ALEC EXPOSED

"ALEC" has long been a secretive collaboration between Big Business and "conservative" politicians. Behind closed doors, they ghostwrite "model" bills to be introduced in state capitols across the country. This agenda–underwritten by global corporations–includes major tax loopholes for big industries and the super rich, proposals to offshore U.S. jobs and gut minimum wage, and efforts to weaken public health, safety, and environmental protections. Although many of these bills have become law, until now, their origin has been largely unknown. With **ALEC EXPOSED**, the Center for Media and Democracy hopes more Americans will study the bills to understand the depth and breadth of how big corporations are changing the legal rules and undermining democracy across the nation.

ALEC's Corporate Board --in recent past or present

- AT&T Services, Inc.
- centerpoint360
- UPS
- Bayer Corporation
- GlaxoSmithKline
- Energy Future Holdings
- Johnson & Johnson
- Coca-Cola Company
- PhRMA
- Kraft Foods, Inc.
- Coca-Cola Co.
- Pfizer Inc.
- Reed Elsevier, Inc.
- DIAGEO
- Peabody Energy
- Intuit, Inc.
- Koch Industries, Inc.
- ExxonMobil
- Verizon
- Reynolds American Inc.
- Wal-Mart Stores, Inc.
- Salt River Project
- Altria Client Services, Inc.
- American Bail Coalition
- State Farm Insurance

For more on these corporations, search at www.SourceWatch.org.

DID YOU KNOW? Corporations VOTED to adopt this. Through ALEC, global companies work as "equals" in "unison" with politicians to write laws to govern your life. Big Business has "a VOICE and a VOTE," according to newly exposed documents. **DO YOU?**

Did you know that global telecommunications company AT&T was the corporate co-chair in 2011?

Information Security Management Act

Summary

An act concerning cyber security for communication and information resources in public agencies, and making an appropriation in connection therewith.

Model Legislation

Be it enacted by the General Assembly of the State of _____:

Section 1. Article _____ of title _____, _____ Revised Statutes, is amended BY THE ADDITION OF A NEW PART to read: PART 4 INFORMATION SECURITY

Legislative declaration. (1) THE GENERAL ASSEMBLY HEREBY FINDS, DETERMINES, AND DECLARES THAT:

(a) Communication and information resources in the various public agencies of the state are strategic and vital assets belonging to the people of (State). Coordinated efforts and a sense of urgency are necessary to protect these assets against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as to assure the confidentiality, integrity, and availability of information.

(b) State government has a duty to (State) citizens to ensure that the information entrusted to public agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction.

(c) Securing the state's communication and information resources is a statewide imperative requiring a coordinated and shared effort from all departments, agencies, and political subdivisions of the state and a long term commitment to state funding that ensures the success of such efforts.

(d) Risks to communication and information resources must be managed, and the integrity of data and the source, destination, and processes applied to data must be assured.

(e) Information security standards, policies, and guidelines must be promulgated and implemented throughout public agencies to ensure the development and maintenance of minimum information security controls to protect communication and information resources that support the operations and assets of those agencies.

Section 2. {Definitions} AS USED IN THIS PART 4, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(1) "AVAILABILITY" means the timely and reliable access to and use of information created, generated, collected, or maintained by a public agency.

(2) "COMMUNICATION AND INFORMATION RESOURCES" shall have the same meaning as applied to procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit, information. The term also includes associated personnel including consultants and contractors.

(3) "CONFIDENTIALITY" means the preservation of authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

(4) "INFORMATION SECURITY" means the protection of communication and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to:

(a) Prevent improper information modification or destruction;

(b) Preserved authorized restrictions on information access and disclosure;

(c) Ensure timely and reliable access to and use of information; and

(d) Maintain the confidentiality, integrity, and availability of information.

(6) "INFORMATION SECURITY PLAN" means the plan developed by a public agency in accordance with this statute.

(7) "INSTITUTION OF HIGHER EDUCATION" means a state-supported institution of higher education.

