ARC 4712C

CHIEF INFORMATION OFFICER, OFFICE OF THE[129]

Notice of Intended Action

Proposing rule making related to information technology governance and providing an opportunity for public comment

The Office of the Chief Information Officer hereby proposes to adopt new Chapter 8, "Information Technology Governance," Iowa Administrative Code.

Legal Authority for Rule Making

This rule making is proposed under the authority provided in Iowa Code sections 8B.4(5), 8B.4(6), 8B.21(1)"d," 8B.21(5), 8B.23, 8B.24(1), 8B.24(2) and 8B.24(3) and section 8B.11(8) as amended by 2019 Iowa Acts, House File 772, section 10.

State or Federal Law Implemented

This rule making implements, in whole or in part, Iowa Code chapter 8B.

Purpose and Summary

The Office is created for the purpose of leading, directing, managing, coordinating, and providing accountability for the information technology resources of state government. In furtherance of this role, the Office is, among other things, required or authorized by Iowa Code chapter 8B to:

1. Develop and implement an information strategic plan for the enterprise;
2. Establish an enterprise strategic and project management function for oversight of all information technology-related projects and resources of participating agencies;
3. Develop information technology governance requirements that apply to participating agencies, including:

- Standards of or related to cybersecurity, geospatial systems, application development, and information technology and procurement, including but not limited to system design and systems integration, and interoperability;
- Policies of or related to security to ensure the integrity of the state's information resources and to prevent the disclosure of confidential records, while still fostering transparency and data sharing;
- Statewide standards for information technology security to maximize the functionality, security, and interoperability of the state's distributed information technology assets, including but not limited to communications and encryption technologies;
- Standards for the implementation of electronic commerce, including standards for electronic signatures, electronic currency, and other items associated with electronic commerce;
- Guidelines for the appearance and functioning of applications;
- Standards for the integration of electronic data across state agencies;
- Standards, policies, and procedures of or applicable to the procurement of information technology;

4. Require all information technology security services, solutions, hardware, and software purchased or used by a participating agency to be subject to approval by the office in accordance with security standards;
5. Develop and implement effective and efficient strategies for the use and provision of information technology and information technology staff for participating agencies and other governmental entities; and
6. Manage and oversee the IowAccess program.

In addition, the Office is required to "adopt rules allowing for participating agencies to seek a temporary or permanent waiver from any of the requirements of [Iowa Code chapter 8B] concerning the acquisition, utilization, or provision of information technology." See Iowa Code section 8B.21(5)"a."

To that end, this new chapter establishes the Office's process for developing and promulgating information technology policies, standards, processes, procedures, and guidelines, with appropriate stakeholder input; related assessment and enforcement processes and procedures; and a uniform process for the granting of information technology waivers requested by a participating agency from such information technology governance requirements.

Fiscal Impact

This rule making is likely to have no fiscal impact because it outlines processes already generally utilized and followed by the Office but not yet codified in rule. This rule making may have a positive fiscal impact, and binding rules that have the force and effect of law may provide the Office with more effective tools to incentivize and ensure compliance with information technology requirements developed, administered, and enforced by the Office.

Jobs Impact

After analysis and review of this rule making, no impact on jobs has been found.

Waivers

As required by Iowa Code section 8B.21(5)"a," this new chapter establishes a uniform process for the granting of information technology waivers requested by a participating agency from information technology governance requirements developed and administered by the Office. In addition, the Office has initiated a separate Notice of Intended Action (**ARC 4710C**, IAB 10/23/19) proposing to adopt general waiver processes pursuant to Iowa Code section 17A.9A(1) simultaneous with this Notice.

