APPROVED
APRIL 15, 2026
BY GOVERNOR

CHAPTER
698
PUBLIC LAW

STATE OF MAINE

IN THE YEAR OF OUR LORD

TWO THOUSAND TWENTY-SIX

H.P. 1407 - L.D. 2092

An Act to Update Certain Terms and References Regarding Information Technology and Cybersecurity

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 5 MRSA §1825-B, sub-§2, ¶F, as amended by PL 2023, c. 516, Pt. A, §1, is further amended to read:

F. The procurement of goods or services involves expenditures of $25,000 or less, in which case the Director of the Bureau of General Services may accept informal written quotes or bids; ~~or~~

Sec. 2. 5 MRSA §1825-B, sub-§2, ¶G, as amended by PL 1999, c. 105, §3, is further amended to read:

G. The procurement of goods or services involves expenditures of $10,000 or less, and procurement from a single source is the most economical, effective and appropriate means of fulfilling a demonstrated need~~.~~;

Sec. 3. 5 MRSA §1825-B, sub-§2, ¶H is enacted to read:

H. The Chief Information Officer, after reasonable investigation, has determined that the procurement of information technology products or services through the procurement offerings to state and local governments from the United States General Services Administration is in the best interest of the State; or

Sec. 4. 5 MRSA §1825-B, sub-§2, ¶I is enacted to read:

I. The Chief Information Officer, after reasonable investigation, has determined that the procurement of information security or cybersecurity products or services on a retainer basis is necessary to detect, prevent and respond to cyberattacks.

Sec. 5. 5 MRSA §1972, sub-§4-A is enacted to read:

4-A. Cyberattack. "Cyberattack" has the same meaning as in Title 37-B, section 703, subsection 1-A.

Sec. 6. 5 MRSA §1972, sub-§4-B is enacted to read:

4-B. Cybersecurity. "Cybersecurity" means the protection of information and communications technology infrastructure, systems and services affecting the enterprise and the State's critical infrastructure, whether physical or nonphysical, by detecting, preventing and responding to cyberattacks.

Sec. 7. 5 MRSA §1972, sub-§7-A is enacted to read:

7-A. Information security. "Information security" means the ability to protect or defend the information and communications technology infrastructure, systems or services affecting the enterprise or the State's critical infrastructure, whether physical or nonphysical, from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.

Sec. 8. 5 MRSA §1973, sub-§5, ¶B, as enacted by PL 2001, c. 388, §14, is amended to read:

B. Approve the ~~Division of Purchases'~~ standards and evaluation procedures of the division of purchases within the Department of Administrative and Financial Services, Bureau of General Services for standard information and telecommunications technology acquisitions and contracts.

Sec. 9. 5 MRSA §1974, sub-§1, as enacted by PL 2001, c. 388, §14, is amended to read:

1. Approve the acquisition and use of equipment. The Chief Information Officer, or the Chief Information Officer's designee, working with the ~~Division of Purchases~~ division of purchases within the Department of Administrative and Financial Services, Bureau of General Services and in accordance with written standards established by this chapter, shall approve acquisition and use of all data processing and telecommunications services, equipment and systems by state agencies.

Sec. 10. 5 MRSA §1974, sub-§2, as enacted by PL 2001, c. 388, §14, is amended to read:

2. Develop training and development programs in data processing. The Chief Information Officer, or the Chief Information Officer's designee, is responsible for developing training and development programs for state employees in data processing and for the implementation of these programs.

Sec. 11. 5 MRSA §1974, sub-§3, as amended by PL 2005, c. 12, Pt. SS, §12, is further amended to read:

3. Develop and administer written standards for data processing and telecommunications. The Chief Information Officer, or the Chief Information Officer's designee, shall develop and administer written standards for data processing and telecommunications. These written standards pertain to:

A. Acquisition of equipment;

B. Acquisition of computer software and systems;

C. Development of computer systems and computer programs;

D. Computer operations; ~~and~~

D-1. Information security and cybersecurity policies, procedures and related operations; and

E. Any other standards determined necessary by the Chief Information Officer ~~and the board~~.

Sec. 12. 5 MRSA §1975, as amended by PL 2005, c. 12, Pt. SS, §15, is further amended to read:

§1975. Noncompliance

The purchase of data processing equipment, software or services or internal systems development efforts may not be made except in accordance with this chapter. An agency may not purchase any data processing equipment, software or services without the prior written approval of the commissioner or the Chief Information Officer or the Chief Information Officer's designee. The State Controller may not authorize payment for data processing equipment, software or services without evidence of prior approval of the purchases by the commissioner or the Chief Information Officer or the Chief Information Officer's designee.

1. Noncompliance ~~defined~~. A state agency is in noncompliance with this chapter if the agency:

A. Purchases data processing equipment, software or services in noncompliance with this chapter; or

B. Fails to adhere to the data processing standards established by the commissioner and the Chief Information Officer or the Chief Information Officer's designee.

2. Penalty. Any state agency found to be in noncompliance as defined in this section is prohibited from acquiring or purchasing data processing equipment, software and services until the commissioner or the Chief Information Officer determines that the state agency is in compliance with this chapter.

Notwithstanding the provisions of this section, the commissioner or the Chief Information Officer may act to acquire or purchase data processing equipment, software and services to maintain or meet the emergency needs of a state agency.

3. Cybersecurity services. Notwithstanding the requirements of sections 1553 and 1825-B, or any other statutory or regulatory provisions to the contrary, the Chief Information Officer, after reasonable investigation, may procure cybersecurity services on a retainer basis when determined necessary to ensure the State is prepared to detect, prevent and respond to cyberattacks.