

## CHAPTER 16E

### DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES

<p>16E.01 DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES.</p> <p>16E.015 DEFINITIONS.</p> <p>16E.016 RESPONSIBILITY FOR INFORMATION TECHNOLOGY SERVICES AND EQUIPMENT.</p> <p>16E.02 DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES; STRUCTURE AND PERSONNEL.</p> <p>16E.03 STATE INFORMATION AND COMMUNICATIONS SYSTEMS.</p> <p>16E.031 USER ACCEPTANCE TESTING.</p> <p>16E.036 ADVISORY COUNCIL.</p> <p>16E.04 INFORMATION AND TELECOMMUNICATIONS TECHNOLOGY POLICY.</p> <p>16E.05 GOVERNMENT INFORMATION ACCESS.</p> <p>16E.06 DATA PRIVACY.</p>	<p>16E.07 ONLINE GOVERNMENT INFORMATION SERVICES.</p> <p>16E.14 MNIT SERVICES REVOLVING FUND.</p> <p>16E.15 SOFTWARE SALES.</p> <p>16E.16 MODIFICATION OF OPERATING AND MANAGEMENT PROCEDURES.</p> <p>16E.17 TELECOMMUNICATION; POWERS.</p> <p>16E.18 STATE INFORMATION INFRASTRUCTURE.</p> <p>16E.19 ADMINISTRATION OF STATE COMPUTER FACILITIES.</p> <p>16E.21 INFORMATION AND TELECOMMUNICATIONS ACCOUNT.</p> <p>16E.30 GEOSPATIAL INFORMATION OFFICE.</p> <p>16E.35 COUNTY AND LOCAL CYBERSECURITY GRANTS.</p> <p>16E.36 CYBERSECURITY INCIDENTS.</p>
---	---

#### 16E.01 DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES.

Subdivision 1. **Creation; chief information officer.** The Department of Information Technology Services, which may also be known as Minnesota Information Technology Services or Minnesota IT Services, referred to in this chapter as the "department," is an agency in the executive branch headed by a commissioner, who also is the chief information officer. The appointment of the commissioner is subject to the advice and consent of the senate under section 15.066.

Subd. 1a. **Responsibilities.** The department shall provide oversight, leadership, and direction for information and telecommunications technology policy and the management, delivery, accessibility, and security of executive branch information and telecommunications technology systems and services in Minnesota. The department shall partner with executive branch state agencies to manage strategic investments in information and telecommunications technology systems and services to ensure sufficient access to and efficient delivery of accessible government services and to maximize benefits for the state government as an enterprise.

Subd. 1b. **Deputy; appointments.** The commissioner may appoint a deputy, assistant commissioners, and a confidential secretary. Each serves at the commissioner's pleasure in the unclassified service.

Subd. 2. **Discretionary powers.** The department may:

(1) enter into contracts for goods or services with public or private organizations and charge fees for services it provides;

(2) apply for, receive, and expend money from public agencies;

(3) apply for, accept, and disburse grants and other aids from the federal government and other public or private sources;

(4) enter into contracts with agencies of the federal government, local governmental units, the University of Minnesota and other educational institutions, and private persons and other nongovernmental organizations as necessary to perform its statutory duties;

(5) sponsor and conduct conferences and studies, collect and disseminate information, and issue reports relating to information and communications technology issues;

(6) review the technology infrastructure of regions of the state and cooperate with and make recommendations to the governor, legislature, state agencies, local governments, local technology development agencies, the federal government, private businesses, and individuals for the realization of information and communications technology infrastructure development potential;

(7) sponsor, support, and facilitate innovative and collaborative economic and community development and government services projects or initiatives, including technology initiatives related to culture and the arts, with public and private organizations; and

(8) review and recommend alternative sourcing strategies for state information and communications systems.

Subd. 3. **Duties.** (a) The department shall:

(1) manage the efficient and effective use of available federal, state, local, and public-private resources to develop statewide information and telecommunications technology systems and services and its infrastructure;

(2) approve state agency and intergovernmental information and telecommunications technology systems and services development efforts involving state or intergovernmental funding, including federal funding, provide information to the legislature regarding projects and initiatives reviewed, and recommend projects and initiatives for inclusion in the governor's budget under section 16A.11;

(3) promote cooperation and collaboration among state and local governments in developing intergovernmental information and telecommunications technology systems and services;

(4) cooperate and collaborate with the legislative and judicial branches in the development of information and communications systems in those branches, as requested;

(5) continue to collaborate on the development of MN.gov, the state's official comprehensive online service and information initiative;

(6) manage and promote the regular and periodic reinvestment in the information and telecommunications technology systems and services infrastructure so that state and local government agencies can effectively and efficiently serve their customers;

(7) facilitate the cooperative development of and ensure compliance with standards and policies for information and telecommunications technology systems and services and electronic data practices and security within the executive branch;

(8) eliminate unnecessary duplication of existing information and telecommunications technology systems and services provided by state agencies;

(9) identify, sponsor, develop, and execute shared information and telecommunications technology projects and initiatives, and ongoing operations;

(10) ensure overall security of the state's information and technology systems and services; and

(11) manage and direct compliance with accessibility standards for informational technology, including hardware, software, websites, online forms, and online surveys.

(b) The chief information officer, in consultation with the commissioner of management and budget, must determine when it is cost-effective for agencies to develop and use shared information technology systems, platforms, and services for the delivery of digital government services. The chief information officer may require agencies to use shared information and telecommunications technology systems and services. The chief information officer shall establish reimbursement rates in cooperation with the commissioner of management and budget to be billed to agencies and other governmental entities sufficient to cover the actual development, operating, maintenance, and administrative costs of the shared systems. The methodology for billing may include the use of interagency agreements, or other means as allowed by law.

(c) A state agency that has an information and telecommunications technology project or initiative, whether funded as part of the biennial budget or by any other means, shall register with the department by submitting basic project or initiative startup documentation as specified by the chief information officer in both format and content. State agency business and technology project leaders, in accordance with policies and standards set forth by the chief information officer, must demonstrate that the project or initiative will be properly managed, ensure alignment with enterprise technology strategic direction, provide updates to the project or initiative documentation as changes are proposed, and regularly report on the current status of the project or initiative on a schedule agreed to with the chief information officer. The chief information officer has the authority to define a project or initiative for the purposes of this chapter.

(d) The chief information officer shall monitor progress on active information and telecommunications technology projects and initiatives and report on the performance of the projects or initiatives in comparison with plans in terms of time, scope, and budget. The chief information officer may conduct an independent audit of the project or initiative. If an independent audit is conducted, the audit analysis and evaluation of the project or initiative must be presented to agency executive sponsors, the project governance bodies, and the chief information officer. All reports and responses must become part of the project or initiative record.

(e) For any active information and telecommunications technology project or initiative, with a total expected cost of more than \$10,000,000, an annual independent audit that conforms to published audit principles adopted by the department must be conducted.

(f) The chief information officer shall report by January 15 of each year to the chairs and ranking minority members of the legislative committees and divisions with jurisdiction over the department on the status of the state's comprehensive project and initiatives portfolio. The report must include descriptions of each project and its current status, information technology costs associated with the project, and estimated date on when the information technology project is expected to be completed.

