Trustworthy Information Systems Handbook

State Archives Department
Minnesota Historical Society

Version 4, July 2002

Trustworthy Information Systems Handbook

Version 4, July 2002

www.mnhs.org/preserve/records/tis/tis.html

State Archives Department, Minnesota Historical Society
345 Kellogg Boulevard West
Saint Paul, Minnesota, 55102-1906

Shawn P. Rounds
Government Records Specialist
shawn.rounds@mnhs.org
651.259.3265

Mary P. Klauda
Government Records Specialist

The authors would like to acknowledge the valuable contributions made Jeryn A. Konezny, Esq., and the staff of the Minnesota State Archives, particularly Robert Horton, Angela Goertz, and Jennifer Johnson. This work was completed with funding from the National Historic Publications and Records Commission.

The Trustworthy Information Systems Handbook is an analytical tool, not intended to be a substitute for individualized legal advice. Professional legal advice should be sought for specific legal concerns and recommendations. The most current version of the Handbook is available online at: http://www.mnhs.org/preserve/records/tis/tis.html

Table of Contents

Section 1:
What's in it for you?

Good news! The *Trustworthy Information Systems Handbook* can help you—information systems developers, policy makers, and current and future system users—to be confident that your information systems can support accountability to elected officials and citizens by creating reliable, authentic, and accessible information and records.

The *Handbook* provides tools so you can:

- Understand why trustworthy information systems are important
- Apply statutory and legal mandates and policies to information management
- Evaluate the level of government accountability that your records and information embody
- Determine the importance of your government agency records and information
- Establish how much documentation or evidence in record keeping is adequate
- Use the trustworthy information systems criteria effectively

Records and information in government are extremely important for the following reasons:

- They facilitate government business
- They demonstrate government accountability
- They serve as evidence of government activity in Minnesota for current and future users of government information

In the face of the rapid growth of information technology, government information systems must demonstrate accountability through sound information management and documentation of government activity.

For these reasons, records in government need to be reliable and authentic. With electronic records and information in digital formats, we cannot demonstrate reliability and authenticity as easily as we can with paper records. We cannot see, touch, or examine electronic records in any intelligible way without the assistance of hardware and software. The *Handbook* provides the next best thing—the tools needed to examine government information systems for trustworthiness.

Keep reading to find out the best way to achieve information system trustworthiness for your government agency.

Section 2: How do you use this handbook?

Use this handbook to look at all of the technical and non-technical workings of information systems in order to determine the level of trustworthiness required of your system. The *Handbook* provides a thorough, effective, and practical set of tools to craft procedures based on the specific and unique needs and information requirements of your government agency.

The *Handbook* tools can help to answer:

- What is meant by a trustworthy system?
- What is the process for establishing trustworthiness?
- Who should participate in the process?
- Why are metadata and documentation so important?
- How important is your information?
- How do you use the Trustworthy Information Systems (TIS) criteria set?
- What are the criteria for a trustworthy information system?

The *Handbook* provides additional background and useful information, including:

- A glossary of terms
- A bibliography of sources that were the basis for the *Handbook*
- The methodology for developing and testing the TIS criteria
- Pertinent Minnesota laws and policies
- Relevant citations to case law
- Case studies of five government agency applications of the TIS criteria
- Citation of the *Handbook*

Use of the *Handbook* should not be limited to computer-based information systems, although they are the focus. Systems frequently are connected to, or interface with, other information systems in different formats, such as paper and microforms. They also may encompass legacy systems that contain similar data from an earlier time period and other platforms.

The *Handbook* can be applied to systems that contain *data*, *information* and/or *records*.

- *Data* simply asserts facts but provides no context for those facts. Data can be such items as the discrete elements in a field in a database or the dynamic components of a web page.

- *Information* has meaning to us based on the context of its creation and use. For example, customized reports from a database is information.

- *Records*, on the other hand, are accessed, understood, and retained as evidence of a particular situation or event. These could include the minutes from a meeting or all of

> the data captured to serve as evidence of an electronic commerce transaction. Though all of the elements of a record may exist within a single computer file, they may also be distributed across a network. The integrity of these elements and the links between them are much more important than where they physically reside.

You can use the *Handbook* at any time during information system development. It is never too late to think about system trustworthiness. However, the earlier during the system development life cycle that you consider its trustworthiness, the better off you'll be. During the analysis phase of system development, before a lot of time and money is spent on system design, is the most opportune time to weigh all of the TIS criteria that might be important to implement. At this time, you can think about the big picture without the constraints of a system that's already well along in development or operation.

