House Bill 2268

Introduced and printed pursuant to House Rule 12.00. Presession filed (at the request of Governor Kate Brown for Oregon Department of Administrative Services)

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure **as introduced.**

Permits Adjutant General, with approval of Governor, to order members of organized militia to state active duty for purpose of supporting State Chief Information Officer in conduct of vulnerability assessments of state agency information systems or related activities.

A BILL FOR AN ACT

Relating to security of information systems; amending ORS 276A.300 and 399.075.

Be It Enacted by the People of the State of Oregon:

SECTION 1. ORS 399.075 is amended to read:

399.075. (1)**(a)** The Adjutant General, with the approval of the Governor, may order members of the organized militia to state active duty as defined in the Oregon Code of Military Justice. Members, while on state active duty, shall receive not less than the pay and allowances of their corresponding grades in the Armed Forces of the United States in accordance with a schedule approved by the Adjutant General for the period of time in state active duty.

(b) State active duty under this subsection [*includes*] **may be ordered for a purpose that includes**, but is not limited to[*, support of*]**:**

(A) Supporting federal, state and local drug eradication, interdiction and other counterdrug operations under a counterdrug support plan approved by the Governor, and reasons related to homeland security. When participating in such support operations, and to the extent authorized by 32 U.S.C. 112, applicable regulations of the National Guard Bureau and the Oregon Counterdrug Support Plan, the Oregon Military Department is designated as a law enforcement agency for the purpose of carrying out federal asset forfeiture laws only.

(B) Supporting the State Chief Information Officer in the conduct of vulnerability assessments of state agency information systems or related activities under ORS 276A.300.

(2) Members of the organized militia serving on courts-martial, courts of inquiry, efficiency boards, medical boards or other special duty requiring absence from their stations or business under competent orders may be reimbursed for necessary expenses incurred at the rate established for state employees under appropriate travel regulations issued by the Oregon Department of Administrative Services.

(3) In lieu of other provisions of this chapter, a medical examiner may be paid for services and necessary disbursements and a properly appointed judge advocate may be paid for legal services and necessary disbursements in any suit, action or proceeding, such amounts as shall be approved by the Governor.

(4) Members of the organized militia shall not receive from the state the pay or the pay and allowances provided for by this section when eligible for such pay and allowances from federal

NOTE: Matter in **boldfaced** type in an amended section is new; matter [*italic and bracketed*] is existing law to be omitted. New sections are in **boldfaced** type.

funds.

(5) Notwithstanding any of the provisions of this chapter, members of the organized militia may with their consent perform without pay or without pay and allowances any of the types of military duty prescribed in this chapter and ORS chapters 396 and 398 pursuant to orders issued by competent military authority; provided however, that necessary traveling expenses, subsistence and per diem allowances may be furnished such members within the discretion of the Adjutant General and within the amount appropriated therefor.

(6) All pay and allowances provided for by this chapter, except per diem, mileage and expenses while traveling under orders shall be subject to be applied to the payment of penalties and fines imposed by military courts, and to the payment of any shortage of or injury to state or United States property or funds for which a member of the organized militia is responsible or accountable where such responsibility has been fixed by competent authority.

(7)(a) Except as provided in paragraph (b) of this subsection, members of the organized militia who are ordered to state active duty shall be considered temporary employees of the military department.

(b) Members of the organized militia who are ordered to state active duty are not subject to ORS chapter 240 and ORS 243.650 to 243.809.

(8) The limitations on employment imposed by ORS 238.082 (2) and (3) do not apply to a retired member of the Public Employees Retirement System who has attained normal retirement age and is on state active duty. Hours served by a person under this subsection shall not be counted for the purpose of the limitations on employment imposed by ORS 238.082 (2) and (3).

SECTION 2. ORS 276A.300 is amended to read:

276A.300. (1) As used in this section:

(a) "Executive department" has the meaning given that term in ORS 174.112.

