TITLE 1 GENERAL GOVERNMENT ADMINISTRATION
CHAPTER 13 PUBLIC RECORDS
PART 70 PERFORMANCE GUIDELINES FOR THE LEGAL ACCEPTANCE OF PUBLIC RECORDS PRODUCED BY INFORMATION TECHNOLOGY SYSTEMS

1.13.70.1 ISSUING AGENCY: Commission of Public Records - State Records Center and Archives
[10/1/94; 5/15/97; 1.13.70.1 NMAC - Rn, 1 NMAC 3.2.70.1.1, 6/30/05]

1.13.70.2 SCOPE: All state agencies
[9/2/93; 5/15/97; 1.13.70.2 NMAC - Rn, 1 NMAC 3.2.70.1.2, 6/30/05]

1.13.70.3 STATUTORY AUTHORITY: Public Records Act 14-3-4 NMSA 1978
[9/2/93; 5/15/97; 1.13.70.3 NMAC - Rn, 1 NMAC 3.2.70.1.3, 6/30/05]

1.13.70.4 DURATION: Permanent
[10/1/94; 5/15/97; 1.13.70.4 NMAC - Rn, 1 NMAC 3.2.70.1.4, 6/30/05]

1.13.70.5 EFFECTIVE DATE: October 1, 1994 unless a later date is cited at the end of a section or paragraph.
[10/1/94; 5/15/97; 1.13.70.5 NMAC - Rn, 1 NMAC 3.2.70.1.5, 6/30/05]

1.13.70.6 OBJECTIVE:

A. Admissibility into evidence of records produced by information technology systems employing media such as magnetic tape or magnetic disk (and, by implication optical disk) has been addressed at the federal level by statutes and by the rules of evidence as adopted by the New Mexico supreme court.

B. Reported decisions indicate that the courts are quite lenient in interpreting these statutes and rules as applicable to records produced by information technology systems (analog or digital). However, problems arise if appropriate procedures are not followed in creating and maintaining such records, making it difficult to lay a proper foundation for admissibility. The court must be convinced that the process or system used is trustworthy in producing accurate records, i.e., the records reflect the source data used to create them. (Whether the source data are correct is a separate issue.)

C. The purpose of these guidelines is to provide direction for state agencies in the design, management, and operation of their information technology systems to improve the possibility of the admissibility into evidence of their records. The guidelines have been adapted for New Mexico by the commission of public records' legality of electronic records advisory committee composed of representatives from the supreme court law library, the office of the attorney general, the state bar of New Mexico, the general services department, and the state records center and archives. The guidelines were adapted from the association for information and image management's (AIIM) technical report: performance guideline for the legal acceptance of records produced by information technology systems (AIIM TR31-1992).
[9/2/93; 5/15/97; 1.13.70.6 NMAC - Rn, 1 NMAC 3.2.70.1.6, 6/30/05]

1.13.70.7 DEFINITIONS: The following definitions apply to the process or system assessment criteria set forth below:

A. Records: Information preserved by any technique in any medium, now known, or later developed, that can be recognized by ordinary human sensory capabilities either directly or with the aid of technology.

B. Original record: A record prepared in the first instance or any counterpart intended to have the same effect by a person executing or issuing it. If data are stored in a computer or similar device, any printout or other output readable by sight shown to reflect the data accurately is an "original."

C. Duplicate records: A record that is produced by the same impression as the original, or from the same matrix, or by any other technological device for producing or reproducing records.

D. Information technology system: Any process or system that employs a mechanical, photo-optical, magnetic, electronic or other technological device for producing or reproducing records.

E. Records custodian: The statutory head of the agency utilizing or maintaining the information system, or their designate.
[9/2/93; 5/15/97; 1.13.70.7 NMAC - Rn, 1 NMAC 3.2.70.1.7, 6/30/05]

1.13.70.8 EVIDENCE - BACKGROUND:

A. Traditional rules of evidence.

(1) Hearsay: Courts have traditionally classified records as "hearsay." Hearsay is a statement offered to show the truth of the matter asserted when the person who made the statement is not available for cross-examination. SCRA 11-801(C). Such records were initially excluded from evidence because they depended upon the veracity and competence of the out-of-court declarant. Later, through exceptions to the hearsay rule, courts admitted these records into evidence, when the records met the other established criteria for admissibility. These exceptions to the hearsay rule were based on the presumption that the public records reflected accurate information produced by trustworthy procedures. These exceptions were at first restricted to "original writings" but were later modified to accommodate impact printing and other duplication technologies (e.g., micrographics and photocopying machines) as they became common tools.

(2) The best evidence rule:

(a) The courts also developed the "best evidence rule." The rule generally states that only the best form of the evidence is admissible. Initially, only original documents were admissible. As the rule evolved, the courts allowed secondary evidence if it was shown that the original was unavailable without fault of the offering party. Early duplicate records were probably not admissible since they were made using the transcription process - the copying of records by hand involving human intervention. Due to the high likelihood of error, transcription could not produce trustworthy results.

(b) Over time, courts allowed true duplicate records - duplicates produced by mechanical or other non-human processes - to be admitted in evidence in limited circumstances when the originals were not available because:

(i) they were public records;
(ii) the originals had been destroyed;
(iii) the originals were in the possession of an adverse party who refused to cooperate; or
(iv) the originals simply could not be found with reasonable effort. Once these situations were adequately proven to the court, reproductions could then be admitted.