**History:** 1997 c 202 art 3 s 7; 1998 c 366 s 41; 1999 c 250 art 1 s 68; 1Sp2003 c 1 art 2 s 58; 2005 c 156 art 5 s 6,7; 2008 c 318 art 1 s 8; 2009 c 101 art 2 s 109; 2009 c 131 s 4,5; 2013 c 134 s 21,30; 2013 c 142 art 3 s 36; 2014 c 271 art 4 s 1; 2021 c 31 art 2 s 2; 2023 c 62 art 6 s 6-8; 2024 c 123 art 17 s 14,15

### 16E.015 DEFINITIONS.

Subdivision 1. **Applicability.** For the purposes of this chapter, the following terms have the meanings given them.

Subd. 2. **Accessibility; accessible.** "Accessibility" and "accessible" are defined by the accessibility standards developed and required under section 16E.03.

Subd. 3. **Infrastructure hardware.** "Infrastructure hardware" means servers, routers, switches, and non-end-user platform devices and their operating systems.

Subd. 3a. **State information network.** "State information network" means optical fiber facilities and terminal equipment used in the delivery of high-speed telecommunications services.

Subd. 4. **Undue burden.** "Undue burden" means significant difficulty or expense determined and documented by the funding agency, including but not limited to difficulty or expense associated with technical feasibility.

**History:** 2009 c 131 s 6; 2013 c 134 s 22

#### **16E.016 RESPONSIBILITY FOR INFORMATION TECHNOLOGY SERVICES AND EQUIPMENT.**

(a) The chief information officer is responsible for providing or entering into managed services contracts for the provision, improvement, development, and lifecycle management of the following information technology systems and services to state agencies:

- (1) state data centers;
- (2) mainframes including system software;
- (3) servers including system software;
- (4) desktops including system software;
- (5) laptop computers including system software;
- (6) a data network including system software;
- (7) database, electronic mail, office systems, reporting, and other standard software tools;
- (8) business application software and related technical support services;
- (9) help desk for the components listed in clauses (1) to (8);
- (10) maintenance, problem resolution, and break-fix for the components listed in clauses (1) to (8);
- (11) regular upgrades, replacement, and lifecycle management for the components listed in clauses (1) to (8); and
- (12) network-connected output devices.

(b) All state agency employees whose work primarily involves functions specified in paragraph (a) are employees of the Department of Information Technology Services. This includes employees who directly perform the functions in paragraph (a), as well as employees whose work primarily involves managing, supervising, or providing administrative services or support services to employees who directly perform these functions. The chief information officer may assign employees of the department to perform work exclusively for another state agency.

(c) Subject to sections 16C.08 and 16C.09, the chief information officer may allow a state agency to obtain services specified in paragraph (a) through a contract with an outside vendor when the chief information officer and the agency head agree that a contract would provide best value, as defined in section 16C.02, under the service-level agreement. The chief information officer must require that agency contracts with outside vendors ensure that systems and services are compatible with standards established by the Department of Information Technology Services.

(d) The Minnesota State Retirement System, the Public Employees Retirement Association, the Teachers Retirement Association, the State Board of Investment, the Campaign Finance and Public Disclosure Board, the State Lottery, and the Statewide Radio Board are not state agencies for purposes of this section.

**History:** *1Sp2011 c 10 art 4 s 2; 2013 c 134 s 30; 2013 c 142 art 3 s 36; 2021 c 31 art 2 s 3; 2023 c 62 art 6 s 9*

## **16E.02 DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES; STRUCTURE AND PERSONNEL.**

Subdivision 1. **Department management and structure.** (a) The chief information officer is appointed by the governor. The chief information officer serves in the unclassified service at the pleasure of the governor. The chief information officer must have experience leading enterprise-level information technology organizations. The chief information officer is the state's chief information officer and information and telecommunications technology adviser to the governor.

(b) The chief information officer may appoint other employees of the department. Staff of the department must include individuals knowledgeable in information and telecommunications technology systems and services and individuals with specialized training in information security and accessibility.

Subd. 1a. **Accountability.** The chief information officer reports to the governor. The chief information officer must consult regularly with executive branch agency commissioners on technology projects, standards, and services as well as management of resources and staff utilization.

Subd. 2. [Repealed, 2014 c 271 art 4 s 7]

Subd. 3. [Repealed, 2014 c 271 art 4 s 7]

**History:** *1997 c 202 art 3 s 8; 1999 c 250 art 1 s 69; 2000 c 260 s 8; 2005 c 156 art 5 s 8; 2009 c 101 art 2 s 109; 2009 c 131 s 7; 2010 c 392 art 1 s 7; 2013 c 134 s 30; 2013 c 142 art 3 s 36; 2021 c 31 art 2 s 4*

## **16E.03 STATE INFORMATION AND COMMUNICATIONS SYSTEMS.**

Subdivision 1. **Definitions.** (a) For the purposes of this chapter, the following terms have the meanings given them.

(b) "Information and telecommunications technology systems and services" means all computing and telecommunications hardware and software, the activities undertaken to secure that hardware and software, and the activities undertaken to acquire, transport, process, analyze, store, and disseminate information electronically. "Information and telecommunications technology systems and services" includes all proposed expenditures for computing and telecommunications hardware and software, security for that hardware and software, and related consulting or other professional services.

(c) "Telecommunications" means voice, video, and data electronic transmissions transported by wire, wireless, fiber-optic, radio, or other available transport technology.

(d) "Cyber security" means the protection of data and systems in networks connected to the Internet.

(e) "State agency" means an agency in the executive branch of state government and includes the Minnesota Office of Higher Education, but does not include the Minnesota State Colleges and Universities unless specifically provided elsewhere in this chapter.

(f) "Total expected project cost" includes direct staff costs, all supplemental contract staff and vendor costs, and costs of hardware and software development or purchase. Breaking a project into several phases does not affect the cost threshold, which must be computed based on the full cost of all phases.

(g) "Cloud computing" has the meaning described by the National Institute of Standards and Technology of the United States Department of Commerce in special publication 800-145, September 2011.

**Subd. 2. Chief information officer's responsibility.** The chief information officer shall:

(1) design a strategic plan for information and telecommunications technology systems and services in the state and shall report on the plan to the governor and legislature at the beginning of each regular session;

(2) develop and implement processes for review, approval, and monitoring and oversee the state's information and telecommunications technology systems and services;

(3) establish and enforce compliance with standards for information and telecommunications technology systems and services that are cost-effective and support open systems environments and that are compatible with state, national, and international standards, including accessibility standards;

(4) maintain a library of systems and programs developed by the state for use by agencies of government;

(5) direct and manage the shared operations of the state's information and telecommunications technology systems and services; and

(6) establish and enforce standards and ensure acquisition of hardware, software, and services necessary to protect data and systems in state agency networks connected to the Internet.

**Subd. 3. Evaluation and approval.** A state agency may not undertake an information and telecommunications technology project or initiative until it has been evaluated according to the procedures developed under subdivision 4. The chief information officer or delegate shall record project approval as a part of the project.

**Subd. 4. Evaluation procedure.** The chief information officer shall establish and, as necessary, update and modify procedures to evaluate information and communications projects or initiatives proposed by state agencies. The evaluation procedure must assess the necessity, design and plan for development, ability to meet user requirements, accessibility, feasibility, cost, and benefits of the project or initiative.