That's the ideal, but most agencies don't have that luxury. The *Handbook* is useful at any point during the system development life cycle. The *Handbook* also can be used to examine the trustworthiness of systems that are already in place—your legacy systems. You can document what you presently have and establish how well the system is set up to meet various requirements. Information systems are not static; they must respond to changes all of the time. Changes in software, hardware, platforms, means of communications, and growth as systems are becoming more interconnected necessitate considering and revisiting the TIS criteria on a periodic basis.

The *Handbook* can be used for evaluating the trustworthiness of any government information system—large or small, old or new. It provides a valuable set of proven tools that your agency can apply, practically and efficiently. We encourage you to make this handbook your own!

Section 3:
What is a trustworthy information system?

Trustworthiness refers to an information system's accountability and its ability to produce reliable and authentic information and records.

We chose the term *trustworthy* because it denotes integrity, ability, faith, and confidence. We use trustworthiness to describe information system accountability. We use the words *reliable* and *authentic* when we talk about the information and records that the information system creates. Reliability indicates a record's authority and is established when a record is created. Authenticity ensures that a record will be reliable throughout its life, whether that lifetime lasts six months, ten years, twenty years, or forever.

Government creates a lot of information and records, in a variety of ways and formats, and for a number of reasons. The most obvious reason that we create records is simply to do our business, whether that business means running the Governor's office, managing the state's welfare system, or keeping track of spending for a county, city, school district, or township.

There's another reason for creating records: government accountability. Information and records generated in the course of government business must reflect government's accountability. Government reports and is accountable to its elected officials and, ultimately, to the people. Government records document and provide evidence that government is going about its business wisely or unwisely. They indicate whether government business gets managed and conducted properly in accordance with laws, statutes, regulations, and other requirements. Government records also document the history of our state; they contain valuable information about Minnesota's citizens and the social, economic, political, and natural environments in which we live.

Government accountability needs to be considered as information systems are developed. Computer-based information systems can do any number of tasks quickly and efficiently, but we don't always know who is accountable for these systems and the information that they create. The computer, unlike a human being, does not bear accountability for itself; people in government make information systems accountable. It follows, then, that in building information systems, we need to establish and create procedures, system documentation, and descriptions of system information as a means to make the system accountable.

We need trustworthy information systems to ensure our accountability as government agencies.

Section 4:
What is the process for establishing trustworthiness?

Establishing the trustworthiness of an information system typically takes several steps and requires the collaboration of people with a variety of skills and knowledge. The *Handbook*'s structure parallels the process and guides the reader along. Those undertaking the examination process for the first time are strongly encouraged to read through the entire handbook completely before beginning their project. Each successive step in the process builds on those before and it is important that none be slighted or skipped. The proper establishment of the trustworthiness of an information system depends on the completeness of the examination process.

Step 1:

- Assemble team (*Section 5: "Who should participate?"*)

Step 2:

- Document process (*Section 6: "Why are metadata and documentation important?"*)

Step 3:

- Determine the importance of the information in the system (*Section 7: "How important is your information?"*)

Step 4:

- Choose a criteria selection method (*Section 8: "How do you use the Trustworthy Information Systems criteria set?*)

Step 5:

- Select appropriate criteria (*Section 9: "What are the criteria for a trustworthy information system?"*)

Step 6:

- Implement and document choices (*Section 8: "How do you use the Trustworthy Information Systems criteria set?"*)

Section 5: Who should participate?

The *Handbook* encourages collaboration among a variety of people with diverse sets of skills and expertise. They are valuable assets in reaching your goal of information system trustworthiness.

Ideally, teams of agency personnel with a range of skills and knowledge will work together in this process. Your team should include people who have:

- Knowledge of agency and local government business, policy, and procedures. They know which laws and policies apply to your agency's information. Agency attorneys and auditors are valuable in this area.

- Knowledge of information access and data practices. They know who can access the information and for what reasons, and how long information needs to remain accessible. Agency records managers and the Minnesota State Archives can help in the process.

- Skills in computing, information technology, and information systems design. They can provide advice and propose options on what technologies and methodologies would work to accomplish business needs. Your information systems and technology staff, and even selected vendors, should be able to provide answers to questions.

The team should first be educated and made aware of the importance of information system trustworthiness and why the evaluation process is necessary. The team also needs to know the value of documenting their decisions, and they should be kept appraised of progress while system development is underway.

With a diverse and knowledgeable team assembled, you are on the right track for establishing information system trustworthiness.

Section 6: Why are metadata and documentation important?