(c) Besides the historical basis for the best evidence rule, the preference for original records serves to reduce forgeries or other fraud in duplicates. Alterations can readily be detected in original documents while similar detection is difficult if not impossible in duplicates. Handwriting analysts can more accurately analyze signatures from original records than from duplicates.

(d) In New Mexico case law the relation between computer printouts and the best evidence rule is discussed in Sierra Life Ins. Co. v. First National Life Ins. Co. 85 NM 409, 412, 512 P.2d 1245, 1248 (1973).

B. Modern rules of evidence: The federal government follows the federal rules of evidence while most states have adopted one or more uniform laws that establish the admissibility of records in evidence. New Mexico has adopted the uniform rules of evidence with few changes. New Mexico's rules of evidence permit original and duplicate records to be admitted into evidence provided that a proper foundation is laid. For example, visible records produced with a computer in the form of computer printouts or computer output microfilm (COM) are considered originals if an appropriate witness can convince the court that they accurately reflect the information in the computer files. Information processing methods commonly employed in the business world are more readily accepted as reliable, while new information system technologies are subject to greater scrutiny.

C. Problems with rules of evidence.

(1) Based upon the traditional position of courts and regulatory agencies, original, paper records are the best evidence, and duplicate records are considered secondary evidence. Modern rules of evidence perpetuate this concept but provide exceptions for properly made duplicate records.

(2) The basic legal principle behind the best evidence rule is seldom applicable in the world of information technology. Paper records systems are often inferior to automated systems in terms of preserving evidence for the following reasons.

(a) Paper records systems generally result in the preparation of one copy of the record. In case of fire, flood, or other natural disaster, the single version of the records will be destroyed and no longer available for any evidence, regulatory or other purpose.

(b) Documents can be removed from paper records systems without detection. While erasures can be detected on originals, most other forms of fraud cannot. For example, when records are subpoenaed by the court or requested by government agencies, certain documents can be provided while others destroyed or hidden. The fraud resulting from the selective withholding of records can rarely be detected.

(3) Alternatively, original paper records can inappropriately be destroyed. These records may then be unavailable for any purpose including evidence and regulation. Unless the fraud related to the destruction is detected, the omission as well as the contents of the records will effectively be excluded from consideration.

(a) Original paper records may not have a very long life expectancy. This is especially true today because original paper records are often produced using poor quality paper, poor quality ink, lift-off

typewriter ribbons, or other inexpensive, short-term methods. Even records properly organized and stored may not be usable by the time they are needed for a court proceeding.

(b) Paper records are rarely created as part of a rigorous process or system. Many agencies do not have a records management program. Even those that do, rarely establish rigorous procedures related to records creation, maintenance and disposition. Many records created in each agency reflect individual whims rather than systematic policy. The accuracy of records will therefore vary based upon the integrity, accuracy and capabilities of the individuals involved.

(c) Paper records are rarely audited for accuracy. Few agencies audit paper records systems to determine the accuracy of the information recorded.

(d) Paper records are rarely subjected to adequate security. Any individual, including the janitor, may get access to paper records. The types of fraud discussed above can be accomplished without detection.

(4) Modern information technology systems often differ from paper-based systems through the establishment of processes or systems that reliably produce accurate results. Modern reproduction systems such as microfilm or optical disk, and even data processing systems, offer the following characteristics that generally provide for more accurate and trustworthy records than are possible with paper records systems.

(a) Modern information technology systems by their nature produce records as part of a process or system that requires a disciplined operation based on standard procedures, written documentation, adequate training, and thoroughly tested equipment and software components.

(b) Modern information technology systems can provide an audit trail that identifies not only what actions were taken related to records but also the individuals involved.

(c) Modern information technology systems can prohibit or detect alterations and attempted alterations to records. Most optical disk systems, for example, inherently preclude alteration of images. Bypass of alteration safeguards can be very difficult, requiring special knowledge and technical capabilities.

(d) Modern information technology systems can provide for routine security backup for records produced. Typically, microfilm, magnetic tape or disk, and optical disk systems will produce backup records at appropriate intervals as required. These records are generally stored in properly maintained remote locations where they can be retrieved if the original information is damaged or destroyed.

(5) In sum, properly designed, implemented and maintained information technology systems are capable of producing records that are more reliable and accurate than paper-based systems.

(6) It should be noted, however, that although paper-based systems are more susceptible to irretrievable loss or destruction of records and undetectable omissions, without the safeguards stated above, disasters and fraud can be much more costly and damaging to an agency dependent on an information technology system.

D. Further challenges.

(1) With the safeguards that can be built into today's modern information technology systems, the best evidence of a record should not be dependent on a specifically sanctioned technology, but on a showing that the record was the result of a process or system that accurately produced it.

(2) Rule 901(b) of the New Mexico rules of evidence lists examples that conform with the requirement of authentication or identification as a condition precedent to admissibility of evidence, i.e., "evidence sufficient to support a finding that the matter in question is what its proponent claims." Example (9) of Rule 901(b) reflects what should be the criteria for introducing records produced by information technology systems into evidence in all jurisdictions.

(3) Example (9) of Rule 901(b) provides for authentication or identification by "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." This example was designed for evidence such as x-rays and computer printouts where accuracy of the evidence is dependent upon the process or system that produces it.