**Subd. 4a. Cloud computing services.** The project evaluation procedure required by subdivision 4 must include a review of cloud computing service options, including any security benefits and cost savings associated with purchasing those service options from a cloud computing service provider. When projects involve cloud computing services, the state chief information officer shall, in consultation with the Technology Advisory Council, establish metrics to assess the progress of any cloud computing project for each state agency.

**Subd. 5. Report to legislature.** The chief information officer shall submit to the legislature, at the same time as the governor's budget required by section 16A.11, a concise narrative explanation of any information and communication technology project or initiative being proposed as part of the governor's budget that involves collaboration between state agencies and an explanation of how the budget requests of the several agencies collaborating on the project or initiative relate to each other.

**Subd. 5a. Cloud computing progress report.** (a) No later than January 15, 2024, and annually thereafter, the state chief information officer shall, in consultation with the Technology Advisory Council, report on the progress of executive branch cloud adoption to the chairs and ranking members of the legislative

committees with jurisdiction over executive branch information technology policy. The report shall include, but not be limited to, the following:

(1) an accounting of each state agency's expenditures for cloud computing initiatives and software as service solutions; and

(2) cost projections, timelines, and the names of any cloud provider selected for current computing projects that incorporate cloud computing solutions, and percentage of total cloud use.

(b) This subdivision expires December 31, 2027.

**Subd. 6. System development methods.** The chief information officer shall establish and, as necessary, update and modify methods for developing information and communications systems appropriate to the specific needs of individual state agencies. The development methods shall be used to define the design, programming, and implementation of systems.

**Subd. 7. Cyber security systems.** (a) In consultation with the attorney general and appropriate agency heads, the chief information officer shall develop cyber security policies, guidelines, and standards, and shall advise, implement, and administer state data security solutions and practices on the state's information technology services, systems, and applications consistent with these policies, guidelines, standards, and state law to ensure the integrity, confidentiality, and availability of information technology systems and services, and data and to ensure applicable limitations on access to data, consistent with the public's right to know as defined in chapter 13. The chief information officer is responsible for overall security of state agency networks connected to the Internet. Each department or agency head is responsible for the security of the department's or agency's data within the guidelines of established enterprise policy.

(b) The state chief information officer, or state chief information security officer, may advise and consult on security strategy and programs for state entities and political subdivisions not subject to section 16E.016.

**Subd. 8.** [Repealed, 2014 c 271 art 4 s 7]

**Subd. 9. Accessibility standards.** (a) The chief information officer shall develop accessibility standards applicable to technology, software, and hardware procurement, with the exception of infrastructure hardware. The standards shall not impose an undue burden on the state.

(b) The chief information officer shall require state agencies to adhere to the standards developed under this subdivision unless an exception is approved pursuant to subdivision 10. Except as provided in paragraph (c), the standards developed under this section must incorporate section 508 of the Rehabilitation Act, United States Code, title 29, section 794d, as amended by the Workforce Investment Act of 1998, Public Law 105-220, August 7, 1998, and the Web Content Accessibility Guidelines, 2.0. The chief information officer must review subsequent revisions to section 508 of the Rehabilitation Act and to the Web Content Accessibility Guidelines and may incorporate the revisions in the accessibility standards.

(c) If the chief information officer determines that any standard developed under this subdivision poses an undue burden to the state, the chief information officer may modify the burdensome standard, provided written findings and rationale are made explaining the deviation.

**Subd. 10. Exceptions to accessibility standards.** Exceptions to the standards may be granted by the chief information officer based upon a request by an agency.

Subd. 11. **Technical support to legislature.** The chief information officer, or a designee, must provide technical support to assist the legislature to comply with accessibility standards under section 3.199, subdivision 2. Support under this subdivision must include:

- (1) clarifying the requirements of the accessibility standards;
- (2) providing templates for common software applications used in developing documents used by the legislature;
- (3) assisting the development of training for staff to comply with the accessibility standards and assisting in providing the training; and
- (4) assisting the development of technical applications that enable legislative documents to be fully accessible.

The chief information officer must provide these services at no cost to the legislature.

**History:** 1997 c 202 art 3 s 9; 1997 c 212 s 3,4; 1998 c 359 s 15; 1998 c 366 s 42-45; 1999 c 250 art 1 s 114; 2005 c 107 art 2 s 60; 2005 c 156 art 5 s 9-12,23; 2008 c 318 art 1 s 9; 2009 c 101 art 2 s 109; 2009 c 131 s 8-11; 2014 c 271 art 4 s 2; 2019 c 50 art 1 s 11,12; 1Sp2019 c 10 art 5 s 2-4; 2021 c 31 art 2 s 5-8; 2023 c 62 art 6 s 10-12; 2024 c 123 art 17 s 16-20

#### **16E.031 USER ACCEPTANCE TESTING.**

Subdivision 1. **Applicability.** As used in this section:

- (1) "primary user" means an employee or agent of a state agency or local unit of government who uses an information technology business software application to perform an official function; and
- (2) "local unit of government" does not include a school district.

Subd. 2. **User acceptance testing.** (a) A state agency implementing a new information technology business software application or new business software application functionality that significantly impacts the operations of a primary user must provide opportunities for user acceptance testing, unless the testing is deemed not feasible or necessary by the relevant agency commissioner, in consultation with the chief information officer and representatives of the primary user.

(b) The requirements in paragraph (a) do not apply to routine software upgrades or application changes that are primarily intended to comply with federal law, rules, or regulations.

**History:** 2019 c 62 s 1

**16E.035** MS 2022 [Repealed, 2024 c 123 art 17 s 31]

#### **16E.036 ADVISORY COUNCIL.**

(a) The Technology Advisory Council is created to advise the governor, the executive branch, and the state chief information officer. The council shall consist of 15 voting members. The governor shall appoint six members who are individuals actively involved in business planning for state executive branch agencies, one county member designated by the Association of Minnesota Counties, one member appointed by the governor as a representative of a union that represents state information technology employees, and one member appointed by the governor to represent private businesses. The governor shall also select six additional members with private-sector or public-sector information technology experience or experience



in academia pertaining to information technology. The council shall have the following four ex-officio nonvoting members:

- (1) a member of the house of representatives selected by the speaker of the house;
- (2) a member of the house of representatives selected by the minority leader of the house of representatives;
- (3) a member of the senate selected by the majority leader of the senate; and
- (4) a member of the senate selected by the minority leader of the senate.

The governor shall designate one of the 15 voting members to serve as the council's chair.

(b) Membership terms, removal of members, and filling of vacancies are as provided in section 15.059. Members do not receive compensation or reimbursement for expenses.

(c) The chief information officer shall provide administrative support to the council.

(d) The council shall advise the chief information officer on:

- (1) development and implementation of the state information technology strategic plan;
- (2) critical information technology initiatives for the state;
- (3) standards for state information architecture;
- (4) identification of business and technical needs of state agencies;
- (5) strategic information technology portfolio management, project prioritization, and investment decisions;
- (6) the department's performance measures and fees for service agreements with executive branch agencies;
- (7) management of the state MNIT services revolving fund; and
- (8) the efficient and effective operation of the department.

