SB 90 STAFF MEASURE SUMMARY

Joint Committee On Information Management and Technology

Prepared By:	Sean McSpaden, Committee Coordinator
Sub-Referral To:	Joint Committee On Ways and Means
Meeting Dates:	3/30, 4/6, 5/4

WHAT THE MEASURE DOES:

Requires state agencies and State Chief Information Officer (SCIO) to cooperatively develop plan to consolidate information technology security functions with SCIO, including transfer of personnel, records and property. Directs state agencies to retain unexpended funds designated for administration of functions being transferred. Requires state agencies to cooperate with security assessment and remediation program; follow unification instructions; conduct and document completion of specified training; report information and participate in activities as directed by SCIO. Authorizes SCIO to determine costs and collect payment from state agencies for information technology services for deposit into State Information Technology Operation Fund.

Authorizes SCIO to enter into agreements and accept and deposit funds into State Information Technology Operation Fund as specified. Directs SCIO to develop plan for establishment of a Cyber Security Center of Excellence, describes required content within plan, and directs SCIO to submit plan to Legislative Assembly by January 1, 2018.

ISSUES DISCUSSED:

- Merits of consolidation
- Exempting statewide elected offices from consolidation
- Possibility of discrete entities under one security umbrella
- Value of common security architecture
- Impetus for measure: Executive Order 16-13
- Recent security breaches, danger of breach generally
- Possibility of forming work group
- Merits of Cyber Security Center of Excellence
- Concerns/questions regarding proper placement of Cyber Security Center of Excellence - within state government or in the private sector
- Convening power of Governor and State CIO to bring stakeholders together on cyber security issues affecting government at all levels and the private sector in Oregon
- Available and needed educational/degree programs for cybersecurity in Oregon
- Commitments - financial and in-kind - to the Cyber Security Center of Excellence from interested stakeholders and potential partner organizations
- Scarce cybersecurity work force
- Cybersecurity trends across the nation
- Fiscal impacts of the measure

EFFECT OF AMENDMENT:

The amendment to the measure:

- Prescribes January 1, 2018 as date by which SCIO shall develop plan to transfer agency information technology security functions, records and property to office of SCIO.
- Prescribes January 1, 2018 as operative date for Section 2 of Act.
- Removes language regarding establishment of a Cybersecurity Center of Excellence and Cybersecurity Fund.

- Establishes Oregon Cyber Security Advisory Council within office of SCIO and specifies membership and purposes of council. The council is to be comprised of voting members representing cyber-related industries, post-secondary institutions of education and public law enforcement agencies in Oregon, and will also include a diverse group of non-voting members.
- Includes term of office language (staggering terms) for voting council members.
- Directs SCIO to develop a plan for establishment of an Oregon Cybersecurity Center of Excellence, describes required content within plan, and directs SCIO to submit plan to Legislative Assembly by January 1, 2018.
- Modifies language regarding SCIO's authority to enter into agreements related to state cybersecurity.
- Modifies language regarding SCIO's authority to accept moneys from federal government and other sources related to state cybersecurity.
- Directs SCIO to deposit moneys related to provisions of Act into State Information Technology Operating fund established under ORS 291.041.
- Makes minor modifications to language related to ORS 291.041.
- Prescribes an effective date for measure - 91 days following sine die of this 2017 legislative session.

BACKGROUND:

Senate Bill 90-A stems from Executive Order 16-13, which was implemented in response to recent information technology (IT) security breaches and other vulnerabilities among state executive branch entities. The state's IT security functions are currently the responsibility of each independent agency, an approach that is criticized for creating an environment where one agency can be put at risk because of deficiencies at another. The measure directs the consolidation of IT security functions with the State Chief Information Officer according to timelines established within a plan the measure directs the State Chief Information Officer to develop.

Oregon also lacks a mechanism to exchange cybersecurity information across political subdivisions, and with the private sector and other partners in an organized and useful way. Senate Bill 90-A, among other things, sought to create an Oregon Cybersecurity Center of Excellence (Center) within the office of the State Chief Information Officer to centralize cybersecurity information sharing between public and private sectors; serve as “Information Sharing and Analysis Organization” for purposes of federal critical infrastructure protection programs; act as liaison with Department of Homeland Security and other entities concerning cybersecurity; and promote development of cybersecurity workforce. The amendment to the measure instead directs the State Chief Information Officer to develop a plan for establishment of the Center, describes required content within plan, and directs the State Chief Information Officer to submit the plan to Legislative Assembly by January 1, 2018. Upon review of the plan during the 2018 Legislative Session, the Legislature can then determine whether and, if so, in what timeframe to authorize the establishment of the Center.