(4) When applied to records produced by information technology systems, this provision has no bias towards originals, duplicates, or any particular technology. The accuracy of the process or system used to produce the result will determine the authenticity or identification, and hence the admissibility of the evidence.

(5) As new information technologies evolve, such as electronic imaging and optical disk systems, some jurisdictions feel compelled to modify existing laws or establish additional criteria for legal acceptance in evidence. It is important that New Mexico develop realistic and non-conflicting requirements.

(6) The performance guidelines represent reasonable criteria to provide for designing and operating information technology systems that insure accuracy, reliability, and ultimately, the trustworthiness of information. Once implemented, the guidelines can apply to future technologies.

(7) The guidelines relate to the functional or performance criteria for the system used to produce the records rather than to the media or specific technology involved. The trustworthiness of the process or system determines the legal admissibility of records in evidence, not the type of media or technology utilized.

[9/2/93; 5/15/97; 1.13.70.8 NMAC - Rn, 1 NMAC 3.2.70.1.8, 6/30/05]

1.13.70.9 APPLICABILITY: The guidelines apply to records produced by information technology systems regardless of the physical characteristics of the record media or technology employed. This includes records produced by any technique employing an information technology system as defined above.
[9/2/93; 5/15/97; 1.13.70.9 NMAC - Rn, 1 NMAC 3.2.70.1.9, 6/30/05]

1.13.70.10 INFORMATION TECHNOLOGY SYSTEM ASSESSMENT CRITERIA: Following are criteria for designing and operating an information technology system to improve the admissibility of records into evidence.

A. The issue of accuracy:

(1) These guidelines provide an analytical structure for validating electronic record systems with respect to the preservation of accuracy from the time of original source data capture until the time of record output. While the accuracy of the data that is passed to the system needs to be of concern to agencies, that issue can only be addressed after the reliability of the record management system is established. As such, the guidelines are only concerned with the integrity of record management processes as implemented within automation systems.

(2) While the guidelines do need to be applied to the entire record management process from the agency's receipt/creation of data until the eventual destruction of agency records, they are designed to be applied to individual subsystems which can be independently validated. This block structured approach allows a single subsystem to be changed without having to reexamine the entire process. It also facilitates the separation of original data accuracy and other record creation issues from those issues associated with the process of subsequent data manipulation and storage. Compliance with the guidelines will thereby ensure that the processes that agencies use to manage data do not jeopardize the legal admissibility of agency records, regardless of the accuracy of the original source material.

B. Quality: Quality relates to ability of the information technology system to reliably produce and preserve records so that they can be used or recognized by the intended audience.

(1) General requirements: The following should appear with sufficient clarity so that each can be recognized:

(a) individual letters, numbers and symbols;
(b) combinations of letters, numbers and symbols forming words or sentences;
(c) graphics such as signatures, logos, pictures, etc.;
(d) sounds;
(e) other features of records such as color, shape, texture, etc., that relate to the content of the information.

(2) Original records.

(a) Original records preserve information over time in the identical or functionally equivalent form to the original information.

(b) Original records may present information in a form different from the original information without affecting its quality. For example, information preserved in digital format may be printed on paper using different print fonts at different times.

(3) Duplicate records.

(a) Duplicate records accurately reproduce original records. Information that is readable or recognizable on originals should be readable or recognizable on duplicates. Similarly, information that is readable or recognizable on duplicates must be readable or recognizable on originals, except that duplicates may contain production, control, indexing, certification or other data not related to informational content of the records.

(b) The exception allows additional data to be included on duplicates for administration of the reproduction process if it does not adversely affect the informational content of the record. For example, control and indexing data stored with digital images may be necessary to retrieve the images, but does not affect the content of the records themselves.

(c) Image enhancement techniques may be used provided that they do not change the information content of the records.

(d) When duplication processes change informational content of the records, the resulting records will be new originals.

C. Records retention versus life expectancy of data on media:

(1) Records should be retained, regardless of media, for the period required by the agency's records retention program for any legal, user, historical or other purpose. The life expectancy of the media per se has no bearing on the admissibility of the records.

(2) The information maintained on the media and the ability of the system to produce records from the information must achieve the required retention period. This means that for some technologies it may be

necessary to periodically convert, regenerate, copy or transfer the information from one medium or technology to another to preserve the information for the required period.

(3) Regardless of the retention period or life expectancy of the media, records must continue to exist when litigation, government investigation or audit is pending, imminent or, in some cases, merely foreseeable. In some instances, a court order will issue prohibiting specified records from being destroyed or otherwise rendered unavailable.

(4) The life expectancy of the data on the media must be at least as long as the retention period established for the original record by the commission of public records, or there needs to be a provision in the system for the periodic reproduction of the data, or the periodic revitalization of the data on the media. (also see Subparagraph (b) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC)

D. Conversion of records: Procedures followed to convert records from one medium or technology to another should be carefully documented. Conversion of the records should not affect their legal status provided that quality and accuracy does not functionally change during conversion.

E. Form of evidence:

(1) Records should be presented in a readable or recognizable form acceptable to the court. For written records, the records may be readable without any equipment or readable using equipment available to the court. The court may also accept records in other forms when equipment for their retrieval and use is also provided.