**History:** *1Sp2011 c 10 art 4 s 3; 2013 c 134 s 30; 2013 c 142 art 3 s 36; 2021 c 31 art 2 s 9,16*

#### **16E.04 INFORMATION AND TELECOMMUNICATIONS TECHNOLOGY POLICY.**

Subdivision 1. **Development.** The office shall develop, establish, and enforce policies and standards for state agencies to follow in developing and purchasing information and telecommunications technology systems and services and training appropriate persons in their use. The office shall develop, promote, and manage state technology, architecture, standards and guidelines, information needs analysis techniques, contracts for the purchase of equipment and services, and training of state agency personnel on these issues.

Subd. 2. **Responsibilities.** (a) The office may develop and establish a state information architecture to ensure:

- (1) that state agency information and communications systems, equipment, and services do not needlessly duplicate or conflict with the systems of other agencies; and

(2) enhanced public access to data can be provided consistent with standards developed under section 16E.05, subdivision 4.

When state agencies have need for the same or similar public data, the chief information officer, in coordination with the affected agencies, shall manage the most efficient and cost-effective method of producing and storing data for or sharing data between those agencies. The development of this information architecture must include the establishment of standards and guidelines to be followed by state agencies. The office shall ensure compliance with the architecture.

(b) The office shall review and approve agency requests for funding for the development or purchase of information systems equipment or software before the requests may be included in the governor's budget.

(c) The office may review and approve agency requests for grant funding that have an information and technology component.

(d) The office shall review major purchases of information systems equipment to:

(1) ensure that the equipment follows the standards and guidelines of the state information architecture;

(2) ensure the agency's proposed purchase reflects a cost-effective policy regarding volume purchasing; and

(3) ensure that the equipment is consistent with other systems in other state agencies so that data can be shared among agencies, unless the office determines that the agency purchasing the equipment has special needs justifying the inconsistency.

(e) The office shall review the operation of information systems by state agencies and ensure that these systems are operated efficiently and securely and continually meet the standards and guidelines established by the office. The standards and guidelines must emphasize uniformity that is cost-effective for the enterprise, that encourages information interchange, open systems environments, and portability of information whenever practicable and consistent with an agency's authority and chapter 13.

**Subd. 3. Risk assessment and mitigation.** (a) A risk assessment and risk mitigation plan are required for all information systems development projects or initiatives undertaken by a state agency in the executive or judicial branch or by a constitutional officer. The chief information officer must contract with an entity outside of state government to conduct the initial assessment and prepare the mitigation plan for a project or initiative estimated to cost more than \$10,000,000. The outside entity conducting the risk assessment and preparing the mitigation plan must not have any other direct or indirect financial interest in the project or initiative. The risk assessment and risk mitigation plan must provide for periodic monitoring by the commissioner until the project or initiative is completed.

(b) The risk assessment and risk mitigation plan must be paid for with money appropriated for the information and telecommunications technology project or initiative.

**History:** 1997 c 202 art 3 s 10; 1999 c 250 art 1 s 114; 2000 c 488 art 12 s 17; 2001 c 7 s 11; 1Sp2001 c 10 art 2 s 45; 2005 c 156 art 5 s 13; 2008 c 318 art 1 s 10; 2009 c 101 art 2 s 109; 2010 c 392 art 1 s 8; 1Sp2011 c 10 art 4 s 4; 2013 c 134 s 23; 2014 c 271 art 4 s 4; 2021 c 31 art 2 s 10; 2024 c 123 art 17 s 21,22

**16E.0465** Subdivision 1. MS 2022 [Repealed, 2024 c 123 art 17 s 31]

Subd. 2. MS 2022 [Repealed, 2024 c 123 art 17 s 31]

Subd. 3. [Repealed, 2005 c 156 art 5 s 24]

**16E.0466** Subdivision 1. MS 2020 [Repealed, 2021 c 31 art 2 s 17]

Subd. 2. MS 2022 [Repealed, 2023 c 62 art 6 s 17]

**16E.0475** [Repealed, 2014 c 271 art 4 s 7; 2014 c 286 art 1 s 5]

### **16E.05 GOVERNMENT INFORMATION ACCESS.**

Subdivision 1. **Duties.** The department, in consultation with interested persons, shall explore ways and means to improve citizen and business access to public services, including implementation of technological improvements.

Subd. 2. **Approval of state agency initiatives.** A state agency shall coordinate with the office when implementing a new initiative for providing electronic access to state government information.

Subd. 3. MS 2020 [Repealed, 2021 c 31 art 2 s 17]

Subd. 4. **Standards for transparency.** The chief information officer, in consultation with the Information Policy Analysis Division of the Department of Administration, shall develop standards to enhance public access to electronic data maintained by state government, consistent with the requirements of chapter 13. The standards must ensure that:

- (1) the state information architecture facilitates public access to agency data;
- (2) publicly available data is managed using an approved state metadata model; and
- (3) all geospatial data conform to an approved state geocode model.

**History:** 1997 c 202 art 3 s 11; 2010 c 392 art 1 s 9; 2014 c 271 art 4 s 5; 2021 c 31 art 2 s 12

**16E.055** MS 2022 [Repealed, 2024 c 123 art 17 s 31]

### **16E.06 DATA PRIVACY.**

The following data submitted to the office by businesses are private data on individuals or nonpublic data: financial statements, business plans, income and expense projections, customer lists, and market and feasibility studies not paid for with public funds.

**History:** 1997 c 202 art 3 s 12

### **16E.07 ONLINE GOVERNMENT INFORMATION SERVICES.**

Subdivision 1. **Definition.** (a) The definition in this subdivision applies to this section.

(b) "Government unit" means a state department, agency, commission, council, board, task force, or committee; a constitutional office; a court entity; the Minnesota State Colleges and Universities; a county, statutory or home rule charter city, or town; a school district; a special district; or any other board, commission, district, or authority created under law, local ordinance, or charter provision.

Subd. 2. **Established.** The department shall collaborate with state agencies to maintain MN.gov and associated websites that provide online government information services.

Subd. 3. **Access to data.** The legislature determines that the greatest possible access to certain government information and data is essential to allow citizens to participate fully in a democratic system of government. Certain information and data, including, but not limited to the following, must be provided free of charge or for a nominal cost associated with reproducing the information or data:

(1) directories of government services and institutions;

(2) legislative and rulemaking information, including an electronic version of the State Register, public information newsletters, bill text and summaries, bill status information, rule status information, meeting schedules, and the text of statutes and rules;

(3) supreme court and court of appeals opinions and general judicial information;

(4) opinions of the attorney general;

(5) Campaign Finance and Public Disclosure Board and election information;

(6) public budget information;

(7) local government documents, such as codes, ordinances, minutes, meeting schedules, and other notices in the public interest;

(8) official documents, releases, speeches, and other public information issued by government agencies; and

(9) the text of other government documents and publications that government agencies determine are important to public understanding of government activities.

Subd. 4. MS 2022 [Repealed by amendment, 2024 c 123 art 17 s 23]

Subd. 5. MS 2022 [Repealed by amendment, 2024 c 123 art 17 s 23]

Subd. 6. **Fees.** The office may establish fees for technical and transaction services for government units. The office may not charge a fee for viewing or inspecting data made available through MN.gov or linked facilities, unless specifically authorized by law.