Public Comment

Any interested person may submit written or oral comments concerning this proposed rule making. Written or oral comments in response to this rule making must be received by the Office no later than 4:30 p.m. on November 12, 2019. Comments should be directed to:

Matt Behrens
Office of the Chief Information Officer
Hoover State Office Building, Level B
1305 East Walnut Street
Des Moines, Iowa 50319
Phone: 515.281.5503
Fax: 515.281.6137
Email: cio@iowa.gov

Public Hearing

A public hearing at which persons may present their views orally or in writing will be held as follows:

November 12, 2019 1 to 2 p.m.	Hoover State Office Building, Level A OCIO Innovation Lab, Room 12 Des Moines, Iowa

Persons who wish to make oral comments at the public hearing may be asked to state their names for the record and to confine their remarks to the subject of this proposed rule making.

Any persons who intend to attend the public hearing and have special requirements, such as those related to hearing or mobility impairments, should contact the Office and advise of specific needs by calling 515.281.5503.

Review by Administrative Rules Review Committee

The Administrative Rules Review Committee, a bipartisan legislative committee which oversees rule making by executive branch agencies, may, on its own motion or on written request by any individual or group, review this rule making at its regular monthly meeting or at a special meeting. The Committee's meetings are open to the public, and interested persons may be heard as provided in Iowa Code section 17A.8(6).

The following rule-making action is proposed:

Adopt the following **new** 129—Chapter 8:

CHAPTER 8
INFORMATION TECHNOLOGY GOVERNANCE

129—8.1(8B) Definitions. The definitions in Iowa Code section 8B.1 shall apply to this chapter. In addition, the following definitions shall also apply:

"Agency" or *"state agency"* means a unit of state government, which is an authority, board, commission, committee, council, department, examining board, or independent agency as defined in Iowa Code section 7E.4, including but not limited to each principal central department enumerated in Iowa Code section 7E.5. However, "agency" or "state agency" does not mean any of the following:

1. The office of the governor or the office of an elective constitutional or statutory officer.
2. The general assembly, or any office or unit under its administrative authority.
3. The judicial branch, as provided in Iowa Code section 602.1102.
4. A political subdivision of the state or its offices or units, including but not limited to a county, city, or community college.

"Chief information officer" or *"CIO"* means the state chief information officer or the CIO's designee.

"Information technology governance document(s)" or *"information technology governance requirement(s)"* means compulsory information technology statutes, rules, policies, standards, processes, or procedures which are promulgated, administered, or enforced by the office and which govern participating agencies' acquisition, utilization, or provision of information technology.

"Information technology waiver" or *"waiver"* means, as applied to a participating agency on the basis of the particular circumstances of that agency, any action by the office that suspends, in whole or in part, the requirements of any information technology governance requirement.

"Participating agency" shall have the meaning ascribed to it under Iowa Code chapter 8B but does not include state agencies that are excluded from the definition of state agency as defined in this chapter or that are otherwise exempt pursuant to their specific enabling acts.

129—8.2(8B) Purpose and applicability.

8.2(1) *Purpose.* The office is created for the purpose of leading, directing, managing, coordinating, and providing accountability for the information technology resources of state government. In furtherance of this role, the office is, among other things, required or authorized to:

a. Develop and implement an information strategic plan for the enterprise.

b. Establish an enterprise strategic and project management function for oversight of all information technology-related projects and resources of participating agencies. In exercising this power and duty, the office will endeavor to collaborate and coordinate with participating agencies to the maximum extent possible.

c. Develop information technology governance requirements that apply to participating agencies, including but not limited to:

(1) Standards of or related to cybersecurity, geospatial systems, application development, and information technology and procurement, including but not limited to system design and systems integration, and interoperability.

(2) Policies of or related to security to ensure the integrity of the state's information resources and to prevent the disclosure of confidential records, while still fostering transparency and data sharing.

(3) Statewide standards for information technology security to maximize the functionality, security, and interoperability of the state's distributed information technology assets, including but not limited to communications and encryption technologies.

(4) Standards for the implementation of electronic commerce, including standards for electronic signatures, electronic currency, and other items associated with electronic commerce.

(5) Guidelines for the appearance and functioning of applications.

(6) Standards for the integration of electronic data across state agencies.

