HOUSE RESEARCH

Bill Summary

FILE NUMBER: H.F. 2470   **DATE:** March 14, 2012
          Version: As introduced

          Authors: Cornish

          Subject: Criminal intelligence data

          Analyst: Jeff Diebel

This publication can be made available in alternative formats upon request. Please call 651-296-6753 (voice); or the Minnesota State Relay Service at 1-800-627-3529 (TTY) for assistance. Summaries are also available on our website at: www.house.mn/hrd.

Overview

This bill establishes standards for collecting, storing and sharing criminal intelligence data.

1   **Criminal intelligence data.**

Subd. 1. Definitions. Defines "association data," criminal intelligence data," "criminal intelligence data assessment," "criminal predicate," "critical infrastructure," "law enforcement agency," "terrorist activity," and "threat of imminent serious harm."

Subd. 2. Data classification and retention. Classifies criminal intelligence data as either confidential data on individuals or protected nonpublic data for a period of one year. After one year, the classification level is changed to either private data on individuals or nonpublic data, unless five criteria for confirming the accuracy of the information are met. Data that changes classifications must be deleted after 3 years.

Subd. 3. Sharing authorized. Establishes grounds for sharing criminal intelligence data and criminal intelligence data assessments.

Subd. 4. Data prohibitions. Requires a criminal predicate for a law enforcement agency to maintain or use criminal intelligence data. Prohibits the maintenance and sharing of association data.

Subd. 5. Dissemination record. Requires law enforcement agencies to keep a dissemination record for each disclosure made under subdivision 3.

2   **Criminal intelligence systems.**

Subd. 1. Definitions. Defines the terms: "criminal intelligence data," "criminal intelligence system," "intelligence project," "interjurisdictional intelligence system," "participating agency," and "validation of data."

Subd. 2. Operating principles. Establishes standards for:

•   when a project can collect and maintain criminal intelligence data on an individual and

what type of data can be collected and maintained;

- the dissemination and protection of criminal intelligence data by a project;

- the tools and techniques that can be used to collect criminal intelligence data; and

- tracing the data from the entity that submitted it to the project.

Subd. 3. Supervision. Establishes standards and requirements for supervision of projects and the data maintained by the projects.

Subd. 4. Audit of data submitted to system; reports. Requires the BCA to audit criminal intelligence systems.

Subd. 5. Classification of intelligence data. Classifies criminal intelligence data as confidential data on individuals or protected nonpublic data.