HOUSE RESEARCH

Bill Summary

FILE NUMBER: H.F. 2155 **DATE:** March 9, 2004

Version: As introduced

Authors: Holberg

Subject: CriMNet Data Classifications

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

Overview

The bill classifies CriMNet data, requires fingerprints in order to reduce the number of criminal history files that cannot be linked to a subject by fingerprints, and requires a report on specified CriMNet issues.

Section

1 **Change in classification.** Adds judicial branch data to the "traveling data" provision that gives data the same access in an agency that receives it as the data had in the sending agency.

2 **CriMNet data classification.**

Subd. 1. Definitions.

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

"CriMNet data" are criminal justice agency and court 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

Section

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 to criminal justice agencies, public defenders, federal criminal justice agencies, and other states' criminal justice agencies. Classifies audit trail data as confidential and allows access only by persons ensuring security of the system.

Subd. 3. Requests by data subject. When a data subject asks CriMNet for data about herself/himself, CriMNet will provide a list of agencies that gave it data about the individual. Provides for CriMNet to do system audits based on complaints about unauthorized access to data about a data subject. Requires CriMNet to give the data subject a summary of the audit outcome, including administrative or disciplinary actions. Requires CriMNet to maintain and Internet list of law enforcement agencies that have access to it.

3 **Required fingerprinting.** In order to reduce suspense files (those where an individual cannot be linked to a record by fingerprints), requires that fingerprints be taken in post arrest interviews, while making court appearances, while in custody, or on any form of supervised release.

4 **Court disposition record in suspense; fingerprinting.** Requires the Bureau of Criminal Apprehension (BCA) to notify a prosecutor if a court disposition record is in suspense for lack of fingerprints. Allows the prosecutor to bring a motion in court to compel taking fingerprints on a showing that the person is the subject of the court disposition record.

5 **Information on released prisoner.** Amends a corrections institution statute to specify a duty to furnish fingerprints when requested by the BCA to reduce suspense files.

6 **Data classification.** Cross-reference.

7 **Access to government data.** Gives the public defender access to data about criminal convictions of witnesses in a case and access to broader criminal history data on the defender's client. Provides the access may be via CriMNet or other methods.

8 **Report required. R** equires the Juvenile And Criminal Information Task Force to study and prepare recommendations to the policy group by December 1, 2004, on Web- based access to CriMNet data by data subjects, use of CriMNet for noncriminal justice background checks, a process to coordinate data subject data challenges, advisability of public access to CriMNet, and Data Practices Act Compliance.