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 Internet protocol (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.

[**ARC 4824C**, IAB 12/18/19, effective 1/22/20]