SENATE
STATE OF MINNESOTA
EIGHTY-EIGHTH LEGISLATURE

S.F. No. 1565

(SENATE AUTHORS: SCHMIT)

DATE	D-PG	OFFICIAL STATUS
04/08/2013	1686	Introduction and first reading Referred to Jobs, Agriculture and Rural Development

A bill for an act

relating to telecommunications; broadband; requiring a study and report on cyber security and broadband infrastructure vulnerabilities.

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

Section 1. **BROADBAND CYBER SECURITY; REPORT.**

Subdivision 1. **Policy statement.** The legislature of the state of Minnesota, as part of its efforts to deploy and improve broadband service in the state under Minnesota Statutes, section 237.012, finds that it is of critical importance to determine (1) whether any potential single point of system failure or other vulnerabilities to cyber terrorism exist, and (2) what, if any, steps need to be taken to address identified shortcomings.

Subd. 2. **Study; cyber security.** (a) The Minnesota Broadband Task Force, established under Executive Order 11-27, shall commission a study that analyzes the current and desired status of the state's broadband infrastructure security. The study should focus on issues related to public safety, law enforcement, and the provision of electrical power, other utilities, and essential services to gauge the potential impact widespread disruption to broadband services would have on commercial enterprise in the state.

(b) The study shall be conducted by qualified technical experts, including state and local officials and business technology leaders with varied cyber security experiences. The Minnesota Broadband Task Force shall oversee and manage the study and work to ensure the widest participation possible by the business community. By January 15, 2015, the Minnesota Broadband Task Force shall report back on the study's findings, including any recommended legislative initiatives, to the legislative committees having jurisdiction over telecommunications, commerce, and public safety.

(c) The study's key findings must summarize the areas where the state's broadband infrastructure is most vulnerable. The study must contain detailed research and recommendations, including an analysis of the economic impact that would result from widespread disruption of broadband service, as well as the positive impact on economic development that might accrue if the state enhanced cyber security readiness and leveraged inherent advantages related to broadband or data center deployment.

(d) Notwithstanding any laws to the contrary, the Minnesota Broadband Task Force and the individuals participating in the study are authorized to review data, findings, and recommendations in a closed, nonpublic session to ensure that protected and proprietary data remain secure. Any proprietary or nonpublic information used in developing the report must be handled in a manner consistent with Minnesota Statutes, chapter 13.

Subd. 3. **Study; report contents.** At a minimum, the report shall evaluate and make recommendations regarding:

(1) how cyber attacks are currently identified and responded to, including:

(i) an assessment on the impact of cyber terrorism on critical infrastructure, including but not limited to public safety infrastructure, water and sewers, and the electrical grid;

(ii) a determination regarding how to protect the confidentiality of sensitive security information, while still making appropriate disclosure to practitioners and public policy makers;

(iii) a threat assessment, assuming both worst-case and most-likely cyber breach scenarios, analyzing the impact of a situation where the state's critical and major broadband and Internet hubs were breached or taken down; and

(iv) an evaluation of the extent to which cyber hackers have or could obtain access to intellectual property or other protected, private data;

(2) how to enhance the state's response to cyber threats and attacks, including an assessment on how quickly the state can currently respond to and contain cyber threats and any recommended improvements;

(3) the extent to which a risk assessment shows broadband traffic in the state is susceptible to a single point of failure, including:

(i) an evaluation of significant co-location sites in the Twin Cities and the respective downstream dependencies;

(ii) an evaluation of the state's middle-mile broadband infrastructure to determine whether the infrastructure has any single points of failure in the event of a disaster or attack; and

(iii) recommendations or options for robust ways to increase performance and reduce vulnerability, including an analysis of the investments and efforts needed to ensure

the state's broadband infrastructure remains fully functioning in the event of an attack or disaster elsewhere;

(4) the state's broadband cyber security strategies compared to other states and peer entities, assessing the degree to which the strategies might contribute to the state's security and redundancy goals and reduce the state's vulnerability, including:

(i) an assessment of any broadband advantages the state has that it is not currently leveraging; and

(ii) a brief assessment of the strategies and procedures other states are using to prepare for cyber security threats, as well as any recommended national protocols or best practices the state should consider implementing; and

(5) a description of the security, vulnerability, and redundancy actions necessary to ensure reliability, drawing heavily on the actions plans documented in the 2009 Minnesota Ultra High-Speed Broadband Report that describe the duties and targets for the office, including any recommendations regarding the establishment of formal links between a new broadband office and related activities in other agencies to ensure effective collaboration and information sharing.

EFFECTIVE DATE. This section is effective the day following final enactment.