(2) The form of records acceptable in evidence will vary based upon the nature of the information. For example, digitized voice information must be presented in an audible, understandable form while digitized video information must be presented in a readable or recognizable form. Records that contain information that relates to multiple human senses such as video records that must be both seen and heard to be complete must be presented in a form that provides all the necessary sensory information to the court.

(3) Records systems should be able to produce readable (by either visual or tactile means) or audible records regardless of the technology used.

F. Process or system used to produce records:

(1) **Characteristics of a process or system:** Characteristics of the process or system used to produce the information facilitate the accuracy of the information. A description of these characteristics in simple terms facilitates the showing that the process or system is reliable and accurate, and hence capable of producing trustworthy records. Each records system should regularly maintain and update complete documentation of both the collection (input) process and the output process.

(a) **Records produced as part of a regularly conducted activity:** Records produced as part of a regularly conducted activity such as those produced in the regular course of operations are more inherently reliable than those produced for a special purpose or for litigation. A regularly conducted activity may include a regular pattern of activity to produce the records on a daily, weekly, monthly, yearly or other cyclical schedule. A regularly conducted activity may also include records created as part of a regular program of the agency, but at irregular times. For example, records created as part of a retro-conversion project may still, in appropriate circumstances, be regarded as converted in the regular course of operations, even though it only occurred once.

(b) **Accuracy:** Accuracy may be increased by systematic quality control and audit procedures, as well as operational oversight by persons with detailed knowledge of the process or system used to produce the records.

(c) **Timeliness:** Records produced within a short period after the event or activity occurs tend to be more readily acceptable as accurate than records produced long after the event or activity. However, a challenge to admissibility of a later-produced record can be overcome by a showing that the time lapse had no effect on the record's contents. For example, a computer printout of a statistical report produced annually in the regular course of operations can be shown to accurately consolidate data compiled over the course of a year.

(2) **Components of a process or system:** The records program depends upon both the system's components and the processes used in preparing them. The records are more trustworthy if the program under which they were produced included adequate procedures, training programs, audit trails and audits.

(a) **Procedures:** Procedures reflect the detailed steps to be followed when creating, modifying, duplicating, destroying or otherwise managing records. They provide for consistent quality control, problem resolution and other activities that might otherwise be subject to inconsistent action, multiple interpretation or misinterpretation. Established procedures only show what an agency intended to do in managing and controlling the process or system. The trustworthiness of an agency's records depends not only upon established procedures but depend also on how closely they are followed. Deviations from established procedures will be scrutinized, and such deviations might result in the records being inadmissible.

(b) **Training programs:** Formal training programs for staff on details of the system procedures help insure that the procedures were correctly followed. When an agency can demonstrate that staff understood the required procedures, the court will tend to find that the procedures were in fact followed. It may be

advisable to provide certification of training for certain staff members prior to the staff members' assumption of responsibility for those procedures, especially for those who are likely to testify in court.

(c) Security controls: Effective security controls are essential for maintaining tamper free systems. An agency must be able to demonstrate to the court that security appropriate to the value and importance of the information was in place. Typical security controls would include varying levels of access secured by passwords, restricted terminal locations, physical security of processing equipment, and time use restrictions.

(d) Access and audit trails: Audit trails document who used the system, when they used it, what they did while using the system, and what were the results. Properly implemented audit trails can automatically detect who had access to the system, whether staff followed standard procedures or whether fraud or other unauthorized acts occurred or might be suspected. They provide independent confirmation that proper procedures were in fact followed. It may be advisable to provide various levels of access security.

(e) Audits: The term "audits" as used in this section is different than quality control specified in most system procedures. Audits performed periodically can confirm that the process or system produces accurate results. Audits should compare the procedures stated in the procedure's documentation with procedures actually followed. They provide verification that the system adheres to these guidelines. For purposes of establishing the credibility of the records, audits should be performed by an independent source, i.e., persons other than those who created the records or persons without an interest in the content of the records. Trained auditors with agency-wide audit responsibilities provide an acceptable level of independence. No particular method of auditing is required. For purposes of original records, audits should focus on whether the records accurately incorporate information of the acts, events, or activities leading to the record. For duplicates and other forms of information transfer, audits should confirm that the duplicates accurately reproduce the original information. Such audits must be accomplished prior to destruction of the originals. The destruction must be conducted in accordance with existing agency retention and disposition schedules.

(3) Documentation of a process or system: Documentation of the process or system provides verification of the process or system followed to produce the records. Without documentation, witnesses must rely solely on memory -- which over time becomes less trustworthy and more susceptible to contradiction. Documentation preserves the information about the process or system independent of the individuals involved. The documentation should always be reviewed by the agency witness prior to giving testimony. In a proper case, the documentation can be introduced into evidence.