Documentation and metadata serve as the fundamental foundation of any trustworthy information system, enabling proper data creation, storage, retrieval, use, modification, retention, and destruction.

Metadata can be simply defined as "data about data." More specifically, metadata consists of a standardized structured format and controlled vocabulary which allow for the precise description of record content, location, and value. Metadata often includes items like file type, file name, creator name, date of creation, and the data classification from the Minnesota Government Data Practices Act. Metadata capture, whether automatic or manual, is a process built into the actual information system.

Documentation has two meanings. On a broad level, it is the process of recording actions and decisions. On a system level, documentation is information about planning, development, specifications, implementation, modification, and maintenance of system components (hardware, software, networks, etc.). System documentation includes such things as policies, procedures, data models, user manuals, and program codes. Documentation capture is not a system process.

As discussed in Section 3 of this handbook (*What is a trustworthy information system?*), documentation and metadata establish accountability for information systems, and accountability goes hand-in-hand with trustworthiness—the ability to produce reliable and authentic records.

From the very beginning of your examination process, no matter where in the information system development life cycle you start, you must make a conscious effort to keep documentation. Documentation gathered after the fact always carries the possibility of incorrectness and/or incompleteness. Begin by gathering such information as:

- System name, owner, life cycle phase, purpose, etc.
- Rationale for the examination process
- Names and functions of team members
- Dates

As the examination process moves along, collect other documentation as appropriate. For example:

- Which version of the *Handbook* was used? (refer to *Appendix A*)
- Which criteria were selected? Why?
- Which criteria were not selected? Why?
- What were the responses to the various additional considerations?

- Who is responsible for implementation of the chosen criteria and each piece of supporting documentation?
- When were your choices implemented?

At the end of your initial system examination, you should have a complete record of your process and the choices you made along the way. By following up with consistent application of your choices and by maintaining the currency of your documentation as you make changes and revisit the criteria set, you will not only have an effective management tool for your system's proper administration, you will have evidence of its trustworthiness.

Bear in mind: complete documentation of an entire system is a daunting task that may not always be necessary for your particular situation—perhaps only certain functions need the careful attention outlined above. The value of your records must be weighed against cost and risk. The next section in the handbook (Section 7, *How important is your information?*) discusses this important step.

Section 7:
How important is your information?

Records and data are not all equally valuable. Therefore, not all information systems containing records will require the same security measures and levels of trustworthiness. In determining the importance of your information, you may want to consider such things as:

- What laws and regulations apply to your data?
- What are your industry's standards for system security, data security, and records retention?
- What areas and records might lawyers and auditors target?
- What data is of permanent and/or historical value to you and to others?

Certain policy mandates, such as the Minnesota Data Practices Act and others concerned with records management (refer to Appendix D), determine the precise value and security level of some information. These laws are written without respect to media or format. At present, however, there are no widely applicable models available for managing electronic records like there are for paper. The ever-increasing use of electronic records forces us to look at new ways to actually answer policy demands while efficiently using government resources.

Agencies should have some leeway to decide the significance of their records, their functional priorities, and the resources available to them as a basis for making informed choices about the appropriate practices to apply. The criteria set will help government agencies manage the risks associated with their information systems. While comprehensive in scope, the set will not apply to all systems equally. A system holding purchase orders, for example, will not have as high a legal profile and need for security and trustworthiness as one containing confidential medical information.

You must show that you have made informed choices that are appropriate for your records and that you have appropriate policies and procedures in place that are followed during the routine course of business—you are accountable for your actions. Lawyers and auditors, for instance, may examine your information systems in minute detail, looking for things like undocumented delays, variances from established procedures, and holes in your security in terms of access to your system and your records (refer to Appendix E for case laws regarding electronic records and to the Legal Risk Analysis Tool in Appendix G for additional assistance). These inquiries can be answered with documentation showing that you have examined your systems and have made informed decisions concerning the handling of your records.

So, you see, the criteria set is really a tool for risk management!

Section 8: How do you apply the Trustworthy Information Systems criteria?

The Trustworthy Information Systems (TIS) criteria can be used in many ways depending on your agency's particular situation. Use of the criteria varies depending on a number of agency-specific factors such as:

- Agency information needs and policies
- Information system size, type, and scope
- Phase of information system development life cycle
- Agency size, staff, and procedures

The TIS criteria set presents itself much like a cafeteria line, with a wide array of criteria choices in different categories. The costs for implementing any of the criteria vary. If you think about a cafeteria line, customers make choices based on their hunger, dietary needs, and budgets. Most customers think about all the risks of buying an item that's not in their budget or diet. If a customer buys two desserts along with an entree and a beverage, the result may be a stomach ache, a few extra pounds, or not enough money to go to a movie after dinner. For another customer, those two desserts may have no effect on their health, girth, or pocketbook.