Subd. 7. **Online government information service account.** The online government information service account is created in the special revenue fund. The account consists of:

(1) grants received from nonstate entities;

(2) fees and charges collected by the office;

(3) gifts, donations, and bequests made to the office; and

(4) other money credited to the account by law.

Money in the account is appropriated to the office to be used to continue the development of online government information services.

Subd. 8. **Secure transaction system.** The office shall plan and develop secure transaction systems to support delivery of government services electronically. A state agency that implements electronic government services for fees, licenses, sales, or other purposes may be required to use secure transaction systems developed in accordance with this section.

Subd. 9. **Aggregation of service demand.** The office may identify opportunities to aggregate demand for technical services required by government units for online activities and may contract with governmental or nongovernmental entities to provide services. These contracts are not subject to the requirements of chapters 16B and 16C, except sections 16C.04, 16C.08, and 16C.09.

Subd. 10. **Outreach.** The office may promote the availability of government online information and services through public outreach and education.

Subd. 11. MS 2022 [Repealed by amendment, 2024 c 123 art 17 s 23]

Subd. 12. **Private entity services; fee authority.** (a) The department may enter into a contract with a private entity to manage, maintain, support, and expand online government information services to citizens and businesses.

(b) A contract established under paragraph (a) may provide for compensation of the private entity through a fee established under paragraph (c).

(c) The department, subject to the approval of the agency or department responsible for the data or services involved in the transaction, may charge and may authorize a private entity that enters into a contract under paragraph (a) to charge a convenience fee for users of online government information services up to a total of \$2 per transaction, provided that no fee shall be charged for viewing or inspecting data. A fee established under this paragraph is in addition to any fees or surcharges authorized under other law.

(d) Receipts from the convenience fee shall be deposited in the online government information service account established in subdivision 7. Notwithstanding section 16A.1285, subdivision 2, receipts credited to the account are appropriated to the department for payment to the contracted private entity under paragraph (a). In lieu of depositing the receipts in the online government information service account, the department can directly transfer the receipts to the private entity or allow the private entity to retain the receipts pursuant to a contract established under this subdivision.

(e) Information regarding any convenience fee receipts collected under paragraph (d) must be reported to the chairs and ranking minority members of the house of representatives and senate committees with jurisdiction over state government finance by January 15 of each odd-numbered year.

**History:** 1997 c 202 art 2 s 63; art 3 s 13; 1998 c 366 s 46; 1998 c 386 art 2 s 15; 1999 c 250 art 1 s 114; 1Sp2003 c 1 art 2 s 59; 2005 c 156 art 5 s 17,23; 2009 c 131 s 13; 2013 c 142 art 3 s 24; 2021 c 31 art 2 s 13; 2024 c 123 art 17 s 23

**16E.071** MS 2020 [Repealed, 2021 c 31 art 2 s 17]

**16E.08** [Repealed, 1Sp2001 c 10 art 2 s 102]

**16E.09** [Repealed, 1Sp2003 c 1 art 2 s 136]

**16E.11** [Repealed, 1999 c 250 art 1 s 115]

**16E.12** [Repealed, 1999 c 250 art 1 s 115]

**16E.13** [Repealed, 1999 c 250 art 1 s 115]

#### **16E.14 MNIT SERVICES REVOLVING FUND.**

Subdivision 1. **Creation.** The MNIT services revolving fund is created in the state treasury.

Subd. 2. **Appropriation and uses of fund.** Money in the MNIT services revolving fund is appropriated annually to the chief information officer to operate information and telecommunications services, including management, consultation, and design services.

Subd. 3. **Reimbursements.** Except as specifically provided otherwise by law, each agency shall reimburse the MNIT services revolving fund for the cost of all services, supplies, materials, labor, and depreciation of equipment, including reasonable overhead costs, which the chief information officer is authorized and directed to furnish an agency. The chief information officer shall report the rates to be charged for the revolving fund no later than July 1 each year to the chair of the committee or division in the senate and house of representatives with primary jurisdiction over the budget of the Department of Information Technology Services.

Subd. 4. **Cash flow.** (a) The commissioner of management and budget shall make appropriate transfers to the revolving fund when requested by the chief information officer. The chief information officer may make allotments and encumbrances in anticipation of such transfers. In addition, the chief information officer, with the approval of the commissioner of management and budget, may require an agency to make advance payments to the revolving fund sufficient to cover the office's estimated obligation for a period of at least 60 days. All reimbursements and other money received by the chief information officer under this section must be deposited in the MNIT services revolving fund.

(b) Each biennium, the commissioner of management and budget is authorized to provide cash flow assistance of up to \$60,000,000 from the special revenue fund or other statutory general fund as defined in section 16A.671, subdivision 3, paragraph (a), to the Department of Information Technology Services for the purpose of managing revenue and expenditure differences. These funds shall be repaid with interest by the end of the closing period of the second fiscal year of the same biennium.

Subd. 5. **Liquidation.** If the MNIT services revolving fund is abolished or liquidated, the total net profit from the operation of the fund must be distributed to the various funds from which purchases were made. The amount to be distributed to each fund must bear to the net profit the same ratio as the total purchases from each fund bears to the total purchases from all the funds during the same period of time.

**History:** 2005 c 156 art 5 s 18; 2009 c 101 art 2 s 109; 2013 c 134 s 30; 2013 c 142 art 3 s 36; 2021 c 31 art 2 s 16; 2023 c 62 art 6 s 13

**16E.145** MS 2020 [Repealed, 2021 c 31 art 2 s 17]

## **16E.15 SOFTWARE SALES.**

Subdivision 1. **Authorization.** The chief information officer may sell or license computer software products or services developed by state agencies or custom developed by a vendor, through whatever sales method the chief information officer considers appropriate. Prices for the software products or services may be based on market considerations.

Subd. 2. **Software sale fund.** (a) Except as provided in paragraphs (b) and (c), proceeds from the sale or licensing of software products or services by the chief information officer must be credited to the MNIT services revolving fund. If a state agency other than the Department of Information Technology Services has contributed to the development of software sold or licensed under this section, the chief information officer may reimburse the agency by discounting computer services provided to that agency.

(b) Proceeds from the sale or licensing of software products or services developed by the Pollution Control Agency, or custom developed by a vendor for the agency, must be credited to the environmental fund.

(c) If the Department of Transportation develops software products or services using trunk highway funds, proceeds from the subsequent sale or licensing of the software products or services must be credited to the trunk highway fund. This paragraph also applies to software products or services custom developed by a vendor for the department using trunk highway funds.

**History:** 1987 c 365 s 12; 1990 c 506 art 2 s 12; 1991 c 199 art 1 s 6; 1995 c 220 s 27; 1999 c 205 art 4 s 1; 2003 c 130 s 12; 2005 c 156 art 5 s 23; 2007 c 100 s 1; 2011 c 97 s 1; 2013 c 134 s 30; 2013 c 142 art 3 s 36; 2015 c 75 art 2 s 2; 2021 c 31 art 2 s 16

#### **16E.16 MODIFICATION OF OPERATING AND MANAGEMENT PROCEDURES.**

When improved program effectiveness, better use of services, and greater efficiency and economy in state government can be demonstrated, the chief information officer with the approval of the governor may require a state agency to adjust its operating and management procedures to take advantage of improved systems, procedures, and methods resulting from systems analysis and information science technology.