(a) Content: knowledgeable person should prepare and maintain documentation for the process or system used to produce the records. Documentation should be prepared during the design of the system. If the system was implemented without documentation, documentation should be prepared immediately. Documentation should be kept of all changes in the system. All documentation of changes should be kept for the full retention period of the data. Documentation should be complete and up-to-date. This enables staff to know and follow the most current procedures. It also ensures that reliable system documentation is immediately available if needed for court proceedings. Documentation of a system prepared for purposes of litigation is subject to greater challenge. No particular form or level of detail is required for describing the process or system, although visual aids outlining the documentation can be helpful. Documentation should be sufficient to demonstrate the steps required to get from the beginning to the end of the process. Documentation should be understandable to non-technical personnel. Detailed documentation may be required by the courts. An agency may be required to introduce evidence that any equipment or software involved operated properly at the time the records were produced. Program documentation should state the control methods in force and how they are to be applied and should also state the times at which each part of a process is to be performed. Training documentation should record the distribution of written procedures, course materials, attendance of individuals at training sessions, remedial or refresher training programs, certifications of training completion and other relevant information. The actual audit trail records demonstrate what activities actually took place as part of the process or system. The actual audit reports indicate whether the records were accurately produced. Where audit reports have revealed inaccuracies, the documentation should reflect what remedial procedures were applied. The documentation should state who (by individual or job class) has access to the system at each level of access and should indicate how audit trails are maintained. Evidence of the actual system procedures followed during the period the records in question were produced should be maintained in sufficient detail to enable the records custodian to describe the process or system to the court.

(b) Retention: When the documentation changes, the old versions should continue to be maintained for the requisite period. The agency should establish procedures to insure that the Records Custodian is notified whenever a record needs to be maintained longer than its retention period.
[9/2/93, 10/1/94; 5/15/97; 1.13.70.10 NMAC - Rn, 1 NMAC 3.2.70.1.10, 6/30/05]

1.13.70.11 AVAILABILITY OF PROCESS OR SYSTEM FOR OUTSIDE INSPECTION:

A. The courts encourage pretrial discovery of computer programs and related materials in order to

facilitate effective cross examination when computer produced data are introduced into evidence. These guidelines apply this principle to records produced by any information systems technology.

B. Inspection:

(1) The process or system used to produce records introduced into evidence is subject to outside inspection by opposing parties and the court. Outside inspection may include review of procedures documentation, review of system operation, independent audits and quality control tests, independent audit, testing of process or system operation, review of equipment design and software documentation, review of training programs or any other matter related to the operation of the process or system.

(2) If the records were produced on the current or substantially similar system, access to the system may be required. Outside parties may request to process their own test data on the agency's system. If the system used to produce the records no longer exists, the court may require that all existing documentation be made available. Lack of pertinent documentation because it no longer exists may jeopardize admissibility of the records if their trustworthiness cannot otherwise be established.

(3) In sum, any relevant step of the process or system can be reviewed by the outside party.
[9/2/93; 5/15/97; 1.13.70.11 NMAC - Rn, 1 NMAC 3.2.70.1.11, 6/30/05]

1.13.70.12 LEGAL STATUS OF PUBLIC RECORDS OFFERED AS EVIDENCE:

A. The destruction of the original copy of a public record, after reproduction, will not affect the legal status of such reproduction as a public record.

B. An agency's ability to show that the process or system used to store and reproduce a public record is trustworthy in terms of producing an accurate result, will normally be sufficient to insure reliability.
[9/2/93; 5/15/97; 1.13.70.12 NMAC - Rn, 1 NMAC 3.2.70.1.12, 6/30/05]

1.13.70.13 TESTIMONY OF RECORDS CUSTODIAN: The records custodian is the statutory head of the agency that utilizes or maintains the information system. This responsibility may be delegated in appropriate circumstances down to the level of clerk. However, it is customary to have the individual who is responsible for the management of the information system documentation and operation provide testimony about the system. In some circumstances, it might be necessary to have the testimony of the individual who actually prepared the record.

A. Appearing in court: When records from an information system are required to be introduced in court, the level of proof may vary from simply certifying a record produced by the system to providing expert testimony about the operations of the system. When confronted with testifying in court, it is usually sufficient for a records custodian to provide for the following:

(1) copy of the record;

(2) documentation of the system;

(3) documentation of any variance of standard operating procedure in the production of the record, especially variations with respect to time and format.

B. Certification of records:

(1) Recommended form of certification: The following is a recommended form of certification: As a custodian of this record, I certify that it is a copy accurately recorded, maintained, and reproduced by this agency in accordance with the procedures attached hereto. This is page _____of_____ pages of certified document. This _____is certified on this _____day of _____.

_____
Records Custodian

(2) Sample certification procedure for data capture: The following is a sample certification procedure; it is meant to be suggestive only. An agency's certification procedure will vary according to the type and complexity of the system.
The (agency name) of the state of New Mexico has recorded the requested information using the following procedures:

(a) The original document/data containing the information requested was received in this office in the normal course of operations of the (agency name) carrying out its duties pursuant to the laws of the state of New Mexico. It was then (method of conversion/input) placed onto (method of storage).

(b) The accuracy of this production was verified at the time of conversion/input by comparison. The storage procedure allows the agency to determine whether the stored data was altered from the time of this document's conversion/input to the production of the attached (printout).

(c) Documents are converted/input from the original within _____ days after the original is received for official recordation or filing.

(d) Specifically as to the attached (printout), the following deviations from the above procedure are noted as follows: (none).

_____
Signature by Records Custodian of agency

(3) Sample certification procedure for data output:

The **(agency name)** has examined all records pertaining to data storage including audit trails, operations logs, and maintenance logs and has determined that there has been no purposeful alterations of the stored data and that there has been no hardware malfunctions that would compromise the integrity of the data.
Any deviations from standard operating procedure are noted as follows:

_____
Signature by Records Custodian of agency

C. Challenges to testimony: The testimony offered by the records custodian will vary based upon their own expertise, level of responsibility, and most especially any challenge offered to the introduction of the record. In appropriate cases and based on the nature of the challenge, it may be necessary to introduce expert witnesses. Information system records can be challenged on many grounds, a discussion of the most common grounds follow.