(7) Standards, policies, and procedures of or applicable to the procurement of information technology.

d. Require all information technology security services, solutions, hardware, and software purchased or used by a participating agency to be subject to approval by the office in accordance with security standards. In exercising this power and duty, the office will endeavor to collaborate and coordinate with participating agencies to the maximum extent possible.

e. Develop and implement effective and efficient strategies for the use and provision of information technology and information technology staff for participating agencies and other governmental entities.

f. Manage and oversee the IowAccess program.

This chapter outlines the office's process for achieving such objectives with appropriate stakeholder input, including the process by which the office establishes information technology governance requirements; related assessment and enforcement processes and procedures; and a uniform process for the granting of information technology waivers requested by a participating agency from such information technology governance requirements.

8.2(2) *Applicability.*

a. Information technology governance requirements established by the office, unless waived in accordance with the waiver process set forth herein, shall apply to all participating agencies.

b. The office of the governor and the offices of elective constitutional or statutory officers are not required to comply with information technology governance requirements established by the office. However, as required by Iowa Code section 8B.23, they must:

(1) Consider the information technology governance requirements adopted by the office; and

(2) In the case of any acquisition of information technology, consult with the office prior to making any such acquisition and provide a written report to the office relating to any decision regarding such acquisitions.

129—8.3(8B) Advisory groups. The office may establish advisory groups and related policies and procedures to organize and effectively and efficiently utilize such advisory groups. Advisory groups may be comprised of information technology leaders from agencies across state government to advise and assist the CIO and office in accomplishing the objectives, duties, and responsibilities outlined herein and in Iowa Code chapter 8B. Advisory groups established by the office shall be solely advisory to the CIO and office, and the CIO and office retain all final decision-making authority as conferred by Iowa Code chapter 8B.

129—8.4(8B) Information technology governance requirements.

8.4(1) *Proposing information technology governance requirements.* Anyone may recommend the development or adoption of an information technology governance requirement to the CIO or office or advisory committee created and designated by the CIO for such purpose.

8.4(2) *Development of information technology governance requirements.* Where the CIO, office, or advisory committee created and designated by the CIO for such purpose is of the opinion that a proposed

information technology governance requirement has merit, the CIO, office, or advisory committee created and designated by the CIO for such purpose may work with the individual proposing the information technology governance requirement to develop the requirement. In developing information technology standards, the CIO, office, or advisory committee created and designated by the CIO for such purpose may consider, by way of example only:

a. Whether and how such requirement furthers the objectives of the enterprise;

b. Current industry standards or best practices;

c. Whether and how the requirement would help avoid the duplication of services, resources, or support;

d. Whether and how the requirement would further the state's information technology strategic plan, enterprise architecture, security plans, or any other information technology governance requirements;

e. Whether and how the requirement would affect expenditures across the enterprise;

f. Existing technology deployments;

g. The impact on state resources;

h. Acquisition, development and deployment time frames associated with implementing the requirement.

8.4(3) *Types of information technology governance requirements.* Information technology governance requirements may include any of the following:

a. "Policy(ies)" means a high-level statement of intent applicable to the acquisition, utilization, or provision of information technology designed to facilitate an enterprisewide goal or objective.

b. "Standard(s)" means a specific, minimum requirement(s) applicable to the acquisition, utilization, or provision of information technology, typically designed to facilitate the uniform application or implementation of one or more policies. Standards may set forth required or prohibited technical approaches, solutions, methodologies, products or protocols which must be adhered to in the design, development, implementation, or upgrade of systems architecture, including hardware, software and services. Standards are intended to establish uniformity in common technology infrastructures, applications, processes or data, and may define or limit the tools, proprietary product offerings or technical solutions which may be used, developed or deployed by participating agencies.

c. "Process(es)" means a high-level overview of required tasks, approvals, procedures, or other processes, typically designed to operationalize one or more policies or standards in a manner that leads to consistent results.

d. "Procedure(s)" means an in-depth set of instructions for the completion of a specific process, task, or action typically designed to operationalize one or more processes or standards in a manner that leads to consistent results.

e. "Guideline(s)" or "best practices" means a recommended policy, process, task, or action related to the acquisition, utilization, or provision of information technology, typically designed to support related policies or standards. Guidelines or best practices are not required but are intended to aid participating agencies in assessing risks associated with technology decisions, facilitate knowledge transfer, and communicate lessons learned from past experience.

