MAINE STATE LEGISLATURE

The following document is provided by the

LAW AND LEGISLATIVE DIGITAL LIBRARY

at the Maine State Law and Legislative Reference Library

http://legislature.maine.gov/lawlib

Reproduced from electronic originals

(may include minor formatting differences from printed original)

132nd MAINE LEGISLATURE

SECOND REGULAR SESSION-2026

Legislative Document **No. 2092**

H.P. 1407 House of Representatives, January 7, 2026

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

Submitted by the Department of Administrative and Financial Services pursuant to Joint Rule 203.

Reference to the Committee on State and Local Government suggested and ordered printed.

ROBERT B. HUNT
Clerk

Presented by Representative SALISBURY of Westbrook.

Printed on recycled paper

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 §1971, sub-§2, as enacted by PL 2005, c. 12, Pt. SS, §9, is amended to read:

2. Provide services. Direct and oversee the provision of information technology ~~and~~ enterprise services ~~in data processing and telecommunications~~ throughout State Government in a manner that prioritizes the confidentiality, integrity and availability of the information transacted, stored or processed by information and communications technology infrastructure, systems or services affecting the enterprise, whether physical or nonphysical.

Sec. 6. 5 MRSA §1972, sub-§2, as amended by PL 2005, c. 12, Pt. SS, §10, is further amended to read:

2. Chief Information Officer. "Chief Information Officer" means the person who holds the lead information technology position within the executive branch that directs, coordinates and oversees information technology policy making, planning, architecture and standardization. The Chief Information Officer is also responsible for the provision of information technology ~~and~~ enterprise services ~~in data processing and telecommunications~~ throughout State Government.

Sec. 7. 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. 8. 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. 9. 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. 10. 5 MRSA §1973, sub-§1, ¶A, as enacted by PL 2001, c. 388, §14, is amended to read:

A. Provide central leadership and vision in the use of information technology, information security and telecommunications technology on a statewide basis to safeguard the confidentiality, integrity and availability of the information transacted, stored or processed by information and communications technology infrastructure, systems or services affecting the enterprise or the State's critical infrastructure, whether physical or nonphysical;

Sec. 11. 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. 12. 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~~ information technology products, hardware, software and telecommunications services, equipment and systems by state agencies.

Sec. 13. 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~~ information technology, information security and enterprise services. 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~~ information technology, information security and enterprise services and for the implementation of these programs.

Sec. 14. 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~~ information technology enterprise services and telecommunications. The Chief Information Officer, or the Chief Information Officer's designee, shall develop and administer written standards for ~~data processing~~ information technology enterprise services 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. 15. 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~~ information technology equipment, hardware, 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~~ information technology equipment, hardware, software or services ~~without~~ that are out of compliance with the office's policies and procedures. All such purchases require 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~~ information technology equipment, hardware, 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~~ information technology equipment, hardware, software or services in noncompliance with this chapter; or

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

2. Penalty. ~~Any~~ A state agency found to be in noncompliance as ~~defined~~ described in this section is prohibited from acquiring or purchasing ~~data processing equipment,~~ information technology equipment, hardware, 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,~~ information technology equipment, hardware, 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.

Sec. 16. 5 MRSA §1981, first ¶, as enacted by PL 2005, c. 12, Pt. SS, §16, is amended to read:

The mission of the Office of Information Technology includes providing high-quality, responsive, cost-effective information technology services to the agencies, instrumentalities and political subdivisions of State Government to ensure the confidentiality, integrity and availability of the information transacted, stored or processed by information and communications technology infrastructure, systems or services affecting the enterprise, whether physical or nonphysical. These services include, but are not limited to, information security, cybersecurity, voice and data computer and networking services, applications development and maintenance and desktop support, centralized geographic information systems and data and security ~~advice to~~ services for customers.

Sec. 17. 5 MRSA §1981, sub-§2, as enacted by PL 2005, c. 12, Pt. SS, §16, is amended to read:

2. Duties of office. The office shall provide the ~~major data processing and telecommunications~~ information technology enterprise services in State Government, including computer operations and programming and applications systems. The office, as authorized by the commissioner, shall work to ensure consistency in programming services, stability in data processing functions, reliability in the operation and maintenance of systems throughout State Government and responsiveness and flexibility to react to changing situations and needs. The office shall establish information security and cybersecurity standards and policies to ensure the protection of information and communications technology infrastructure, systems and services affecting the enterprise, whether physical or nonphysical, against emerging cybersecurity risks and cyberattacks.

SUMMARY

This bill makes necessary technical changes to update the statutes governing the Department of Administrative and Financial Services, Office of Information Technology to align with recent statutory updates and best practices. The bill does the following.

1. It allows the Chief Information Officer to have an authorized designee in certain instances.

2. It includes certain definitions to align with the recently enacted definition of "cyberattack" and updates terminology to reflect national best practices for cybersecurity and information security.

3. It updates language regarding the mission of the office to reflect the bill's terminology changes.

4. It updates a provision of statute regarding competitive bidding to allow the office to procure information technology products or services necessary to detect, prevent and respond to cyberattacks.