

## Allied Radio Matrix for Emergency Response (ARMER) Standards, Protocols, Procedures

Document Section 1	<b>Management of System</b>	<b>Status: Complete</b>
State Standard Number	<b>1.6.6</b>	
Standard Title	<b>Infrastructure Security: Data Classification</b>	
Date Established	<b>2/26/2009</b>	<b>SRB Approval: 2/26/2009</b>
Replaces Document Dated		
Date Revised		

### **1. Purpose or Objective**

The purpose of this standard is to define the classification of data about the ARMER system with respect to the Data Practices Act.

### **2. Technical Background**

Under the Minnesota Government Data Practices Act (MGDPA), data coming into the possession of the Minnesota Department of Transportation (MnDOT) is government data and presumed public unless exempted, excluded, or classified by state or federal law as something other than public. (Minn. Stat. Section 13.03, subd. 1).

No ARMER data is expressly defined as non-public by state law; however some data concerning the ARMER system has been determined to be “security information,” as defined in Minn. Stat. Section 13.37, which means that data is non-public.

Subdivision 1....(a) "***Security information***" means government data the disclosure of which would be likely to substantially jeopardize the security of information, possessions, individuals, or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury.

### **3. Operational Context**

ARMER data can be identified as security information if it meets the legal test for that classification, which means that disclosure of the data would cause substantial jeopardy. Some information about the ARMER system, if widely known and made easily available, could create an opportunity for thieves, vandals, or people wishing to disrupt public safety communications or ARMER system operations.

Even though some data may be available from independent sources, it is still valuable to restrict the distribution of ARMER data that is classified as security information to those individuals and agencies that need the information for business and to operate on the system.

The Statewide Emergency Services Board (SECB) is the expert source for an analysis of security needs concerning its data.

#### **4. Recommended Protocol/ Standard**

The following data about the ARMER system is identified as security data:

- Encryption keys
- Control channel frequencies associated with each site
- Zone controller locations (building, room, floor, address, etc.)
- Microwave path maps
- Precise geographic tower locations (latitude and longitude)
- System management resource manuals (State Standard 1.1.0)
- Technical resource manuals that contain the methods for performing detailed network operations (State Standard 1.2.0)
- Technical resource manuals and training materials that contain the methods for performing the database operations (State Standard 1.3.0)
- System manuals pertaining to security (State Standard 1.6.2)
- Fleetmap configuration information (the master fleetmap spreadsheets), including talkgroup IDs, user IDs, user privileges, and other related system information. (State Standard 2.6.0)
- Information in the master fleetmap spreadsheets for “unlisted,” private talkgroups used for undercover operations and other highly sensitive, confidential law enforcement activities (State Standard 2.6.0)
- Any radio code plug programming file, system key file, encryption key file, or any infrastructure configuration database file for any radio, console, or other infrastructure element on the system (State Standard 4.10.0)
- Draft audit findings under Section 7 of the State Standards
- Final audit findings under Section 7 of the State Standards should be reviewed for non-public data, and the data should be removed prior to release
- Other data as determined by the Statewide Radio Board and concurred with by MnDOT

The SECB may determine that some data, although public, should be considered sensitive and not posted on public web sites. When such data has been identified by the SECB, partner agencies should not release this data outside their agencies but should refer all requests to the owner of the data or MnDOT, Office of Electronic Communications (OEC).

#### **5. Recommended Procedure**

Security information, which is non-public data, should be handled as follows:

- Security information may not be included in the publicly posted meeting materials or minutes of the SECB, Regional Radio Boards (RRBs), or any partner agency.
- If it is necessary to discuss security information in an open meeting, handout materials should be distributed by confidential e-mail or by hard copy. Distribution

of the materials should be limited to those who are members of the committee or who otherwise need the information.

- Any public requests for data that is classified as security information must be directed to the agency that owns the data for any information about the ARMER backbone, a regional radio authority, or a partner agency with respect to information about a regional subsystem.
- Manuals should be reviewed to determine whether entire manuals or only parts of manuals are subject to security classification. Each manual determined to contain security information must contain notations similar to the following:

"This entire manual is (or sections of this manual are) classified as security information under Minnesota Statutes 13.37 and may not be shared publicly. Please consult the Minnesota Department of Transportation, Data Practices Office, before sharing with anyone whose work does not reasonably require access to these materials."

If only sections of documents are deemed to be security related, pages in those sections should be marked in some fashion.

Trade secret information is also considered non-public. Any information that is received that may be a trade secret will be submitted to MnDOT's Data Practices Office for review and possible classification as trade secret data under Minnesota Statutes 13.37, Subd. 1(b).

Data listed in Part 4 as "sensitive" should not be posted on websites, and any requests for sensitive information must be directed to the agency that owns the data for any information about the ARMER backbone, regional radio authority, or a partner agency with respect to information about a regional subsystem.

## **6. Management**

The SECB makes the determination that certain data, if released, would cause substantial jeopardy to the system, and the SECB shall periodically review the classification of data.

Data concerning the ARMER backbone is considered to be owned by MnDOT. Prior to making any changes in the data classification, the MnDOT Data Practices Specialist needs to be consulted and should concur with the proposed changes.