In the TIS criteria cafeteria line, agency information system development teams face similar choices:

- What criteria items do we absolutely need to do our business and to meet information requirements?
- Which ones would be nice to have?
- What are the costs of implementing selected criteria?
- What are the costs (up-front and hidden) associated with not implementing them?

Agencies have different information needs and operate under different policy mandates and statutes. What's important to one agency may have little relevance to another.

When can you apply the criteria?

Obviously, establishing the trustworthiness of an information system is a process most easily undertaken during the analysis/planning phase before the design is nailed down.
The steps, in this instance, are to:

- Determine the value of your data
- Weigh that value against the costs (time, money, etc.) of implementing each criteria
- Choose only those criteria that support your determined level of risk
- Implement

- Document your choices (including handbook version, refer to Appendix A) and actions
- Reassess needs and risks on a regular basis

The criteria set can also be used to examine systems that are already in place—your legacy systems. Documentation of what you presently have can serve as a check on how well the system is set up to meet your various requirements. The steps in this instance are to:

- Decide the value of your data
- Examine your system with reference to the criteria
- Determine which are already in place
- Ask whether your current system configuration offsets your risks
- Choose additional criteria for implementation after weighing the costs
- Implement
- Document your choices (including handbook version, refer to Appendix A) and actions
- Reassess needs and risks on a regular basis

Who has used the criteria?

Four state agencies and one local government agency used the TIS criteria set during the *Handbook*'s draft/testing phase. The agencies, representing a variety of government business and information needs and policies, agreed to let the State Archives field test the criteria set on their information systems projects.

The systems were at various phases in the system development life cycle. Each of the agency development teams found the criteria useful and relevant to their particular situation. You can read more about the field test cases in the *Appendices* section. The test case descriptions will give you an idea of how you might want to get started using the criteria. Keep in mind, however, that you don't need to choose the same criteria or use the same methods as these agencies. Remember: What worked for one agency may not work for yours.

Upon its publication, Minnesota's Information Policy Council began recommending the *Handbook*'s use by state agencies. As a result, a number of governmental entities have incorporated the TIS methodology into their systems development process. As well, the Ohio Electronic Records Committee has adapted the *Handbook* for use within that state.

What tools are available to help?

The Legal Risk Analysis Tool (refer to Appendix G, only available online) will assist you in assessing the legal risks associated with your data. The TIS criteria worksheet form (refer to Appendix G) was useful for recording information during agency field test evaluation sessions. The form lists all of the criteria in table format (Microsoft Word 2000) and contains sections for recording evaluation responses to each criteria.

Any time is the right time to start considering the information system trustworthiness. So, let’s jump into the criteria set.

Section 9:
Criteria for Trustworthy Information Systems

The following criteria outline the best available practices for implementing a trustworthy information system. The most appropriate practices for a particular system may comprise only a certain number of these. Agencies choose what is reasonable and practical depending on a variety of factors. The important point is to make, justify, and document your choices in order to ensure consistent application and your agency's accountability for its decisions.

The criteria range from system- to record-level and are categorized into five main groups:

- system documentation
- security measures
- audit trails
- disaster recovery plans
- record metadata

Each of these areas contain specific criteria as well as items for further consideration:

- *Did You Know* highlights items drawn from Minnesota government sources concerning information systems and records management.

- Points under *Consider This* expand upon the criteria.

- The left-hand sidebar offers general *Questions to Ask* while working with the criteria set; those opposite a particular criteria group are complementary to its issues.

The criteria set will be updated as necessary to reflect new information. Sources are listed in the *Bibliography* section of this handbook.

QUESTIONS TO ASK

- What laws and/or regulations (state and federal) apply to the data within your system?

- What are your industry's standards for system security?

- What are your industry's standards for data security?

- What areas/records might lawyers target?

- What areas/records might auditors target?

- What data falls under the Minnesota Government Data Practices Act?

- What data is of permanent/historical value to you and/or to others?

Criteria Group 1: System administrators should maintain complete and current documentation of the entire system.

Questions to Ask

- What is the system's unique identifier and/or common name?
- What is the agency and department responsible for the system?
- What is the agency and department responsible for applications?
- What is the name and contact information of the person(s) responsible for system administration?
- What is the name and contact information of the person(s) responsible for system security?
- Has a formal risk assessment of the system been completed? Date? Performed by? Methodology? Findings?
- Were design reviews and system tests run prior to placing the system in production? Were the tests documented?
- Is application software properly licensed for the number of copies in use?
- If connected to external systems lacking commensurate security measures, what mitigation procedures are in place?
- What other systems might records be migrated to?

