that consultation with agencies to be audited takes place to determine whether a third party is needed to assist with an audit.
359	Weatherspoon	Answers, yes; security is a team effort.
392	Chair Dallum	Summarizes the various agency processes and asks if the Audits Division uses an outside agency to look at its IT.
431	Hibner	Replies that IT could better answer that question.

433	Chair Dallum	Summarizes processes and asks about suitable proposed legislation.
440	Hibner	Seeks clarification.

TAPE 22, A

010	Chair Dallum	Describes a four-level plan to insure the state's IT security. Asks if the plan sounds reasonable.
027	Weatherspoon	Responds that a multi-layered approach is necessary. Believes every organization needs a security officer to keep vigilant watch for vulnerabilities and threats.
050	Chair Dallum	Asks if they concur.
051	Weatherspoon	Replies, believe we do.
061	Chair Dallum	States that it appears a state agency needs the authority to "pull the plug."
070	Weatherspoon	Comments on the generally accepted controls for security.
076	Chair Dallum	Summarizes the planned procedures for security.

The following material is submitted for the record without public testimony:

	Dallas Weyand	Secretary of State Audits Division agency protocol **(EXHIBIT C)**.
080	Chair Dallum	Closes the informational meeting on information technology security and audits and adjourns at 2:58 p.m.

EXHIBIT SUMMARY

A. **Protecting Confidential State Information Assets, information packet, Theresa Masse, 12 pp**
B. **Oregon Cyber Security, PowerPoint presentation, Greg Hutchins, 10 pp**

The following material is submitted for the record without public testimony:

C. **Secretary of State Audits Division agency protocol, written information, staff, 12 pp**