8.4(4) *Goals for information technology governance requirements.* The underlying purpose of information technology governance requirements is, by way of example only:

a. To promote collaboration and consistency in the automation of systems;

b. To eliminate duplicative development efforts and promote efficiencies for improved services to citizens and businesses;

c. To ensure continuity of ongoing state operations;

d. To ensure system security and the confidentiality, integrity, and availability of confidential or sensitive information stored or processed by state information systems;

e. To promote administrative efficiencies relating to development and maintenance of systems; and

f. To enable the state to realize its full purchasing power from the use of a statewide, enterprise approach to the selection of technology solutions.

8.4(5) *Adopting of information technology governance requirements and taking effect.*

a. Following the development of a proposed information technology governance requirement, the CIO may adopt the information technology governance requirement. The CIO shall solicit stakeholder input and feedback, including feedback from participating agencies to which the information technology governance requirement would apply, prior to adopting an information technology governance requirement.

b. The effective date of an information technology governance requirement shall be as stated in the applicable information technology governance document.

c. Upon taking effect, an information technology governance requirement shall apply to all participating agencies.

d. Participating agencies may request additional time to comply with information technology governance requirements. Such requests shall be considered a request for temporary waiver and must be submitted in accordance with rule 129—8.6(8B).

129—8.5(8B) Assessment and enforcement of information technology governance requirements.

8.5(1) *Compliance assessments and requests for information.* The office may periodically assess participating agencies' compliance with information technology governance requirements. In so doing, the office will coordinate and collaborate with participating agencies. Participating agencies shall provide appropriate information, access, and assistance to complete such assessments, or as is otherwise necessary for the office to carry out its duties and responsibilities under Iowa Code chapter 8B. As part of such assessments, participating agencies may be required to, by way of example only:

a. Provide the office with information as required by Iowa Code section 8B.21(1)*"k"* and *"l,"* or as otherwise required pursuant to Iowa Code chapter 8B or 22. Such information may include, but not be limited to:

(1) An inventory of information technology used by the participating agency.

(2) Budget or spending information of or related to information technology.

(3) Competitive selection documents, acquisition documents, internal procurement policies adopted by the participating agency, and other documents relied on, issued by, or executed by the participating agency related to the acquisition of information technology.

(4) Information about any security incidents.

(5) Security logs and reports, such as latency statistics, user access summaries, user access IP address summaries, user access history and security logs for information technology systems of the participating agency or its vendors.

(6) Security processes and technical limitations of the participating agency or its vendors, such as those related to virus checking and port sniffing.

b. Permit the office or its third-party designee to conduct security testing and compliance audits on a participating agency's or its vendor's information systems. Such testing and compliance audits may include but not be limited to unannounced penetration and security tests as they relate to the receipt, maintenance, use or retention of the state of Iowa's sensitive or confidential information.

Failure of a participating agency to provide the office with information or submit to compliance audits as requested by the office may be considered a violation of these rules and Iowa Code chapter 8B.

8.5(2) *Alternative assessment methods.* Participating agencies may request the acceptance of results of like assessments conducted by third parties in lieu of an assessment by the office. Whether to accept such alternative assessment methods shall be determined in the discretion of the CIO in coordination with the applicable participating agency.

