DEPARTMENT : HEALTH

STATE OF MINNESOTA

Office Memorandum

DATE : May 30, 2005

TO : File

FROM : Patricia A. Bloomgren, Director
Division of Environmental Health

Douglas J. Mandy, Manager
Section of Drinking Water Protection

PHONE : 651-215-0731
651-215-0757

SUBJECT : Policy on Access, Distribution, and Use of Drinking Water Related Security Information.

PURPOSE

The Minnesota Department of Health (MDH), Section of Drinking Water Protection (DWP), collects, stores, and distributes data pertaining to Public Water Systems in the State. This data provides a valuable resource to various groups for planning and implementing programs to protect source water in the state, and may also be required reporting data to our federal Safe Drinking Water Act co-regulators.

Under Minnesota Statutes, Chapter 13, Section 13.37, the Minnesota Department of Health may determine that disclosure of certain data can jeopardize the security of: information, possessions, individuals, or property; through theft, tampering, improper use, trespass, or physical injury. MDH has determined that some of the data collected by DWP is non-public security information, and as such, special care must be taken to protect it.

This policy identifies this non-public security information, and sets requirements and restrictions on its use and distribution.

NON-PUBLIC SECURITY INFORMATION

The following information pertaining to Public Water Systems, which is collected, stored, or distributed by the Section of Drinking Water Protection, is considered non-public security data.

- Locational data of certain infrastructure components within a public water system can pinpoint a potential vulnerablity of the system. If a vulnerable infrastructure component is compromised through contamination, destruction, or other illegal activity, the health and welfare of individuals that use the drinking water would be at risk, as would the economy of the community involved.

Data indicating the location of the following infrastructure components of a drinking water system are considered non-public security information

- Wells
- Surface Water Intakes
- Treatment Facilities
- Storage Facilities
- Source Water Assessment Areas
- Inner Wellhead Management Areas
- 2000 Foot Buffers Of Public Water Systems
- Potential Contaminant Source Inventory

- The Environmental Protection Agency requires all community public water systems to perform assessments of their systems vulnerabilities. These assessments pinpoint vulnerabilities in the system that leave it open to contamination, destruction, or other illegal activity that would compromise the health and welfare of individuals using the drinking water, and the economy of the community involved. Vulnerability assessments are considered extremely sensitive data and are non-public security information.

- Emergency preparedness information, developed to guide Department staff during and after a disruptive event at a drinking water system, could be used by those planning illegal activities to thwart prevention and recovery activities. Emergency preparedness information is considered non-public security information.

- Data on treatments used by drinking water systems indicate specific chemicals that are used and stored at treatment plants or other system facilities. Many of these chemicals can cause serious contamination, or destruction if used improperly or illegally and could compromise the health and welfare of individuals using the drinking water, and the economy of the community involved. Data on specific treatments used in the water system are considered non-public security information.

- Engineering plans and specifications of drinking water system infrastructure provides information about layout and potential vulnerabilities of water systems. Access to this information could be used for illegal activity that could compromise the health and welfare of individuals using the drinking water, and the economy of the community involved. Engineering plans and specifications are considered non-public security information.

CONDITION OF USE

Security information can be distributed to Cooperative Data Partners (defined by Information Sharing Agreements) and Private Third Parties who agree to steward the information in accordance with the following:

- Information will be secured in a manner to preclude unauthorized access.
- Information will be used for internal business purposes or environmental assessment only, other uses are not authorized.
- Redistribution of information in any format is not permitted.
- Display of information on the Internet, or in publications or in public displays is not permitted without written permission.
- Information may be referenced in publications in summary form.

CONDITION OF INFORMATION

- Information is provided “as-is”. MDH makes no warranty, express or implied, and disclaims all implied warranties of the data for any purpose.
- MDH does not warrant that the information is error free. Security information was developed for MDH internal business purposes.
- MDH shall not be liable for any activity involving the information with respect to the following:
    - Lost profits, lost savings or any other consequential damages
    - The fitness of the information for a particular purpose
    - The installation of the information, its use, or the results obtained.