

This Document can be made available in alternative formats upon request

State of Minnesota

HOUSE OF REPRESENTATIVES

NINETIETH SESSION

H. F. No. 2868

02/20/2018 Authored by Nash, Scott, Albright and Pugh
The bill was read for the first time and referred to the Committee on Government Operations and Elections Policy
03/26/2018 Adoption of Report: Re-referred to the Committee on State Government Finance

1.1 A bill for an act
1.2 relating to state government; requiring state agencies to dedicate a portion of their
1.3 information technology expenditures to cyber security enhancements; amending
1.4 Minnesota Statutes 2016, sections 16A.11, subdivision 1, by adding a subdivision;
1.5 16E.03, subdivision 7.

1.6 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

1.7 Section 1. Minnesota Statutes 2016, section 16A.11, subdivision 1, is amended to read:

1.8 Subdivision 1. When. The governor shall submit a three-part budget to the legislature.
1.9 Parts one and two, the budget message and detailed operating budget, must be submitted
1.10 by the fourth Tuesday in January in each odd-numbered year. However, in a year following
1.11 the election of a governor who had not been governor the previous year, parts one and two
1.12 must be submitted by the third Tuesday in February. Part three, the detailed recommendations
1.13 as to capital expenditure, must be submitted as follows: agency capital budget requests by
1.14 July 15 of each odd-numbered year, and governor's recommendations by January 15 of each
1.15 even-numbered year. Detailed recommendations as to information technology expenditure
1.16 must be submitted as part of the detailed operating budget. Information technology
1.17 recommendations must include projects to be funded during the next biennium and planning
1.18 estimates for an additional two bienniums. Information technology recommendations must
1.19 specify purposes of the funding such as infrastructure, hardware, software, or training.

1.20 Sec. 2. Minnesota Statutes 2016, section 16A.11, is amended by adding a subdivision to
1.21 read:

1.22 Subd. 6a. Information technology and cyber security. (a) Detailed recommendations
1.23 as to information and telecommunications technology systems and services expenditures

2.1 must be submitted as part of the detailed operating budget. These recommendations must  
 2.2 include projects to be funded during the next biennium and planning estimates for an  
 2.3 additional two bienniums, and must specify purposes of the funding, such as infrastructure,  
 2.4 hardware, software, or training. The detailed operating budget must also separately  
 2.5 recommend expenditures for the maintenance and enhancement of cyber security for the  
 2.6 state's information and telecommunications technology systems and services.

2.7 (b) The commissioner of management and budget, in consultation with the state chief  
 2.8 information officer, shall establish budget guidelines for the recommendations required by  
 2.9 this subdivision. Unless otherwise set by the commissioner at a higher amount, the amount  
 2.10 to be budgeted each fiscal year for maintenance and enhancement of cyber security must  
 2.11 be at least five percent of a department's or agency's total operating budget for information  
 2.12 and telecommunications technology systems and services in that year.

2.13 (c) As used in this subdivision:

2.14 (1) "information and telecommunications technology systems and services" has the  
 2.15 meaning given in section 16E.03, subdivision 1, paragraph (a); and

2.16 (2) "cyber security" has the meaning given in section 16E.03, subdivision 1, paragraph  
 2.17 (d).

2.18 Sec. 3. Minnesota Statutes 2016, section 16E.03, subdivision 7, is amended to read:

2.19 Subd. 7. **Cyber security systems.** In consultation with the attorney general and  
 2.20 appropriate agency heads, the chief information officer shall develop cyber security policies,  
 2.21 guidelines, and standards, and shall install and administer state data security systems on the  
 2.22 state's computer facilities consistent with these policies, guidelines, standards, and state law  
 2.23 to ensure the integrity of computer-based and other data and to ensure applicable limitations  
 2.24 on access to data, consistent with the public's right to know as defined in chapter 13. The  
 2.25 chief information officer is responsible for overall security of state agency networks  
 2.26 connected to the Internet. Each department or agency head is responsible for the security  
 2.27 of the department's or agency's data within the guidelines of established enterprise policy.  
 2.28 Unless otherwise expressly provided by law, at least five percent of each department's or  
 2.29 agency's expenditures in a fiscal year for information and telecommunications technology  
 2.30 systems and services must be directed to the maintenance and enhancement of cyber security.

2.31 **EFFECTIVE DATE.** This section is effective July 1, 2018, and applies to expenditures  
 2.32 in fiscal years beginning on or after that date.