8.5(3) *Determination of noncompliance.*

a. If the office determines that a participating agency is noncompliant with an information technology governance requirement, the office shall send a report to the head of the noncompliant participating agency, which report shall outline:

(1) The specific information technology governance requirement(s) forming the basis of a violation or ground for noncompliance;

(2) The relevant facts and corresponding reasoning supporting the office's findings and conclusions;

(3) The office's recommendations for remedying the violations or noncompliance.

b. Within 30 calendar days of receipt of the noncompliance notification, the participating agency shall submit to the office a written plan describing the actions the agency will take to achieve compliance or submit a written request for waiver in accordance with rule 129—8.6(8B). The office may, on its own motion or at the request of the participating agency, schedule a meeting between the participating agency and the office. Based on the participating agency's response and outcome of any meeting between the participating agency and the office, or office's decision with respect to any request for waiver submitted by the participating agency, the office may modify, alter, or amend its original report and recommendations.

8.5(4) *Emergency remediation.* When noncompliance with information technology governance requirements is determined by the CIO to be a threat to critical state information resources or information resources outside state government, the CIO may order the immediate shutdown or disconnection of the agency technology services that are contributing to the threat. If the agency does not immediately comply, the office, Iowa communications network, or other body may disconnect the agency from all shared services. The agency will be reconnected to shared services when the CIO determines there is no longer a critical threat.

129—8.6(8B) Waivers from information technology governance requirements.

8.6(1) *Requests for waiver.* A participating agency may file a request for waiver from an information technology governance requirement, in whole or in part, in accordance with the following form, manner, and content requirements.

a. Form and manner. A request for waiver shall be made on forms provided by the office and may be submitted by email to cio@iowa.gov. A request for waiver must be signed by the head of the participating agency seeking the waiver.

b. Content. The request shall:

(1) Include the name and address of the participating agency and a telephone number and email address for the point of contact at the participating agency to whom inquiries and notices regarding the request for waiver may be directed;

(2) Include a reference to the specific information technology governance requirement for which the waiver is submitted;

(3) Include a statement of facts, including a description of the problem or issue prompting the request;

(4) Describe the participating agency's preferred solution;

(5) Outline an alternative approach to be implemented by the participating agency intended to satisfy the waived information technology governance requirement;

(6) Describe the business case for the alternative approach;

(7) Include a copy of a third-party audit or report that compares the participating agency's preferred solution to the information technology solution that can be provided by the office;

(8) Outline the economic justification for the waiver or a statement as to why the waiver is in the best interests of the state;

(9) Specify the time period for which the waiver is requested and, to the extent a permanent waiver is requested, explain why a temporary waiver would be impracticable; and

(10) Include or be accompanied by any other information, including supporting evidence or documentation, deemed relevant by the participating agency, including information that would aid the office in applying the factors outlined in Iowa Code section 8B.21(5)*"b"* or determining whether granting the request, in whole or in part, is in the best interests of the state of Iowa.

c. The office and participating agency shall collaborate on both determining the need for a waiver and, if a waiver is determined to be necessary, the development of request for waiver.

8.6(2) *Notice, additional information, and opportunity for meeting.*

a. Notice. The office may notify other participating agencies that may be interested in or affected by the office's decision regarding a request for waiver and may allow other participating agencies to review the request for waiver and related materials submitted in connection therewith.

b. Additional information.

(1) The office may request, or require in accordance with Iowa Code section 8B.21(1)*"k"* and *"l,"* additional information, evidence, or documentation from the participating agency submitting the request that would aid the office in assessing the request in accordance with the factors outlined in Iowa Code section 8B.21(5)*"b"* and in determining whether granting the request, in whole or in part, is ultimately in the best interests of the state of Iowa.

(2) The office may permit, or require in accordance with Iowa Code section 8B.21(1)*"k"* and *"l,"* other participating agencies that may be interested in or affected by the office's decision to submit supporting or competing viewpoints, evidence, or documentation that would aid the office in assessing the request in accordance with the factors outlined in Iowa Code section 8B.21(5)*"b"* and in determining whether granting the request, in whole or in part, is ultimately in the best interests of the state of Iowa.

c. The office shall coordinate and schedule a meeting with the participating agency submitting the request or any other participating agency that may be interested in or affected by the office's decision.

