*Session of 2025*

# HOUSE BILL No. 2271

By Committee on Legislative Modernization

Requested by Representative Penn

2-5

AN ACT concerning cybersecurity; removing the expiration provisions of cybersecurity legislation; consolidating cybersecurity services under the chief information security officer of each branch; amending K.S.A. 2024 Supp. 40-110, 75-413, 75-623, 75-710, 75-711, 75-7203, 75-7206a, 75-7208a, 75-7245 and 75-7246 and repealing the existing sections; also repealing K.S.A. 2023 Supp. 45-229, as amended by section 11 of chapter 95 of the 2024 Session Laws of Kansas, 75-7201, as amended by section 17 of chapter 95 of the 2024 Session Laws of Kansas, 75-7202, as amended by section 19 of chapter 95 of the 2024 Session Laws of Kansas, 75-7203, as amended by section 21 of chapter 95 of the 2024 Session Laws of Kansas, 75-7205, as amended by section 23 of chapter 95 of the 2024 Session Laws of Kansas, 75-7206, as amended by section 25 of chapter 95 of the 2024 Session Laws of Kansas, 75-7208, as amended by section 27 of chapter 95 of the 2024 Session Laws of Kansas, 75-7209, as amended by section 29 of chapter 95 of the 2024 Session Laws of Kansas, 75-7237, as amended by section 31 of chapter 95 of the 2024 Session Laws of Kansas, 75-7238, as amended by section 33 of chapter 95 of the 2024 Session Laws of Kansas, 75-7239, as amended by section 35 of chapter 95 of the 2024 Session Laws of Kansas, 75-7240, as amended by section 37 of chapter 95 of the 2024 Session Laws of Kansas.

*Be it enacted by the Legislature of the State of Kansas:*

Section 1. K.S.A. 2024 Supp. 40-110 is hereby amended to read as follows: 40-110. (a) The commissioner of insurance is hereby authorized to appoint an assistant commissioner of insurance, actuaries, two special attorneys who shall have been regularly admitted to practice, an executive secretary, policy examiners, two field representatives, and a secretary to the commissioner. Such appointees shall each receive an annual salary to be determined by the commissioner of insurance, within the limits of available appropriations. The commissioner is also authorized to appoint, within the provisions of the civil service law, and available appropriations, other employees as necessary to administer the provisions of this act. The field representatives authorized by this section may be empowered to conduct inquiries, investigations or to receive complaints. Such field

representatives shall not be empowered to make, or direct to be made, an examination of the affairs and financial condition of any insurance company in the process of organization, or applying for admission or doing business in this state.

(b) The appointees authorized by this section shall take the proper official oath and shall be in no way interested, except as policyholders, in any insurance company. In the absence of the commissioner of insurance the assistant commissioner shall perform the duties of the commissioner of insurance, but shall in all cases execute papers in the name of the commissioner of insurance, as assistant. The commissioner of insurance shall be responsible for all acts of an official nature done and performed by the commissioner's assistant or any person employed in such office. All the appointees authorized by this section shall hold their office at the will and pleasure of the commissioner of insurance.

(c) ~~(1)~~ The commissioner shall appoint a chief information security officer who shall be responsible for establishing security standards and policies to protect the department's information technology systems and infrastructure. The chief information security officer shall:

~~(A)~~*(1)* Develop a cybersecurity program for the department that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief information security officer shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

~~(B)~~*(2)* ensure that the commissioner and all employees complete cybersecurity awareness training annually and that if an employee does not complete the required training, such employee's access to any state-issued hardware or the state network is revoked; and

~~(C) (i) (a)~~*(3) (A) (i)* coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the department for compliance with applicable state and federal laws, rules and regulations and department policies and standards; and

~~(b)~~*(ii)* make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

~~(ii)~~*(B)* Results of audits conducted pursuant to this paragraph shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 2. K.S.A. 2024 Supp. 75-413 is hereby amended to read as follows: 75-413. (a) The secretary of state may appoint such other assistants and clerks as may be authorized by law, but the secretary of state shall be responsible for the proper discharge of the duties of all assistants and clerks, and they shall hold their offices at the will and pleasure of the

secretary and shall do and perform such general duties as the secretary may require.