**History:** 1984 c 544 s 49; 2005 c 156 art 5 s 23

#### **16E.17 TELECOMMUNICATION; POWERS.**

The chief information officer shall supervise and control all state telecommunication facilities and services, including any transmission, emission, or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic systems. Nothing in this section or section 16E.18 modifies, amends, or abridges any powers and duties presently vested in or imposed upon the commissioner of transportation or the commissioner of public safety relating to telecommunications facilities or the commissioner of transportation relating only to radio air navigation facilities or other air navigation facilities.

**History:** 1984 c 544 s 51; 1999 c 250 art 1 s 60; 2005 c 156 art 5 s 23

#### **16E.18 STATE INFORMATION INFRASTRUCTURE.**

Subdivision 1. **Policy.** (a) The state through its departments and agencies shall seek ways to meet its telecommunications needs in a manner that will help to promote investment and growth of the private sector information infrastructure throughout the state.

(b) The chief information officer shall ensure that telecommunications services are acquired in a manner that:

(1) promotes the availability of technologies with statewide high-speed or advanced telecommunications capability for both public and private customers in a reasonable and timely fashion;

(2) enables the cost-effective provision of telecommunications services to the entities identified in this section;

(3) uses standards-based open, interoperable networks to the extent practicable;

(4) promotes fair and open competition in the delivery of telecommunications services;

(5) allows effective state information infrastructure network management, responsiveness, and fault protection;

(6) provides networkwide security and confidentiality as appropriate for promoting public safety, health, and welfare; and

(7) meets performance standards that are reasonable and necessary.

(c) The state may purchase, own, or lease customer premises equipment. Customer premises equipment consists of terminal and associated equipment and inside wire located at an end user's premises and connected with communication channels at the point established in a building or a complex to separate customer equipment from the network. Customer premises equipment also includes, but is not limited to, communications devices eligible for distribution to communications impaired persons under section 237.51, subdivision 1.

(d) This section does not prohibit the chief information officer or other governmental entity from owning, leasing, operating, and staffing a network operation center that allows the chief information officer to test, troubleshoot, and maintain network operations.

**Subd. 2. Creation.** Except as provided in subdivision 4, the chief information officer, through the state information infrastructure, shall arrange for the provision of information technology and telecommunications services to state agencies. The state information infrastructure may also serve educational institutions, including public schools as defined in section 120A.05, subdivisions 9, 11, 13, and 17, nonpublic, church or religious organization schools that provide instruction in compliance with sections 120A.22, 120A.24, and 120A.41, and private colleges; public corporations; Indian tribal governments; state political subdivisions; and public noncommercial educational television broadcast stations as defined in section 129D.12, subdivision 2. It is not a telephone company for purposes of chapter 237. The chief information officer may purchase, own, or lease any telecommunications network facilities or equipment after first seeking bids or proposals and having determined that the private sector cannot, will not, or is unable to provide these services, facilities, or equipment as bid or proposed in a reasonable or timely fashion consistent with policy set forth in this section. The chief information officer shall not resell or sublease any services or facilities to nonpublic entities except to serve private schools and colleges. The chief information officer has the responsibility for planning, development, and operations of the state information infrastructure in order to provide cost-effective telecommunications transmission services to state information infrastructure users consistent with the policy set forth in this section.

**Subd. 3. Duties.** (a) The chief information officer shall:

(1) arrange for information technology and telecommunications services to the state and to political subdivisions through an account in the MNIT services revolving fund;

(2) manage vendor relationships, network function, and capacity planning in order to be responsive to the needs of the state information infrastructure users;

(3) set rates and fees for services;

(4) approve contracts for services, facilities, or equipment relating to the system;

(5) develop a system plan and the annual program and fiscal plans for the system; and

(6) in consultation with the commissioner of education in regard to schools, assist state agencies, political subdivisions of the state, and higher education institutions, including private colleges and public and private schools, to identify their telecommunication needs, and develop plans for interoperability of the network consistent with the policies in subdivision 1, paragraphs (a) and (b). When requested, the chief information officer may also assist in identifying, purchasing, or leasing their customer premises equipment.

(b) The chief information officer may purchase, own, or lease any telecommunications network facilities or equipment after first seeking bids or proposals and having determined that the private sector cannot, will



not, or is unable to provide these services, facilities, or equipment as bid or proposed in a reasonable and timely fashion consistent with the policy set forth in this section.

**Subd. 4. Program participation.** The chief information officer may require the participation of state agencies and the commissioner of education, and may request the participation of the Board of Regents of the University of Minnesota and the Board of Trustees of the Minnesota State Colleges and Universities, in the planning and implementation of the network to provide interconnective technologies. The Board of Trustees of the Minnesota State Colleges and Universities may opt out of participation as a subscriber on the network, in whole or in part, if the board is able to secure telecommunications services from another source that ensures it will achieve the policy objectives set forth in subdivision 1.

**Subd. 5. Alternative aggregation.** The chief information officer may, but is not required to, approve community-based aggregation of demand for telecommunications services for state agencies, including Minnesota State Colleges and Universities. To be considered a community-based aggregation project:

(1) the project must aggregate telecommunications demands of state agencies with that of the private sector in a community or a group of communities in a geographic region to the extent permitted by law; and

(2) the aggregation must result in telecommunications infrastructure improvements that ensure the policy set forth in subdivision 1, paragraphs (a) and (b).

**Subd. 6. Rates.** (a) The chief information officer shall establish reimbursement rates in cooperation with the commissioner of management and budget to be billed to participating agencies and educational institutions sufficient to cover the operating, maintenance, and administrative costs of the system.

(b) Except as otherwise provided in subdivision 4, a direct appropriation made to an educational institution for usage costs associated with the state information infrastructure must only be used by the educational institution for payment of usage costs of the network as billed by the chief information officer.

**Subd. 7. Appropriation.** Money appropriated for the state information infrastructure and fees for telecommunications services must be deposited in an account in the MNIT services revolving fund. Money in the account is appropriated annually to the chief information officer to carry out the purposes of this section.

**Subd. 8. Exemption.** The state information network is exempt from the five- and ten-year limitation on contracts set by sections 16C.05, subdivision 2, paragraph (b); 16C.06, subdivision 3b; 16C.08, subdivision 3, clause (5); and 16C.09, clause (6). A contract compliance review must be performed by the office on a five-year basis for any contract that has a total term greater than five years. The review must detail any compliance or performance issues on the part of the contractor.

**History:** 1989 c 246 s 2; 1989 c 335 art 1 s 64; 1990 c 594 art 1 s 47; 1991 c 345 art 1 s 64; 1992 c 514 s 10-12; 1994 c 634 art 1 s 8,9; 1Sp1995 c 3 art 12 s 1; 1996 c 398 s 15; 1997 c 202 art 3 s 4; 1998 c 359 s 9; 1998 c 386 art 2 s 14; 1998 c 397 art 11 s 3; 1998 c 398 art 5 s 55; 1999 c 86 art 1 s 10; 1999 c 214 art 2 s 1; 1999 c 250 art 1 s 61; 2001 c 162 s 5; 2003 c 130 s 12; 1Sp2003 c 1 art 2 s 41,42; 2005 c 156 art 5 s 23; 2007 c 100 s 2-4; 2009 c 101 art 2 s 109; 2013 c 134 s 24,30; 2013 c 142 art 3 s 36; 2014 c 271 art 4 s 6; 2021 c 31 art 2 s 16

## 16E.19 ADMINISTRATION OF STATE COMPUTER FACILITIES.

**Subdivision 1. Chief information officer's responsibility.** The chief information officer shall integrate and operate the state's centralized computer facilities to serve the needs of state government. The chief

information officer shall provide technical assistance to state agencies in the design, development, and operation of their computer systems.