(b) "Information systems" means computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.

(2) The State Chief Information Officer has responsibility for and authority over information systems security in the executive department, including responsibility for taking all measures that are reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. The State Chief Information Officer shall, after consultation and collaborative development with agencies, establish a state information systems security plan and associated standards, policies and procedures. The plan must align with and support the Enterprise Information Resources Management Strategy described in ORS 276A.203.

(3) The State Chief Information Officer may coordinate with the Oregon Department of Administrative Services to:

(a) Review and verify the security of information systems operated by or on behalf of state agencies;

(b) Monitor state network traffic to identify and react to security threats; and

(c) Conduct**, or require to be conducted,** vulnerability assessments of state agency information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems.

[*(4) The State Chief Information Officer shall contract with qualified, independent consultants for*

the purpose of conducting vulnerability assessments under subsection (3) of this section.]

[*(5)*] **(4)** In collaboration with appropriate agencies, the State Chief Information Officer shall develop and implement policies for responding to events that damage or threaten the availability, integrity or confidentiality of information systems or the information stored in information systems, whether those systems are within, interoperable with or outside the state's shared computing and network infrastructure. In the policies, the State Chief Information Officer shall prescribe actions reasonably necessary to:

(a) Promptly assemble and deploy in a coordinated manner the expertise, tools and methodologies required to prevent or mitigate the damage caused or threatened by an event;

(b) Promptly alert other persons of the event and of the actions reasonably necessary to prevent or mitigate the damage caused or threatened by the event;

(c) Implement forensic techniques and controls developed under subsection [*(6)*] **(5)** of this section;

(d) Evaluate the event for the purpose of possible improvements to the security of information systems; and

(e) Communicate and share information with appropriate agencies, using preexisting incident response capabilities.

[*(6)*] **(5)** After consultation and collaborative development with appropriate agencies and the Oregon Department of Administrative Services, the State Chief Information Officer shall implement forensic techniques and controls for the security of information systems, whether those systems are within, interoperable with or outside the state's shared computing and network infrastructure. The techniques and controls must include using specialized expertise, tools and methodologies to investigate events that damage or threaten the availability, integrity or confidentiality of information systems or the information stored in information systems. The State Chief Information Officer shall consult with the Oregon State Police, the Oregon Department of Emergency Management, the Governor and others as necessary in developing forensic techniques and controls under this section.

[*(7)*] **(6)** The State Chief Information Officer shall ensure that reasonably appropriate remedial actions are undertaken when the State Chief Information Officer finds that such actions are reasonably necessary by reason of vulnerability assessments of information systems under subsection (3) of this section, evaluation of events under subsection [*(5)*] **(4)** of this section and other evaluations and audits.

[*(8)(a)*] **(7)(a)** State agencies are responsible for securing computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information outside the state's shared computing and network infrastructure, following information security standards, policies and procedures established by the State Chief Information Officer and developed collaboratively with the agencies. Agencies may establish plans, standards and measures that are more stringent than the standards established by the State Chief Information Officer to address specific agency needs if the plans, standards and measures do not contradict or contravene the state information systems security plan. Independent agency security plans must be developed within the framework of the state information systems security plan.

(b) A state agency shall report the results of any vulnerability assessment, evaluation or audit conducted by the agency to the State Chief Information Officer for the purposes of consolidating statewide security reporting and, when appropriate, to prompt a state incident response.

[*(9)*] **(8)** This section does not apply to:

(a) Research and student computer systems used by or in conjunction with any public university

listed in ORS 352.002; and

(b)(A) Gaming systems and networks operated by the Oregon State Lottery or contractors of the State Lottery; or

(B) The results of Oregon State Lottery reviews, evaluations and vulnerability assessments of computer systems outside the state's shared computing and network infrastructure.

[*(10)*] **(9)** The State Chief Information Officer shall adopt rules to implement the provisions of this section.