8.6(3) *Granting a waiver.* In response to the office's receipt of a request for waiver under and in accordance with this chapter, the CIO may issue an order waiving, in whole or in part, an information technology governance requirement. The CIO may only grant a waiver if the participating agency shows that the waiver would be in the best interests of the state. In determining whether to grant a waiver, in whole or in part, the CIO shall consider the factors outlined in Iowa Code section 8B.21(5)*"b."* The final decision on whether the circumstances justify the grant of a requested waiver, in whole or in part, shall be in the sole discretion of the CIO.

a. An order granting or denying a waiver, in whole or in part, shall be in writing and shall:

(1) Identify the participating agency(ies) to which the order applies;

(2) Identify the specific information technology governance requirements involved;

(3) Include a statement of the relevant facts and reasons for the decision, including an application of the factors outlined in Iowa Code section 8B.21(5)*"b"* and an explanation as to how the waiver is or is not in the best interests of the state; and

(4) To the extent a waiver is granted, describe the precise scope of the waiver including its duration and any conditions associated therewith.

b. A waiver, if granted, shall provide the narrowest exception possible to the information technology governance requirements involved.

c. The CIO may place any condition on a waiver that the CIO finds desirable to protect the best interests of the state.

d. A waiver shall not be permanent unless the requestor can show that a temporary waiver would be impracticable. If a temporary waiver is granted, there is no automatic right to renewal. At the sole discretion of the CIO, a waiver may be renewed if the CIO finds that grounds for a waiver continue to exist.

e. The CIO shall grant or deny a request for waiver as soon as practicable but, in any event, shall do so within 120 days of its receipt, unless the petitioner agrees to a later date or the CIO, specifying good cause, extends this time period with respect to a particular petition for an additional 30 days.

f. Service of order. Within seven days of its issuance, any order issued under this chapter shall be transmitted to the participating agency by email to the contact at the participating agency identified in the request for waiver. The office may also transmit a copy of the order to other participating agencies that may be interested in or affected by the office's decision.

g. Consolidation. In the event the CIO receives similar requests for waivers from multiple participating agencies concerning the same information technology governance requirements, the CIO may consolidate the requests and issue a single ruling granting or denying the requests, in whole or in part.

8.6(4) *Cancellation of a waiver.* A waiver issued by the CIO pursuant to this chapter may be withdrawn, canceled, or modified after appropriate notice and fact-finding. Failure of a participating

agency to cooperate in any fact-finding process initiated by the CIO to determine whether a waiver previously issued pursuant to this chapter should be withdrawn, canceled, or modified is grounds to cancel or modify a previously granted waiver.

8.6(5) *Violation of a waiver.* Violation of a condition in a waiver order shall be treated as a violation of the information technology governance requirement for which the waiver was granted.

8.6(6) *Defense.* After the CIO issues an order granting a waiver, the order is a defense within its terms and the specific facts indicated therein for the participating agency to which the order pertains in any proceeding in which the rule in question is sought to be invoked.

129—8.7(8B,22) Public availability. Reports issued by the office, or orders granting or denying waivers, under this chapter shall be indexed, filed, and made available for public inspection as provided in Iowa Code section 17A.3. Such reports, orders, and related materials may be considered public records under Iowa Code chapter 22; provided, however, that such reports, orders, and related materials may contain information the office is authorized or required to keep confidential. The office may accordingly redact confidential information from petitions or orders prior to public release or inspection.

129—8.8(8B) Appeals. A participating agency may appeal a final decision of the CIO regarding the participating agency's noncompliance with information technology governance requirements under rule 129—8.5(8B), or a denial, in whole or in part, of a request for waiver under rule 129—8.6(8B), to the director of the department of management within seven calendar days following the service of the decision. The director of the department of management shall respond within 14 days following the receipt of the appeal.

These rules are intended to implement Iowa Code chapter 8B.