Subd. 2. **Joint actions.** The chief information officer may, within available funding, join with the federal government, other states, local governments, and organizations representing those groups either jointly or severally in the development and implementation of systems analysis, information services, and computerization projects.

**History:** 1997 c 202 art 3 s 5; 2005 c 156 art 5 s 23

**16E.20** MS 2022 [Repealed, 2024 c 123 art 17 s 31]

### **16E.21 INFORMATION AND TELECOMMUNICATIONS ACCOUNT.**

Subdivision 1. **Account established; appropriation.** The information and telecommunications technology systems and services account is created in the special revenue fund. Receipts credited to the account are appropriated to the Department of Information Technology Services for the purpose of defraying the costs of personnel and technology for activities that create government efficiencies, secure state systems, or address project or product backlogs in accordance with this chapter.

Subd. 2. **Charges.** (a) Upon agreement of the participating agency, the Department of Information Technology Services may collect a charge or receive a fund transfer under section 16E.0466 for purchases of information and telecommunications technology systems and services by state agencies and other governmental entities through state contracts for purposes described in subdivision 1. Charges collected under this section must be credited to the information and telecommunications technology systems and services account.

(b) Notwithstanding section 16A.28, subdivision 3, any unexpended operating balance appropriated to a state agency may be transferred to the information and telecommunications technology systems and services account for the information technology cost of a specific project, product, or services, subject to the review of the Legislative Advisory Commission under subdivision 3.

Subd. 3. **Legislative Advisory Commission review.** (a) No funds may be transferred to the information and telecommunications technology systems and services account under subdivision 2 or section 16E.0466 until the commissioner of management and budget has submitted the proposed transfer to the members of the Legislative Advisory Commission for review and recommendation. If the commission makes a positive recommendation or no recommendation, or if the commission has not reviewed the request within 20 days after the date the request to transfer funds was submitted, the commissioner of management and budget may approve the request to transfer the funds. If the commission recommends further review of a request to transfer funds, the commissioner shall provide additional information to the commission. If the commission makes a negative recommendation on the request within ten days of receiving further information, the commissioner shall not approve the fund transfer. If the commission makes a positive recommendation or no recommendation within ten days of receiving further information, the commissioner may approve the fund transfer.

(b) A recommendation of the commission must be made at a meeting of the commission unless a written recommendation is signed by all members entitled to vote on the item as specified in section 3.30, subdivision 2. A recommendation of the commission must be made by a majority of the commission.

Subd. 4. **Lapse.** Any portion of any receipt credited to the information and telecommunications technology systems and services account from a fund transfer under subdivision 2 that remains unexpended and

unencumbered at the close of the fiscal year four years after the funds were received in the account shall lapse to the fund from which the receipt was transferred.

**Subd. 5. Report.** The chief information officer shall report by September 15 of each odd-numbered year to the chairs and ranking minority members of the legislative committees and divisions with jurisdiction over the Department of Information Technology Services regarding the receipts credited to the account. The report must include a description of projects funded through the information and telecommunications technology systems and services account and each project's current status.

**History:** 2006 c 282 art 14 s 9; 2013 c 134 s 30; 2013 c 142 art 3 s 36; 2016 c 189 art 13 s 22-25; 2021 c 31 art 2 s 14,16; 2023 c 62 art 6 s 14,15

**16E.22** MS 2016 [Expired, L 2009 c 101 art 2 s 59]

### **16E.30 GEOSPATIAL INFORMATION OFFICE.**

**Subdivision 1. Creation.** The Minnesota Geospatial Information Office is created under the supervision of the chief geospatial information officer, who is appointed by the chief information officer.

**Subd. 2. Responsibilities; authority.** The office has authority to provide coordination, guidance, and leadership, and to plan the implementation of Minnesota's geospatial information technology. The office must identify, coordinate, and guide strategic investments in geospatial information technology systems, data, and services to ensure effective implementation and use of Geospatial Information Systems (GIS) by state agencies to maximize benefits for state government as an enterprise.

**Subd. 3. Duties.** The office must:

(1) coordinate and guide the efficient and effective use of available federal, state, local, and public-private resources to develop statewide geospatial information technology, data, and services;

(2) provide leadership and outreach, and ensure cooperation and coordination for all Geospatial Information Systems (GIS) functions in state and local government, including coordination between state agencies, intergovernment coordination between state and local units of government, and extragovernment coordination, which includes coordination with academic and other private and nonprofit sector GIS stakeholders;

(3) review state agency and intergovernment geospatial technology, data, and services development efforts involving state or intergovernment funding, including federal funding;

(4) provide information to the legislature regarding projects reviewed, and recommend projects for inclusion in the governor's budget under section 16A.11;

(5) coordinate management of geospatial technology, data, and services between state and local governments;

(6) provide coordination, leadership, and consultation to integrate government technology services with GIS infrastructure and GIS programs;

(7) work to avoid or eliminate unnecessary duplication of existing GIS technology services and systems, including services provided by other public and private organizations while building on existing governmental infrastructures;

(8) promote and coordinate consolidated geospatial technology, data, and services and shared geospatial web services for state and local governments; and

(9) promote and coordinate geospatial technology training, technical guidance, and project support for state and local governments.

Subd. 4. [Repealed, 2013 c 95 s 5]

Subd. 5. [Repealed, 2013 c 95 s 5]

Subd. 6. **Accountability.** The chief geospatial information officer is appointed by the Minnesota chief information officer who shall advise on technology projects, standards, and services.

Subd. 7. **Discretionary powers.** The office may:

(1) review the Geospatial Information Systems (GIS) technology infrastructure of regions of the state and cooperate with and make recommendations to the governor, legislature, state agencies, local governments, local technology development agencies, the federal government, private businesses, and individuals for the realization of GIS information and technology infrastructure development potential;

(2) sponsor, support, and facilitate innovative and collaborative geospatial systems technology, data, and services projects; and

(3) review and recommend alternative sourcing strategies for state geospatial information systems technology, data, and services.

Subd. 8. **Geospatial Advisory Council created.** (a) The chief information officer must utilize a governance structure that includes an advisory council to provide recommendations for improving the operations and management of geospatial technology within state government and also on issues of importance to users of geospatial technology throughout the state.

(b) The Geospatial Advisory Council must advise the Minnesota Geospatial Information Office regarding the improvement of services statewide through the coordinated, affordable, reliable, and effective use of geospatial technology. The chief information officer must appoint the members of the council. The members must represent a cross-section of organizations including counties, cities, universities, business, nonprofit organizations, federal agencies, tribal governments, and state agencies. In addition, the chief geospatial information officer must be a nonvoting member.