(b) ~~(1)~~ The secretary of state shall appoint a chief information security officer who shall be responsible for establishing security standards and policies to protect the office's information technology systems and infrastructure. The chief information security officer shall:

~~(A)~~*(1)* Develop a cybersecurity program for the office that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief information security officer shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

~~(B)~~*(2)* ensure that the secretary of state and all employees complete cybersecurity awareness training annually and that if an employee does not complete the required training, such employee's access to any state-issued hardware or the state network is revoked; and

~~(C) (i) (a)~~*(3) (A) (i)* coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the office for compliance with applicable state and federal laws, rules and regulations and office policies and standards; and

~~(b)~~*(ii)* make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

~~(ii)~~*(B)* Results of audits conducted pursuant to this paragraph shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 3. K.S.A. 2024 Supp. 75-623 is hereby amended to read as follows: 75-623. (a) The treasurer shall appoint such other assistants, clerks, bookkeepers, accountants and stenographers as may be authorized by law, each of which persons shall take the oath of office required of public officers. Such persons shall hold their offices at the will and pleasure of the state treasurer.

(b) ~~(1)~~ The treasurer shall appoint a chief information security officer who shall be responsible for establishing security standards and policies to protect the office's information technology systems and infrastructure. The chief information security officer shall:

~~(A)~~*(1)* Develop a cybersecurity program for the office that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief information security officer shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

~~(B)~~*(2)* ensure that the treasurer and all employees complete cybersecurity awareness training annually and that if an employee does not

complete the required training, such employee's access to any state-issued hardware or the state network is revoked; and

~~(C) (i) (a)~~*(3) (A) (i)* coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the office for compliance with applicable state and federal laws, rules and regulations and office policies and standards; and

~~(b)~~*(ii)* make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

~~(ii)~~*(B)* Results of audits conducted pursuant to this paragraph shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 4. K.S.A. 2024 Supp. 75-710 is hereby amended to read as follows: 75-710. (a) The attorney general shall appoint such assistants, clerks, and stenographers as shall be authorized by law, and who shall hold their office at the will and pleasure of the attorney general. All fees and allowances earned by said assistants or any of them, or allowed to them by any statute or order of court in any civil or criminal case whatsoever, shall be turned into the general revenue fund of the state treasury, and the vouchers for their monthly salaries shall not be honored by the director of accounts and reports until a verified account of the fees collected by them, or either of them, during the preceding month, has been filed in the director of accounts and reports' office. Assistants appointed by the attorney general shall perform the duties and exercise the powers as prescribed by law and shall perform other duties as prescribed by the attorney general. Assistants shall act for and exercise the power of the attorney general to the extent the attorney general delegates them the authority to do so.

(b) ~~(1)~~ The attorney general shall appoint a chief information security officer who shall be responsible for establishing security standards and policies to protect the office's information technology systems and infrastructure. The chief information security officer shall:

~~(A)~~*(1)* Develop a cybersecurity program for the office that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief information security officer shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

~~(B)~~*(2)* ensure that the attorney general and all employees complete cybersecurity awareness training annually and that if an employee does not complete the required training, such employee's access to any state-issued hardware or the state network is revoked; and

~~(C) (i) (a)~~*(3) (A) (i)* coordinate with the United States cybersecurity

and infrastructure security agency to perform annual audits of the office for compliance with applicable state and federal laws, rules and regulations and office policies and standards; and

~~(b)~~*(ii)* make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

~~(ii)~~*(B)* Results of audits conducted pursuant to this paragraph shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 5. K.S.A. 2024 Supp. 75-711 is hereby amended to read as follows: 75-711. (a) There is hereby established, under the jurisdiction of the attorney general, a division to be known as the Kansas bureau of investigation. The director of the bureau shall be appointed by the attorney general, subject to confirmation by the senate as provided in K.S.A. 75-4315b, and amendments thereto, and shall have special training and qualifications for such position. Except as provided by K.S.A. 46-2601, and amendments thereto, no person appointed as director shall exercise any power, duty or function as director until confirmed by the senate. In accordance with appropriation acts, the director shall appoint agents who shall be trained in the detection and apprehension of criminals. The director shall appoint an associate director, and any such assistant directors from within the agency as are necessary for the efficient operation of the bureau, who shall have the qualifications and employee benefits, including longevity, of an agent. The director also may appoint a deputy director and, in accordance with appropriation acts, such administrative employees as are necessary for the efficient operation of the bureau. No person shall be appointed to a position within the Kansas bureau of investigation if the person has been convicted of a felony.