(1) Challenges to hardware: Because equipment which is not functioning properly can alter the content of computerized information, the reliability of the data processing equipment used to store and produce the records may be challenged. The information contained in the systems documentation should be sufficient to overcome this. However, if the hardware is challenged, it may be necessary to present evidence that the equipment operated reliably the day the data were initially entered and on the day the computer record was produced. A log of computer operations indicating the absence, or presence, of any malfunction that did or did not affect the data is generally adequate. The agency may also be required to produce a person who has actually tested the equipment.

(2) Challenges to software:

(a) Errors in computer records can result from errors in the computer programs. Consequently, the reliability of the computer programs and formulas used to process the data may be challenged. Normally, introduction of the systems documentation will be sufficient to demonstrate the reliability of the programs and formulas. However, evidence about the development and testing of the programs may also be required, as well as expert testimony from the creator of the software or from individuals who have run validation tests on the software.

(b) A records custodian may also be required to present the specific version of the computer program used to process the data on the date the information entered into evidence was created. A different version of the program may be considered, if it is the only one available, but the absence of the exact version of the program may raise some serious questions about the trustworthiness of the computer records.

(c) The measures taken to verify the proper operation and accuracy of these programs and formulas may be challenged. Normally, introduction of the systems documentation will be sufficient to demonstrate the verification of the programs and formulas. However, expert testimony from the creator of the software or from individuals who have run validation tests on the software may be required.

(3) Challenges to input:

(a) The manner in which the basic data were initially entered into the system may be challenged. The information contained in the systems documentation should be sufficient to demonstrate how the data were entered. However, if it is challenged, it may be necessary to produce a person who actually does data entry.

(b) Whether the data were entered in the regular course of operations may be challenged. The information contained in the systems documentation should be sufficient to overcome this. However, if it is challenged, it may be necessary to produce a person who actually does data entry, or who has audited the system.

(c) Whether the data were entered within a reasonable time after the events recorded by persons having knowledge of the events may be challenged. The procedures outlined in Paragraphs 13.3.3.A and 13.3.3.B above [now Subparagraphs (a) and (b) of this paragraph] of should be sufficient to overcome this. However, where the data are entered at a different time, then the agency's records should not only reflect the date the original data were created, but also the date they were entered.

(d) The measures taken to insure the accuracy of the data entered may be challenged. Normally, introduction of the systems documentation will be sufficient to demonstrate the accuracy of the data. However, it may be necessary to have expert testimony on verification, proof reading, internal audit trails, or computer security in general. It may be necessary as well to introduce the training records of the data entry staff.

(4) Challenges to output: Computer printouts prepared in the regular course of operations are considered more trustworthy than similar computer printouts prepared for trial. Consequently, the time and mode of preparation of printouts may be challenged. Normally, introduction of the systems documentation will be sufficient. However, where the printout is not created in the normal course of operations, an audit trail leading to the creation of the data may be required. If a specially written search or program was used to extract the data (as, for example, from a screen) the search or program should be included as well.

(5) Challenges to security: The method of storing the data (for example, magnetic tape) and the safety precautions taken to prevent loss of the data while in storage may be challenged. Backup only becomes an issue if it was used to generate the record. Where an agency is certifying that it does not have any record with regard to a transaction, it will usually be required to search not only the current systems but also the oldest backup that would be likely to contain such a record. Normally, introduction of the systems documentation will be sufficient to demonstrate the method of backup and storage. However, it may be necessary to obtain testimony concerning access to the system, what procedures were in place to prevent unauthorized access, and whether these procedures were carried out with respect to the records in question.
[9/2/93; 1.13.70.13 NMAC - Rn, 1 NMAC 3.2.70.1.13, 6/30/05]

1.13.70.14 INFORMATION TECHNOLOGY SYSTEM PERFORMANCE GUIDELINES CHECK-UP: This legality check-up will assist organizations to assess systems against New Mexico's Performance Guidelines for the Legal Acceptance of Public Records Produced by Information Technology Systems, 1.13.70 NMAC. It is designed to answer the question: How will records produced by our system stand up in court if called on to be used as evidence? Copies of this check-up are available in electronic format.

A.	**PART I: SYSTEM DESCRIPTION AND GENERAL ASSESSMENT INFORMATION**
1.	Agency and department responsible for records
2.	Agency and department maintaining system
3.	Type of storage technology (microfilm, optical disk, magnetic tape, etc.)
4.	Hardware and software components of the information system
5.	Briefly describe the public records maintained by the system and identify any information that is exempted from public inspection
6.	Who are the main users of the system (federal agencies, state agencies, private, etc.)
7.	Regulatory and other agencies which do or might review the system and records
8.	Rules, regulations and statutes governing maintenance of organization records
9.	Recommendations resulting from performance guidelines check-up
10.	Assessment conducted by: Date:

B. PART II: SYSTEM/PROCESS RELIABILITY. The following questions are designed to determine if the system under study is inherently capable of producing accurate records, as is required to enter the records produced into evidence. A negative response to any of the following questions may necessitate the maintenance of hard-copy source data for the purposes of legal documentation.