(c) Members of the Geospatial Advisory Council must be recommended by a process that ensures that each member is designated to represent a clearly identified agency or interested party category. Members of the Geospatial Advisory Council must be selected in compliance with the state's open appointment process. Members shall serve a term of two years.

(d) The Minnesota Geospatial Information Office must provide administrative support for the Geospatial Advisory Council.

Subd. 9. [Repealed, 2011 c 68 s 2]

Subd. 10. **Electronic geospatial data defined.** "Electronic geospatial data" means digital data using geographic or projected map coordinate values, identification codes, and associated descriptive data to locate and describe boundaries or features on, above, or below the surface of the earth or characteristics of the earth's inhabitants or its natural or human-constructed features.

Subd. 11. **Government sharing of electronic geospatial data.** (a) The definitions in section 13.02 apply to this subdivision.

(b) Electronic geospatial government data must be shared at no cost with government entities, the notification center established under section 216D.03, and federal and tribal government agencies. Data received under this subdivision may be reproduced or shared with other government entities or agencies. A release of data under this subdivision must include metadata or other documentation that identifies the original authoritative data source. Government entities providing data under this subdivision are not required to provide data in an alternate format specified by the requestor. A government entity is not required to provide the same data to the same requestor more than four times per year, unless required by law or court order. Government entities and agencies sharing and receiving electronic geospatial data under this subdivision are immune from civil liability arising out of the use of the shared electronic geospatial data. This subdivision does not authorize the release of data that are not public data.

**History:** 2009 c 101 art 2 s 55,107,109; 2011 c 68 s 1; 1Sp2011 c 10 art 4 s 1,8; 2013 c 95 s 1-4

### 16E.35 COUNTY AND LOCAL CYBERSECURITY GRANTS.

Subdivision 1. **Cybersecurity grant program established.** The Department of IT Services may make grants to political subdivisions to support addressing cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or Tribal governments, as provided in section 70612 of Public Law 117-58.

Subd. 2. **Match requirement.** The political subdivision receiving a grant must provide for the remainder of the costs of the project that exceed available state match appropriated funds, or that exceed goals defined in the statewide cybersecurity plan.

Subd. 3. **Criteria.** The department may set criteria for program priorities and standards of review.

**History:** 2023 c 62 art 6 s 16

### 16E.36 CYBERSECURITY INCIDENTS.

Subdivision 1. **Definitions.** (a) For purposes of this section, the following terms have the meanings given.

(b) "Bureau" means the Bureau of Criminal Apprehension.

(c) "Cybersecurity incident" means an action taken through the use of an information system or network that results in an actual or potentially adverse effect on an information system, network, or the information residing therein.

(d) "Cyber threat indicator" means information that is necessary to describe or identify:

(1) malicious reconnaissance, including but not limited to anomalous patterns of communication that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or vulnerability;

(2) a method of defeating a security control or exploitation of a security vulnerability;

(3) a security vulnerability, including but not limited to anomalous activity that appears to indicate the existence of a security vulnerability;

(4) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(5) malicious cyber command and control;

(6) the actual or potential harm caused by an incident, including but not limited to a description of the data exfiltrated as a result of a particular cyber threat; and

(7) any other attribute of a cyber threat, if disclosure of such attribute is not otherwise prohibited by law.

(e) "Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cyber threat or security vulnerability, but does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting an information system not owned by the entity operating the measure, or another entity that is authorized to provide consent and has provided consent to that private entity for operation of the measure.

(f) "Government contractor" means an individual or entity that performs work for or on behalf of a public agency on a contract basis with access to or hosting of the public agency's network, systems, applications, or information.

(g) "Information resource" means information and related resources, such as personnel, equipment, funds, and information technology.

(h) "Information system" means a discrete set of information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or disposing of information.

(i) "Information technology" means any equipment or interconnected system or subsystem of equipment that is used in automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information used by a public agency or a government contractor under contract with a public agency which requires the use of the equipment or requires the use, to a significant extent, of the equipment in the performance of a service or the furnishing of a product. The term information technology also has the meaning given to information and telecommunications technology systems and services in section 16E.03, subdivision 1, paragraph (b).

(j) "Private entity" means any individual, corporation, company, partnership, firm, association, or other entity, but does not include a public agency, or a foreign government, or any component thereof.

(k) "Public agency" means any public agency of the state or any political subdivision; school districts; charter schools; intermediate districts; cooperative units under section 123A.24, subdivision 2; and public postsecondary education institutions.

(l) "Superintendent" means the superintendent of the Bureau of Criminal Apprehension.

**Subd. 2. Report on cybersecurity incidents.** (a) Beginning December 1, 2024, the head of or the decision-making body for a public agency must report a cybersecurity incident that impacts the public agency to the commissioner. A government contractor or vendor that provides goods or services to a public agency must report a cybersecurity incident to the public agency if the incident impacts the public agency.

(b) The report must be made within 72 hours of when the public agency or government contractor reasonably identifies or believes that a cybersecurity incident has occurred.

(c) The commissioner must coordinate with the superintendent to promptly share reported cybersecurity incidents.

(d) By September 30, 2024, the commissioner, in coordination with the superintendent, must establish a cyber incident reporting system having capabilities to facilitate submission of timely, secure, and confidential cybersecurity incident notifications from public agencies, government contractors, and private entities to the office.

(e) By September 30, 2024, the commissioner must develop, in coordination with the superintendent, and prominently post instructions for submitting cybersecurity incident reports on the department and bureau websites. The instructions must include, at a minimum, the types of cybersecurity incidents to be reported and a list of other information to be included in a report made through the cyber incident reporting system.

(f) The cyber incident reporting system must permit the commissioner, in coordination with the superintendent, to:

(1) securely accept a cybersecurity incident notification from any individual or private entity, regardless of whether the entity is a public agency or government contractor;

(2) track and identify trends in cybersecurity incidents reported through the cyber incident reporting system; and

(3) produce reports on the types of incidents, cyber threat, indicators, defensive measures, and entities reported through the cyber incident reporting system.

(g) Any cybersecurity incident report submitted to the commissioner is security information pursuant to section 13.37, is not discoverable in a civil or criminal action absent a court order or a search warrant, and is not subject to subpoena.

(h) Notwithstanding the provisions of paragraph (g), the commissioner may anonymize and share cyber threat indicators and relevant defensive measures to help prevent attacks and share cybersecurity incident notifications with potentially impacted parties through cybersecurity threat bulletins or relevant law enforcement authorities.

(i) Information submitted to the commissioner through the cyber incident reporting system is subject to privacy and protection procedures developed and implemented by the office, which shall be based on the comparable privacy protection procedures developed for information received and shared pursuant to the federal Cybersecurity Information Sharing Act of 2015, United States Code, title 6, section 1501, et seq.

Subd. 3. **Annual report to the governor and legislature.** Beginning January 31, 2026, and annually thereafter, the commissioner, in coordination with the superintendent, must submit a report on its cyber security incident report collection and resolution activities to the governor and to the legislative commission on cybersecurity. The report must include, at a minimum:

(1) information on the number of notifications received and a description of the cybersecurity incident types during the one-year period preceding the publication of the report;

(2) the categories of reporting entities that submitted cybersecurity reports; and

(3) any other information required in the submission of a cybersecurity incident report, noting any changes from the report published in the previous year.

**History:** *2024 c 123 art 17 s 24*