(b) The director, associate director, deputy director, assistant directors and any assistant attorneys general assigned to the bureau shall be within the unclassified service under the Kansas civil service act. All other agents and employees of the bureau shall be in the classified service under the Kansas civil service act and their compensation shall be determined as provided in the Kansas civil service act and shall receive actual and necessary expenses.

(c) Any person who was a member of the bureau at the time of appointment as director, associate director or assistant director, upon the expiration of their appointment, shall be returned to an unclassified or regular classified position under the Kansas civil service act with compensation comparable to and not lower than compensation being received at the time of appointment to the unclassified service. If all such possible positions are filled at that time, a temporary additional position

shall be created for the person until a vacancy exists in the position. While serving in the temporary additional position, the person shall continue to be a contributing member of the retirement system for the agents of the Kansas bureau of investigation.

(d) Each agent of the bureau shall subscribe to an oath to faithfully discharge the duties of such agent's office, as is required of other public officials.

(e) ~~(1)~~ The director shall appoint a chief information security officer who shall be responsible for establishing security standards and policies to protect the bureau's information technology systems and infrastructure. The chief information security officer shall:

~~(A)~~*(1)* Develop a cybersecurity program for the bureau that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief information security officer shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;

~~(B)~~*(2)* ensure that the director and all employees complete cybersecurity awareness training annually and that if an employee does not complete the required training, such employee's access to any state-issued hardware or the state network is revoked; and

~~(C) (i) (a)~~*(3) (A) (i)* coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of the department for compliance with applicable state and federal laws, rules and regulations and department policies and standards; and

~~(b)~~*(ii)* make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

~~(ii)~~*(B)* Results of audits conducted pursuant to this paragraph shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

~~(2) The provisions of this subsection shall expire on July 1, 2026.~~

Sec. 6. K.S.A. 75-7203 is hereby amended to read as follows: 75-7203. (a) The information technology executive council is hereby authorized to adopt such policies and rules and regulations as necessary to implement, administer and enforce the provisions of this act.

(b) The council shall:

(1) Adopt:

(A) Information technology resource policies and procedures and project management methodologies for all executive branch agencies;

(B) an information technology architecture, including telecommunications systems, networks and equipment, that covers all state agencies;

(C) standards for data management for all executive branch agencies;

and

(D) a strategic information technology management plan for the executive branch;

(2) provide direction and coordination for the application of the executive branch's information technology resources;

(3) designate the ownership of information resource processes and the lead executive branch agency for implementation of new technologies and networks shared by multiple agencies within the executive branch of state government;

(4) develop a plan to integrate all information technology services for the executive branch into the office of information technology services and all cybersecurity services for state educational institutions as defined in K.S.A. 76-711, and amendments thereto, into the office of information technology services and the Kansas information security office; and

(5) perform such other functions and duties as necessary to carry out the provisions of this act.

(c) The information technology executive council shall report the plan developed under subsection (b)(4) to the senate standing committee on ways and means ~~and~~, the house standing committee on legislative modernization or its successor committee *and the joint committee on information technology* prior to January 15, 2026, in accordance with K.S.A. 2024 Supp. 75-7245, and amendments thereto.

Sec. 7. K.S.A. 2024 Supp. 75-7206a is hereby amended to read as follows: 75-7206a. (a) There is hereby established the position of judicial branch chief information security officer. The judicial chief information security officer shall be in the unclassified service under the Kansas civil service act, shall be appointed by the judicial administrator, subject to approval by the chief justice and shall receive compensation determined by the judicial administrator, subject to approval of the chief justice.

(b) The judicial chief information security officer shall:

(1) Report to the judicial administrator;

(2) establish security standards and policies to protect the branch's information technology systems and infrastructure in accordance with subsection (c);

(3) ensure the confidentiality, availability and integrity of the information transacted, stored or processed in the branch's information technology systems and infrastructure;

(4) develop a centralized cybersecurity protocol for protecting and managing judicial branch information technology assets and infrastructure;

(5) detect and respond to security incidents consistent with information security standards and policies;

(6) be responsible for the cybersecurity of all judicial branch data and information resources;

(7) collaborate with the chief information security officers of the other branches of state government to respond to cybersecurity incidents;

(8) ensure that all justices, judges and judicial branch employees complete cybersecurity awareness training annually and if an employee does not complete the required training, such employee's access to any state-issued hardware or the state network is revoked;

(9) review all contracts related to information technology entered into by a person or entity within the judicial branch to make efforts to reduce the risk of security vulnerabilities within the supply chain or product and ensure each contract contains standard security language; and

(10) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of judicial branch agencies for compliance with applicable state and federal laws, rules and regulations and judicial branch policies and standards. The judicial chief information security officer shall make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

(c) The judicial chief information security officer shall develop a cybersecurity program of each judicial agency that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The judicial chief information security officer shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030.

