HOUSE RESEARCH

Bill Summary

FILE NUMBER: H.F. 2800 **DATE:** April 14, 2004

Version: Second Engrossment

Authors: Holberg

Subject: CriMNet and Other Information Management Systems

Analyst: Deborah K. McKnight, Legislative Analyst (651-296-5056)

Overview

CriMNet is a statewide information management system for interconnecting criminal justice agency data. This bill provides processes for the commissioner of administration to determine whether various information management systems are in compliance with information policy laws (§§ 5 and 6); requires law enforcement agencies to document certain exchanges of data on individuals (§ 7); regulates CriMNet data access and subscription services (§ 8); requires any state criminal justice agency to report to the legislature before implementing a new information management system to follow the same law as CriMNet (§ 9); provides fingerprint requirements in order to improve the reliability of criminal history files (§10 to 14); clarifies public defender access to criminal history data (§ 15); and requires the study of specified CriMNet issues (§ 16).

Section

1 **Information management system.** Adds a definition of this term to the government data practices act: an electronic system used or maintained by a government entity to manage government data.

2 **Information policy statutes.** Adds a definition of this term. It means the data practices act, the official records act, and the state archives law. Lists actions that government entities are required to take under current law to be in compliance.

3 **Statewide system.** Provides that an information management system is a type of statewide system for purposes of the data practices act. Provides that a statewide system may include a non-government entity which is performing functions normally performed by a government

Section

entity.

4 **Change in classification of data.** Amends the "traveling data" section in current law. Provides that when judicial branch data is given to other government entities, it keeps the same level of accessibility it had in the judicial branch.

5 **Information management systems; compliance with law.** Allows a person who believes an information managed system is noncompliant with the date practices act to seek a commissioner's advisory opinion. Requires the government entity operating the system to provide information in connection with the opinion request.

Lets a person obtain section 13.08 remedies against a noncompliant system. Adds that the court may shut down the system if it does not progress towards compliance.

Prohibits a state agency from taking operational responsibility for a noncompliant system. Before a state agency takes over or participates in a system started by another entity, requires the commissioner of administration to audit the system for compliance with information policy statutes and federal law. Prohibits a state agency from spending to enhance such a system without legislative approval, unless required by federal law.

6 **Information management system review.** Requires the commissioner to check for information policy statute compliance of information management systems added to CriMNet after the effective date of the act..

By January 15, 2005, the commissioner must give the legislature a timetable and cost estimate for reviewing all other state information management systems for compliance with information policy statutes. Prohibits new systems from being implemented until the commissioner does this review.

The legislative auditor would include continuing compliance, as resources permit, as part of each periodic audit.

If the legislative auditor or state auditor finds that a system is noncompliant, the responsible authority must, within 30 days, present a plan to achieve compliance. If the commissioner finds a failure to make progress, the commissioner may shut down the system. If a system is out-of-compliance, the government entity must report to the legislative fiscal committees (1) what the system cost, and (2) what compliance costs.

7 **Exchanges of information.** Amends the law enforcement data section of the data practices act. Provides that when a law enforcement agency requests or disseminates private/confidential data about an individual electronically, it must document the purpose of the request or dissemination, including the case number, if available. Requires this documentation to be kept for ten years. Makes documentation private data on the investigation subject once the investigation is inactive.

8 **CriMNet data.** Adds a new section to the Data Practices Act.

Subd. 1. Definitions.

"CriMNet" is a statewide system that integrates or interconnects data from multiple criminal justice information systems.

Section

"CriMNet data" are criminal justice agency data held by CriMNet for prevention, investigation, or prosecution of crime and criminal justice system responses.

"Audit trail data" are data for purposes of ensuring and verifying that CriMNet was only accessed by authorized persons for authorized purposes.

Subd. 2. Data classification; dissemination. Provides that CriMNet data have the same classification in CriMNet as they did in the originating agency. Except for individuals exercising their rights regarding data on themselves, CriMNet data is only available pursuant to state or federal law to criminal justice agencies, public defenders, federal criminal justice agencies, and other states' criminal justice agencies.

Specifies purposes for which CriMNet data may be released: (1) investigating a crime or delinquent act, (2) seeking to apprehend a person fleeing to avoid prosecution or custody, (3) enforcing a warrant, (4) enforcing terms of pre-trial release, (5) seeking an individual who is violating a condition of some form of supervised release, (6) determining that an individual may be engaged in illegal activities, (7) prosecuting, defending, trying, or sentencing an individual, (8) seeking an individual likely to have information necessary to one of the above, (9) auditing data quality, data protection, and system development and maintenance, or (10) with the subject's informed consent (for a juvenile, only the parent or guardian may consent).

