U.S. Department of Transportation
Federal Highway Administration

Memorandum

Subject **INFORMATION:** Electronic Security Issues--Kansas Department of Transportation's (KDOT) Construction Management System (CMS)

Date JUL 7 1993

From Chief, Construction and Maintenance Division
Office of Engineering

Reply to Attn of HNG-22

To Mr. Volmer K. Jensen
Regional Federal Highway Administrator (HRA-07)
Kansas City, MO

Mr. Eric B. White's June 8 memorandum requesting advice has been forwarded to the Construction and Maintenance Division for a response. Your request pertains to the Kansas Division's review and approval of KDOT's CMS. After a review of the attached materials we offer the following comments.

The KDOT appears to be basically establishing a computerized construction project information management system. While this type of system is currently being established in several States across the country, the distinction in Kansas is that they propose to take their system one step further and go totally paperless with the use of electronic signature technology.

Any computerized project record keeping system must meet certain criteria to ensure that the legal and financial interests of the Federal Government are protected. Such a system must be established so that the collection and retention of construction records are acceptable from an engineering, audit, and legal standpoint. These requirements should be no more stringent than they were for the hard copy system that the computerized system is replacing. In either case, the records must provide for the reconstruction of the chain of events that occurs on a project.

It appears, from the documentation provided by the Division Office's report, that the proposed KDOT CMS is acceptable from an engineering standpoint. It is replacing a paper system, maintaining essentially the same structure and audit trail that was acceptable and logical.

However, the KDOT's CMS, from an auditing and legal standpoint, appears highly suspect. The Division's report notes that within KDOT's various programs in the CMS there is an inability to verify who makes actual approvals via electronic signature. This is comparable to not being able to determine who signed the paper version of an approval letter or not being able to verify a persons handwriting with all the resulting legal implications.

FEDERAL HIGHWAY ADMINISTRATION 1893 1993

The GAO opinion that the Division referred to as only applying to electronic contracting was only one of two decisions that established the safeguards for electronic signatures. In the other decision, (B-238449), the Comptroller focused on the general use of an electronic signature rather than its specific use in contractual obligations. Both opinions were rather clear that the use of electronic signature technology had to be unique to the signer, under the control of the signer, have the capacity to be verified, and be a system of acceptable integrity. It appears that the KDOT's CMS does not meet this established criteria. A copy of both GAO decisions is attached for your information.

What is important in the use of electronic signature technology, is not so much the technology itself (i.e., hardware/software), but how the technology is used and more importantly how that use is controlled. These are the things one takes for granted in the uniqueness of a handwritten signature or more simply in a persons handwritten documentation. The computerized versions cannot be compromised any less, whether the documentation is created for contractual obligations directly or indirectly. If the documentation is something that is normally signed or is a record of information that needs to be identified with a specific user (inspector/project engineer, etc.), it is "official documentation" that must be supportable in a court of law.

The solution to the problem, as we see it, is relatively simple, implement "tighter computer security." This means control of user access in terms of ID's and passwords that are unique to **approved** users. Specifically, ID's and passwords should not be shared among a group of users, and the security codes must be changed periodically. Security of such computerized information systems cannot be compromised for the sake of convenience. We recommend the necessary security changes be implemented immediately.

The other important aspect of computer security is the adequacy of data and program system backups. The KDOT appears to have adequately addressed this issue with the procedures and routines required to backup their proposed system.

We trust that the above guidance satisfactorily addresses your concerns. If you have further questions or concerns please contact Mr. Robert S. Wright of my staff at (202) 366-1558.

William A. Weseman

Attachment

FHWA:HNG-22:RWright:tlf:60355:7/07/93
cc: Official File: 7202 Reader Files: HNG-1/HNG-20 Chron File: HNG-22
(Weseman) HNG-20 (Geiger) HNG-22 (Rockne) HNG-22 (Wright) HNG-22
(Swinford) HFS-30 (Park) HFS-31 HCC-32
Disk File: F:\DOCUMENT\HNG-22\RW\KDOT-CMS.MM2