(d) (1) If an audit conducted pursuant to subsection (b)(10) results in a failure, the judicial chief information security officer shall report such failure to the speaker and minority leader of the house of representatives and the president and minority leader of the senate within 30 days of receiving notice of such failure. Such report shall contain a plan to mitigate any security risks identified in the audit. The judicial chief information security officer shall coordinate for an additional audit after the mitigation plan is implemented and report the results of such audit to the speaker and minority leader of the house of representatives and the president and minority leader of the senate.

(2) Results of audits conducted pursuant to subsection (b)(10) and the reports described in subsection (d)(1) shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

~~(e) This section shall expire on July 1, 2026.~~

Sec. 8. K.S.A. 2024 Supp. 75-7208a is hereby amended to read as follows: 75-7208a. (a) There is hereby established the position of legislative branch chief information security officer. The legislative chief information security officer shall be in the unclassified service under the Kansas civil service act, shall be appointed by the legislative coordinating

council and shall receive compensation determined by the legislative coordinating council.

(b) The legislative chief information security officer shall:

(1) Report to the legislative chief information technology officer;

(2) establish security standards and policies to protect the branch's information technology systems and infrastructure in accordance with subsection (c);

(3) ensure the confidentiality, availability and integrity of the information transacted, stored or processed in the branch's information technology systems and infrastructure;

(4) develop a centralized cybersecurity protocol for protecting and managing legislative branch information technology assets and infrastructure;

(5) detect and respond to security incidents consistent with information security standards and policies;

(6) be responsible for the cybersecurity of all legislative branch data and information resources and obtain approval from the revisor of statutes prior to taking any action on any matter that involves a legal issue related to the security of information technology;

(7) collaborate with the chief information security officers of the other branches of state government to respond to cybersecurity incidents;

(8) ensure that all legislators and legislative branch employees complete cybersecurity awareness training annually and if an employee does not complete the required training, such employee's access to any state-issued hardware or the state network is revoked;

(9) review all contracts related to information technology entered into by a person or entity within the legislative branch to make efforts to reduce the risk of security vulnerabilities within the supply chain or product and ensure each contract contains standard security language; and

(10) coordinate with the United States cybersecurity and infrastructure security agency to perform annual audits of legislative branch agencies for compliance with applicable state and federal laws, rules and regulations and legislative branch policies and standards. The legislative chief information security officer shall make an audit request to such agency annually, regardless of whether or not such agency has the capacity to perform the requested audit.

(c) The legislative chief information security officer shall develop a cybersecurity program of each legislative agency that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The legislative chief information security officer shall ensure that such programs achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030. The agency head of each legislative agency shall coordinate with the legislative

chief information security officer to achieve such standards.

(d) (1) If an audit conducted pursuant to subsection (b)(10) results in a failure, the legislative chief information security officer shall report such failure to the speaker and minority leader of the house of representatives and the president and minority leader of the senate within 30 days of receiving notice of such failure. Such report shall contain a plan to mitigate any security risks identified in the audit. The legislative chief information security officer shall coordinate for an additional audit after the mitigation plan is implemented and report the results of such audit to the speaker and minority leader of the house of representatives and the president and minority leader of the senate.

(2) Results of audits conducted pursuant to subsection (b)(10) and the reports described in subsection (d)(1) shall be confidential and shall not be subject to discovery or disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto.

~~(e) This section shall expire on July 1, 2026.~~

Sec. 9. K.S.A. 2024 Supp. 75-7245 is hereby amended to read as follows: 75-7245. (a) On and after July 1, 2027, all cybersecurity services for each branch of state government shall be administered by the chief information technology officer and the chief information security officer of such branch. All cybersecurity employees within the legislative and executive branches of state government shall work at the direction of the chief information technology officer of the branch.

(b) Prior to January 1, 2026:

(1) The information technology executive council shall develop a plan to integrate all executive branch information technology services into the office of information technology services. The council shall consult with each agency head when developing such plan.