(8) "INTEGRITY" means the prevention of improper information modification or destruction and ensuring information nonrepudiation and authenticity.

(9) "PUBLIC AGENCY" means every state office, whether legislative, executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions.

(10) "SECURITY INCIDENT" means an accidental or deliberative event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources.

Section 3. {Chief information security officer - duties and responsibilities}

(1) The governor shall appoint a chief information security officer who shall serve at the pleasure of the governor. The officer shall exhibit a background and expertise in the security and risk management for communications and information resources. In the event the officer is unavailable to perform the duties and responsibilities under this part 4, all powers and authority granted to the officer may be exercised by the state chief information officer or other person designated by the governor.

(2) THE CHIEF INFORMATION SECURITY OFFICER SHALL:

(a) Develop and assist in the update of information security procedures, standards, and guidelines for all public agencies.

(b) Promulgate rules pursuant to (existing State Statues);

Exposed By the Center for Media and Democracy www.prwatch.org

(c) Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies IN ACCORDANCE WITH THIS STATUTE;

(d) Direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments;

(e) Establish and direct a risk management process to identify information security risks in public agencies and deploy risk mitigation strategies, processes, and procedures;

(f) Annually review and approve the information security plans of public agencies;

(g) Conduct information security awareness and training programs; and

(h) In coordination and consultation with the state budget office and the chief information officer (or corresponding designated officer), review public agency budget requests related to information security systems and make recommendations on such budget requests for state agencies.

Section 4. {Public agencies - information security plans}

(1) On or before each new fiscal year, each public agency shall develop an information security plan utilizing the information security policies, standards, and guidelines developed by the chief information security officer. The information security plan shall provide information security for the communication and information resources that support the operations and assets of the public agency.

(2) THE INFORMATION SECURITY PLAN SHALL INCLUDE:

(a) Periodic assessments of the risk and magnitude of the harm that could result from a security incident;

(b) A process for providing adequate information security for the communication and information resources of the public agency;

(c) Conduct periodic security awareness training to inform the employees and users of the public agency's communication and information resources about information security risks and the responsibility of employees and users to comply with agency policies, standards, and procedures designed to reduce those risks;

(d) Periodic vulnerability assessment testing and evaluation of the effectiveness of information security for the public agency, which shall be performed not less than annually;

(e) A process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines issued by the chief information security officer; and

(f) Plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the public agency in the event of a security incident.

(3) On or before each new fiscal year each public agency shall submit the information security plan developed pursuant to this section to the chief information security officer for approval.

(4) In the even that a public agency fails to submit to the chief information security officer and information security plan on or before the new fiscal year, or such plan is disapproved by the chief information security officer, the officer shall notify the governor and the head and chief information officer of the public agency of noncompliance with

Exposed By the Center for Media and Democracy www.prwatch.org

this section. If no plan has been approved within the three subsequent months, the officer shall be authorized to temporarily discontinue or suspend the operation of a public agency's communication and information resources until such plan has been submitted to or is approved by the officer.

(5) An information security plan may provide for a phase-in period not to exceed three years. An implementation schedule for the phase-in period shall be included in such a plan. Any phase-in period pursuant to this subsection (5) shall be completed by (Current Year plus three (3).

(6) On or before the new fiscal year, and on or before July 1 of each subsequent year, the executive director or head of each public agency shall report to the chief information security officer on the development, implementation, and, if applicable, compliance with the phase-in schedule of the public agency's information security plan.

Section 5. {Reporting} The chief information security officer shall report to the governor and legislature on an annual basis concerning the implementation of the provisions of this plan.

Adopted by the Telecommunications and Information Technology Task Force at the States and Nation Policy Summit on December 9, 2006. Approved by the ALEC Board of Directors January 8, 2007.

About Us and ALEC EXPOSED. The Center for Media and Democracy reports on corporate spin and government propaganda. We are located in Madison, Wisconsin, and publish www.PRWatch.org, www.SourceWatch.org, and now www.ALECexposed.org. For more information contact: editor@prwatch.org or 608-260-9713.