Performance Guideline Area	SRC Rule Reference	Assessment Question	Observations and Comments
11. Information Assessment	N/A	Does the system exist to provide information that fulfills the legal requirements of statutes and regulations? If no, describe system justification.	
12. Content and Completeness	N/A	Can the system provide the type and detail of information required by law? If no, describe limitations. _____ What are the consequences if the data maintained by the system is correct?	
13. Accuracy	N/A	Are the source records sufficiently accurate to insure utility of information for its intended purpose? If no, describe limitations. _____	

		Do the system's internal procedures and/or transformations preserve the accuracy of the source data? _____ Is the information recorded in the shortest reasonable time following events?	
14. Record Quality, General Requirements	Paragraph (1) of Subsection B of 1.13.70.10 NMAC	Do the following appear in the system's output with sufficient clarity to be recognized (answer each, state N/A if not appropriate): letters, numbers and symbols? words and sentences? graphics? sounds (if appropriate)? other? _____ For document capturing systems, is the entire source document captured? If not, describe any limitations, such as area constraints and drop-out ink. _____ For image capturing systems, is the image capture process free from the need of manual data editing (such as occurs in any OCR process)? If no, describe the manual processes involved.	
15. Record Quality, Original Records	Paragraph (2) of Subsection B of 1.13.70.10 NMAC	Are records produced by the system meant to be original records? If no, skip the rest of this block. _____ Describe any differences in form between the source material and the records produced by this system. _____ In conclusion, does the system preserve information over time in an identical or functionally equivalent form to the original information? (Specify either *No, Identical, or Functionally Equivalent.*)	
16. Record Quality, Duplicate Records	Paragraph (3) of Subsection B of 1.13.70.10 NMAC	Are records produced by the system meant to be duplicate records? If no, skip the rest of this block. _____ Describe any information added to the record that is not present in the original record. _____ Describe the resolution limitations of the reproduction process. _____ In conclusion, do duplicate records accurately reproduce their corresponding original records? In no, describe limitations.	
17. Record Quality, Conclusion	Subsection B of 1.13.70.10 NMAC	In conclusion, (i.e., in light of questions 14 thru 16), is the system free from any other limitations that would prevent the system from reliably producing and preserving records for use by the intended audience?	
18. Form of Evidence	Paragraph (1) of Subsection E of	Are the records produced written in nature? If no, skip the rest of this block. _____ Can the record be read without using any type of	

	1.13.70.10 NMAC	equipment? If no, describe the equipment necessary.	
19. Form of Evidence	Paragraph (2) of Subsection E of 1.13.70.10 NMAC	Does the system provide all the sensory and temporal information of the original records? In no, describe limitations. _____ If the records produced are other than written in nature, what senses do the records relate to and does it require a special expertise to interpret the output?	
20. Form of Evidence	Paragraph (3) of Subsection E of 1.13.70.10 NMAC	Does the system produce either readable (by either visual or tactile means) or audible records regardless of the technology used? If no, describe.	
21. System/Process Components, Audit Trails	Sub-paragraph (d) of Paragraph (2) of Subsection F of 1.13.70.10 NMAC	Does the system require its users to identify themselves in order to create or modify records? _____ Does this identification process require a password to be input?	
22. System/Process Components, Audit Trails	Sub-paragraph (d) of Paragraph (2) of Subsection F of 1.13.70.10 NMAC	Does the system provide automated audit trails? _____ Can automated audit trails detect unauthorized acts? _____ Do the automated audit trails record when a record is modified and who modified it? _____ Are operators and other users prohibited from modifying the audit trails?	
23. Availability of Process or System for Outside Inspection	Subsection A of 1.13.70.11 NMAC	If the system used to produce the records is currently in service, can the system be used for pretrial discovery by an adverse party or the court?	
24. Legal Status of Records Provided as Evidence	1.13.70.12 NMAC	In conclusion, can it be shown that the process or system is, in general trustworthy in producing accurate records (i.e., do the records produced reflect the source data used to create them, disregarding the accuracy of the source data). If not, describe any deficiencies or limitations not described above.	

C. PART III: CORRECTABLE FACTORS. The following questions are designed to determine if adequate controls and documentation exist for the system under study, as is required to prove that the system currently is and has been trustworthy in producing accurate records. A negative response to any of the following questions should be considered a deficiency that must be corrected if the records produced by the system are to be entered into evidence.

Performance Guideline Area	**SRC Rule Reference**	**Assessment Question**	**Observations and**

