299C.46 CRIMINAL JUSTICE DATA COMMUNICATIONS NETWORK.

Subdivision 1. **Establishment.** The commissioner of public safety shall establish a criminal justice data communications network that will provide secure access to systems and services available from or through the Bureau of Criminal Apprehension. The commissioner of public safety is authorized to lease or purchase facilities and equipment as may be necessary to establish and maintain the data communications network.

Subd. 2. **Criminal justice agency defined.** For the purposes of sections 299C.46 and 299C.48, "criminal justice agency" means an agency of the state or a political subdivision or the federal government charged with detection, enforcement, prosecution, adjudication or incarceration in respect to the criminal or traffic laws of this state. This definition also includes all sites identified and licensed as a detention facility by the commissioner of corrections under section 241.021 and those federal agencies that serve part or all of the state from an office located outside the state.

Subd. 2a. **Noncriminal justice agency defined.** For the purposes of sections 299C.46 and 299C.48, "noncriminal justice agency" means an agency of the state or a political subdivision of the state charged with the responsibility of performing checks of state databases connected to the criminal justice data communications network.

Subd. 3. **Authorized use, fee.** (a) The criminal justice data communications network shall be used exclusively by:

(1) criminal justice agencies in connection with the performance of duties required by law;

(2) agencies investigating federal security clearances of individuals for assignment or retention in federal employment with duties related to national security, as required by United States Code, title 5, section 9101;

(3) other agencies to the extent necessary to provide for protection of the public or property in a declared emergency or disaster situation;

(4) noncriminal justice agencies statutorily mandated, by state or national law, to conduct checks into state databases prior to disbursing licenses or providing benefits;

(5) the public authority responsible for child support enforcement in connection with the performance of its duties;

(6) the public defender, as provided in section 611.272;

(7) a county attorney or the attorney general, as the county attorney's designee, for the purpose of determining whether a petition for the civil commitment of a proposed patient as a sexual psychopathic personality or as a sexually dangerous person should be filed, and during the pendency of the commitment proceedings;

(8) an agency of the state or a political subdivision whose access to systems or services provided from or through the bureau is specifically authorized by federal law or regulation or state statute; and

(9) a court for access to data as authorized by federal law or regulation or state statute and related to the disposition of a pending case.

(b) The commissioner of public safety shall establish a monthly network access charge to be paid by each participating criminal justice agency. The network access charge shall be a standard fee established for each terminal, computer, or other equipment directly addressable by the data communications network,

as follows: January 1, 1984 to December 31, 1984, $40 connect fee per month; January 1, 1985 and thereafter, $50 connect fee per month.

(c) The commissioner of public safety is authorized to arrange for the connection of the data communications network with the criminal justice information system of the federal government, any state, or country for the secure exchange of information for any of the purposes authorized in paragraph (a), clauses (1), (2), (3), (8) and (9).

(d) Prior to establishing a secure connection, a criminal justice agency that is not part of the Minnesota judicial branch must:

(1) agree to comply with all applicable policies governing access to, submission of or use of the data and Minnesota law governing the classification of the data;

(2) meet the bureau's security requirements;

(3) agree to pay any required fees; and

(4) conduct fingerprint-based state and national background checks on its employees and contractors as required by the Federal Bureau of Investigation.

(e) Prior to establishing a secure connection, a criminal justice agency that is part of the Minnesota judicial branch must:

(1) agree to comply with all applicable policies governing access to, submission of or use of the data and Minnesota law governing the classification of the data to the extent applicable and with the Rules of Public Access to Records of the Judicial Branch promulgated by the Minnesota Supreme Court;

(2) meet the bureau's security requirements;

(3) agree to pay any required fees; and

(4) conduct fingerprint-based state and national background checks on its employees and contractors as required by the Federal Bureau of Investigation.

(f) Prior to establishing a secure connection, a noncriminal justice agency must:

(1) agree to comply with all applicable policies governing access to, submission of or use of the data and Minnesota law governing the classification of the data;

(2) meet the bureau's security requirements;

(3) agree to pay any required fees; and

(4) conduct fingerprint-based state and national background checks on its employees and contractors.

(g) Those noncriminal justice agencies that do not have a secure network connection yet receive data either retrieved over the secure network by an authorized criminal justice agency or as a result of a state or federal criminal history records check shall conduct a background check as provided in paragraph (h) of those individuals who receive and review the data to determine another individual's eligibility for employment, housing, a license, or another legal right dependent on a statutorily mandated background check.

(h) The background check required by paragraph (f) or (g) is accomplished by submitting a request to the superintendent of the Bureau of Criminal Apprehension that includes a signed, written consent for the Minnesota and national criminal history records check, fingerprints, and the required fee. The superintendent

may exchange the fingerprints with the Federal Bureau of Investigation for purposes of obtaining the individual's national criminal history record information.

The superintendent shall return the results of the national criminal history records check to the noncriminal justice agency to determine if the individual is qualified to have access to state and federal criminal history record information or the secure network. An individual is disqualified when the state and federal criminal history record information show any of the disqualifiers that the individual will apply to the records of others.

When the individual is to have access to the secure network, the noncriminal justice agency shall review the criminal history of each employee or contractor with the Criminal Justice Information Services systems officer at the bureau, or the officer's designee, to determine if the employee or contractor qualifies for access to the secure network. The Criminal Justice Information Services systems officer or the designee shall make the access determination based on Federal Bureau of Investigation policy and Bureau of Criminal Apprehension policy.

Subd. 4. **Commissioner administers and coordinates.** The commissioner of public safety shall administer the data communications network and shall coordinate matters relating to its use by other state agencies and political subdivisions. The commissioner shall receive the assistance of the commissioner of administration on matters involving the Department of Administration and its information systems division. Other state department or agency heads shall assist the commissioner where necessary in the performance of the commissioner's duties under this section.

Subd. 5. **Diversion program data.** Counties operating diversion programs under section 401.065 shall supply to the bureau of criminal apprehension the names of and other identifying data specified by the bureau concerning diversion program participants. Notwithstanding section 299C.11, the bureau shall maintain the names and data in the computerized criminal history system for 20 years from the date of the offense. Data maintained under this subdivision are private data.

Subd. 6. **Orders for protection; no contact orders; harassment restraining orders.** (a) As used in this subdivision, "no contact orders" include orders issued as pretrial orders under section 629.72, subdivision 2, orders under section 629.75, and orders issued as probationary or sentencing orders at the time of disposition in a criminal domestic abuse case.

(b) The data communications network must include orders for protection issued under section 518B.01, harassment restraining orders, and no contact orders issued against adults and juveniles. A no contact order must be accompanied by a photograph of the offender for the purpose of enforcement of the order, if a photograph is available and verified by the court to be an image of the defendant.

(c) Data from orders for protection, harassment restraining orders, or no contact orders and data entered by law enforcement to assist in the enforcement of those orders are classified as private data on individuals as defined in section 13.02, subdivision 12. Data about the offender can be shared with the victim for purposes of enforcement of the order.

History: *1965 c 903 s 1; 1967 c 334 s 2; 1977 c 424 s 1; 1983 c 293 s 92; 1986 c 444; 1987 c 166 s 1; 1993 c 326 art 10 s 8; 1996 c 440 art 1 s 51; 1997 c 159 art 2 s 44,45; 1997 c 203 art 6 s 31; 2000 c 377 s 4; 2001 c 167 s 1; 2007 c 54 art 4 s 1; 2009 c 59 art 6 s 9; 2010 c 299 s 3; 2013 c 82 s 26-29; 2015 c 65 art 3 s 10,11; 2017 c 95 art 3 s 11*