(2) The judicial chief information technology officer shall develop an estimated project cost to provide information technology to judicial agencies and all employees of such agencies, including state and county-funded judicial branch district court employees. Such employees shall be required to use such state-issued information technology hardware. The project cost developed pursuant to this paragraph shall include, in consultation with the executive branch information technology officer, a plan to allow each piece of information technology hardware that is used by a judicial branch employee to access a judicial branch application to have access to the KANWIN network and an estimated project cost to develop a cybersecurity program for all judicial districts that complies with the national institute of standards and technology cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024.

(c) The information technology executive council shall report the plan developed pursuant to subsection (b) to the senate standing committee

on ways and means ~~and~~, the house standing committee on legislative modernization or its successor committee *and the joint committee on information technology,* prior to January 15, 2026.

(d) Prior to February 1, 2025, every website that is maintained by a branch of government or state agency shall be moved to a ".gov" domain.

(e) On July 1, 2025, and each year thereafter, moneys appropriated from the state general fund to or any special revenue fund of any state agency for information technology and cybersecurity expenditures shall be appropriated as a separate line item and shall not be merged with other items of appropriation for such state agency to allow for detailed review by the senate committee on ways and means and the house of representatives committee on appropriations during each regular legislative session.

(f) The provisions of this section do not apply to state educational institutions as defined in K.S.A. 76-711, and amendments thereto.

~~(g) This section shall expire on July 1, 2026.~~

Sec. 10. K.S.A. 2024 Supp. 75-7246 is hereby amended to read as follows: 75-7246. (a) On July 1, 2028, and each year thereafter, the director of the budget, in consultation with the legislative, executive and judicial chief information technology officers as appropriate, shall determine if each state agency is in compliance with the provisions of this act* for the previous fiscal year. If the director of the budget determines that a state agency is not in compliance with the provisions of this act for such fiscal year, the director shall certify an amount equal to 5% of the amount:

(1) Appropriated and reappropriated from the state general fund for such state agency for such fiscal year; and

(2) credited to and available in each special revenue fund for such state agency in such fiscal year. If during any fiscal year, a special revenue fund has no expenditure limitation, then an expenditure limitation shall be established for such fiscal year on such special revenue fund by the director of the budget in an amount that is 5% less than the amount of moneys credited to and available in such special revenue fund for such fiscal year.

(b) The director of the budget shall submit a detailed written report to the legislature on or before the first day of the regular session of the legislature concerning such compliance determinations, including factors considered by the director when making such determination, and the amounts certified for each state agency for such fiscal year.

(c) During the regular session of the legislature, the senate committee on ways and means and the house of representatives committee on appropriations shall consider such compliance determinations and whether to lapse amounts appropriated and reappropriated and decrease the

expenditure limitations of special revenue funds for such state agencies during the budget committee hearings for such noncomplying agency.

~~(d) This section shall expire on July 1, 2026.~~

Sec. 11. K.S.A. 2024 Supp. 40-110, 45-229, as amended by section 11 of chapter 95 of the 2024 Session Laws of Kansas, 75-413, 75-623, 75-710, 75-711, 75-7201, as amended by section 17 of chapter 95 of the 2024 Session Laws of Kansas, 75-7202, as amended by section 19 of chapter 95 of the 2024 Session Laws of Kansas, 75-7203, 75-7203, as amended by section 21 of chapter 95 of the 2024 Session Laws of Kansas, 75-7205, as amended by section 23 of chapter 95 of the 2024 Session Laws of Kansas, 75-7206, as amended by section 25 of chapter 95 of the 2024 Session Laws of Kansas, 75-7206a, 75-7208, as amended by section 27 of chapter 95 of the 2024 Session Laws of Kansas, 75-7208a, 75-7209, as amended by section 29 of chapter 95 of the 2024 Session Laws of Kansas, 75-7237, as amended by section 31 of chapter 95 of the 2024 Session Laws of Kansas, 75-7238, as amended by section 33 of chapter 95 of the 2024 Session Laws of Kansas, 75-7239, as amended by section 35 of chapter 95 of the 2024 Session Laws of Kansas, 75-7240, as amended by section 37 of chapter 95 of the 2024 Session Laws of Kansas, 75-7245 and 75-7246 are hereby repealed.

Sec. 12. This act shall take effect and be in force from and after its publication in the statute book.