Subd. 3. Requests by data subject. When an individual requests CriMNet data on herself/himself, a law enforcement agency with CriMNet access must (1) give the individual a list of entities that gave data to CriMNet and (2) allow the individual to obtain a copy of any public or private CriMNet data, and inform the individual that audit trail data are available from CriMNet.

Subd. 4. Audit trail data. Requires that audit trail data indicate for which purpose under subd. 2 and for which matter, including case file if available, CriMNet data on an individual was accessed. Requires audit trail data to be kept for ten years.

Makes audit trail data created as part of an investigation confidential/protected nonpublic while the investigation is active. When the investigation becomes inactive or if data was accessed for a reason unrelated to an investigation:

(1) the identity of an entity that requested data on a data subject is accessible to the subject; and

(2) the CriMNet responsible authority must give the subject the requester's name if the subject's need to know outweighs the risk of harm disclosure would create for the requester or for public safety. Specifies a hearing process to resolve the issue of releasing the individual requester's name.

From the effective date of the bill until June 30, 2010, this subdivision only applies to CriMNet and to specified new systems or enhancements to CriMNet or component systems. On and after July 1, 2010, this subdivision applies to CriMNet and all

Section

systems that are part of it.

Subd. 5. Subscription service. Defines this as a process by which criminal justice agency personnel may obtain ongoing automatic electronic notice of any contacts an individual has with any criminal justice agency.

Allows release of CriMNet data through a subscription service:

(1) to the subject of the data upon his/her request;

(2) with the informed consent of a data subject, or, in the case of a juvenile, parent or guardian consent; or

(3) as an element of sentencing or any kind of supervised release of which the data subject is informed before implementation.

Allows release of CriMNet data with the subject's consent and without notice for 30 days in order to (1) investigate a crime or delinquent act, (2) apprehend an individual fleeing prosecution or custody, (3) enforce a warrant, (4) enforce terms of pre-trial release, (5) seek an individual violating any form of supervised release, (6) determine that an individual may be engaged in illegal activities, (7) prosecute, defend, try, or sentence an individual, or (8) find an individual likely to have information necessary for one of the above.

Allows subscription service for a longer period only by seeking a court order in the same manner as a search warrant. Provides for the court to grant the order if it finds one of the above purposes still exists. Requires the court to specify how long the service may continue, which must not exceed 18 months without a showing of imminent threat to public safety or health.

Subd. 6. Penalties. States that a person who violates this section is subject to the penalties of chapter 13.

Subd. 7. Legislative review of access modifications. Specifies that any CriMNet feature that would give access to data on individuals to any entity, other than the judiciary, that is not subject to the Data Practices Act, must receive prior legislative approval and must be implemented by a statute, contract, or interstate compact that complies with this section.

9 **Criminal justice system approval.** Prior to implementing a new criminal justice information system to be created or maintained by a state criminal justice agency, the agency must report to the house and senate committees with jurisdiction over data practices and fiscal jurisdiction over the agency.

10 **Requires fingerprinting.** Requires the law enforcement agency responsible for an individual's arrest or initial court appearance to take the individual's fingerprints. Requires the sheriff to do so if the initial agency fails. Allows the sheriff to assess cost against that agency.

Section

Provides for obtaining fingerprints of those currently involved in the criminal justice process, in order to reduce suspense files (criminal records not linked to a subject by fingerprints).

11 **Court disposition record in suspense.** Requires the Bureau of Criminal Apprehension to notify a prosecutor if an individual is the subject of a court record in suspense. Allows the prosecutor to bring a court notice to compel the taking of fingerprints.

12 **Law enforcement education.** Expands individuals who must be trained to take fingerprints.

13 **Information on released prisoners.** Requires corrections facilities to provide fingerprints to the BCA to reduce the number of suspense files.

14 **Data classification.** Cross-reference.

15 **Access to government data.** Clarifies that public defenders may access the criminal history of their own clients and the conviction records of witnesses, but may not access prosecutor records.

16 **Reports.** Requires the Juvenile and Criminal Information Task Force to report to the legislature by December 1, 2004 on specified topics related to CriMNet.

17 **Effective date.** Immediate.