			Comments
25. Retention	N/A	Have critical points in the system/process data-flow been identified which would be subject to legal admissibility concerns? _____ Does a current state records center approved retention and disposition schedule exist for the records at the critical processing points? If not, how long are they kept? (The state records center should be contacted if a negative response is given to this question).	
26. Records Retention vs. Life Expectancy	Subsection C of 1.13.70.10 NMAC	Can the records be preserved and retrieved for the required retention period without the need for conversion, regeneration, copying, or transfer from one medium or format to another? If yes, skip to question 27. _____ Are procedures in place which define either: a) a fixed schedule for data regeneration or conversion? b) checkpoints for determining if and/or when data regeneration or conversion ic necessary?	
27. Conversion of Records	Subsection D of 1.13.70.10 NMAC	Can the records be preserved and retrieved for the required retention period without the need for conversion, regeneration, copying, or transfer from one medium or format to another? In yes, skip to question 28. _____ Are conversion procedures well documented with regards to their effect on data accuracy and quality? _____ Are the individual conversion processes performed well documented with regards to their effect on data accuracy and quality?	
28. System/Process Components, Procedures	Sub-paragraph (a) of Paragraph (2) of Subsection F of 1.13.70.10 NMAC	Do detailed procedures exist for at least the following operations (answer each): Record creation? Record modification? Record duplication? Record destruction? Consistent quality control? Problem resolution?	
29. System/Process Components, Procedures	Sub-paragraph (a) of Paragraph (2) of Subsection F of 1.13.70.10 NMAC	Is the system periodically tested? _____ On what frequency is the system testing performed? _____ Does the testing follow formal procedures? _____ Who performs the testing?	
30. System/Process Components, Training Program	Sub-paragraph (b) of Paragraph (2) of Subsection F of	Is there a formal training program for staff on system procedures? _____ Does the training program include measurement and documentation of learned skills? _____ Does the training program result in certification of key	

	1.13.70.10 NMAC	personnel? _____ Is training/certification required for all operational personnel? If no, describe.	
31. System/Process Components, Audit Trails	Sub-paragraph (d) of Paragraph (2) of Subsection F of 1.13.70.10 NMAC	Do automated audit trails record (answer each): Who used the system? When was it used? What they did during the use? Whether procedures were followed?	
32. System/Process Components, Audits	Sub-paragraph (e) of Paragraph (2) of Subsection F of 1.13.70.10 NMAC	Are periodic audits of the system conducted? _____ On what frequency are audits performed? _____ Are audits performed by an independent source? _____ Do the audits performed compare the procedures stated in the system documentation with the procedures that are actually followed? _____ For original records, do the audits focus on whether the records accurately incorporate information on the acts, events, or activities leading to the record? _____ For duplicates and other forms of information transfer, do the audits confirm that duplicate records accurately reproduce the original information?	
33. Documentation, Timeliness and Status	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC	Was the initial documentation prepared during the design and implementation of the system? If not, when was it prepared? _____ Are records kept of all changes to the system? _____ Is the system documentation up to date?	
34. Documentation, General Content	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC	Does the system documentation describe all operational steps? _____ Is the documentation understandable by non-technical personnel? If no, is it understandable by non-agency technical personnel?	
35. Documentation, Procedures	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10	Are all operational, maintenance, and testing procedures documented? _____ Does the documentation of these procedures include the times and places at which each part of the process is to be performed?	

	NMAC		
36. Documentation, Training	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC	Does the training documentation reflect (answer each): Distribution of written procedures? Course material used? Attendance records? Skill level measurement results? Remedial or refresher training programs? Certification of training? Other?	
37. Documentation, Security	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC	Does the security documentation record (answer each): Internal access controls? A description of levels of access? Physical access controls?	
38. Documentation, Audit	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC	Does the audit documentation record (answer each): Statistically valid samples? Results pertaining to accuracy? Remedial procedures?	
39. Documentation, Audit Trails	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC	Does the audit trail documentation describe (answer each): Who had access to the system? What levels of access are granted to each user? How audit trails are maintained?	
40. Documentation, Operations	Sub-paragraph (a) of Paragraph (3) of Subsection F of 1.13.70.10 NMAC	Are records maintained that describe system failures, malfunctions, and any corrective actions that are performed? _____ Are records maintained that describe changes in the system configuration and software versions? _____ Are records maintained that track the results of periodic system testing and/or calibration? _____ Are all operational records time stamped and authenticated by the appropriate personnel? _____ Who is responsible for maintaining documentation of system operations?	
41. Documentation, Retention	Sub-paragraph (b) of Paragraph	Is all system documentation, specifically including old versions of the documentation, maintained for the maximum retention period of any record produced by the system?	

	(3) of Subsection F of 1.13.70.10 NMAC	Is all system documentation maintained on archival quality media? Is the documentation archival schedule consistent with that of the electronic records archival schedule? Does a procedure exist to ensure the records custodian is notified whenever system documentation needs to be maintained longer than its current retention period, as to ensure that old versions of the documentation are maintained for the maximum retention period of any record produced by the system?	
42. Documentation, Conclusion	Paragraph (3) of Subsection F of 1.13.70.10 NMAC	In conclusion, is the system documentation maintained in sufficient detail to enable the records custodian to describe the process or system to a court?	
43. Certification of Records	Subsection B of 1.13.70.13 NMAC	Are certifications performed during the record capture process? Are certifications performed during record production? Does the certification process require the physical examination of selected samples of the records captured or produced? Does the certification process require the physical examination of all records captured or produced? Does the certification process require the physical comparison of at least selected samples of input records with their associated output records? Does the certification process require the physical comparison of all input records with their associated output records? Does the certification process require the review and consideration of all known operational anomalies? Who is responsible for the certification process?	

[10/1/94; 5/15/97; 1.13.70.14 NMAC - Rn, 1 NMAC 3.2.70.1.14, 6/30/05]

HISTORY OF 1.13.70 NMAC:
Pre-NMAC History: The material in this part was derived from that previously filed with the State Records Center:
SRC Rule 93-05, Performance Guidelines for the Legal Acceptance of Public Records Produced by Information Technology Systems, filed 9/2/93.

History of Repealed Material: [RESERVED]