1A. System documentation should include, but is not limited to:

1. hardware (procurement, installation, modifications, and maintenance)
2. software (procurement, installation, modifications, and maintenance)
3. communication networks (procurement, installation, modifications, and maintenance)
4. interconnected systems
   a. list of interconnected systems (including the Internet)
   b. names of systems and unique identifiers
   c. owners
   d. names and titles of authorizing personnel
   e. dates of authorization
   f. types of interconnection
   g. indication of system of record
   h. sensitivity levels
   i. security mechanisms, security concerns, and personnel rules of behavior

Did You Know:

☑ "Agencies shall take reasonable measures to ensure that only agency authorized computer equipment is installed on or connected to state systems and that only approved software is installed or executed on state computer resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

Consider This:

➥ System documentation, including specifications, program manuals, and user guides, should be covered in retention schedules, and retained for the longest retention time applicable to the records produced in accordance with the documents.

- ➥ Unique names and identifiers should remain the same over the lifetime of the units to allow tracking.
- ➥ When a system is installed at more than one site, steps should be taken to ensure that each site is running an appropriate, documented, up-to-date version of the authorized configuration.
- ➥ Audit trails of hardware and software changes should be maintained such that earlier versions of the system can be reproduced on demand.
- ➥ A process should be implemented to ensure that no individual can make changes to the system without proper review and authorization.

1B. Policy and procedure documentation should include, but is not limited to:

1. programming conventions and procedures
2. development and testing activities, including tools

   Consider This:

   - ➥ Periodic functional tests should include anomalous as well as routine conditions, and be documented such that they can be repeated by any knowledgeable programmer.

3. applications and associated procedures such as methods of entering/accessing data, data modification, data duplication, data deletion, indexing techniques, and outputs
4. identification of when records become official
5. record formats and codes
6. routine performance of system back-ups. Each back-up should be documented with back-ups being appropriately labeled, stored in a secure, off-line, off-

site location, and subjected to periodic integrity tests.

7. routine performance of quality assurance and control checks, as well as performance and reliability testing of hardware and software on a schedule established through consultation with the manufacturers

   Consider This:

   ➥ Identification devices (e.g., security cards) should be included in periodic testing runs to ensure proper functioning and to verify the correctness of identifying information and system privilege levels.

   ➥ Each type of storage medium used should undergo regular statistical sampling following established procedures outlining sampling methods, identification of data loss and corresponding causes, and the correction of identified problems.

8. migration of records to new systems and media as necessary. All record components should be managed as a unit throughout the transfer.

9. standard training for all users and personnel with access to equipment

   Did You Know:

   ☑ "The agency head shall ensure that agency employees understand the importance of security measures and their role in sharing the responsibility for the security and integrity of state computerized information resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   ☑ "Agencies shall make a copy of the state Security Policy available to each agency employee and shall make all employees, contractors, and information users aware of their responsibilities under the state Security Policy and the agency security plan." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "The agency head shall ensure that each agency employee is aware that violation of the principles of the state Security Policy or the agency security plan could be cause for disciplinary action or termination from employment." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

Consider This:

➥ Users should sign statements agreeing to terms of use. Such a document should include guidelines for: user responsibilities and expected behavior, consequences of inconsistent behavior or non-compliance, remote-access use, Internet use, use of copyrighted works, unofficial use of resources, assignment and limitations of system privileges, and individual accountability.

Criteria Group 2: System administrators should establish, document, and implement security measures.

Questions to Ask

- Who can invoke change mechanisms for object, process, and user security levels?
- Who (creator, current owner, system administrator, etc.) can grant access permissions to a record after the record is created?
- Is there a help desk or group that offers advice and can respond to security incidents in a timely manner?
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is there a list of all internal and external user groups and the types of data created and/or accessed?
- Have all positions been reviewed with respect to appropriate security levels?
- What are the procedures for the destruction of controlled-access hard copies?
- How is information purged from the system?
- How is reuse of hardware, software, and storage media prevented?

2A. User Identification / Authorization

1. User identification and access procedures should be established and documented. Users should be authenticated prior to being granted access.

   Did You Know:

   ☑ "Agencies shall limit access to computerized information resources and computer systems to authorized users." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   ☑ "Agencies shall identify and control each point of access to computerized information or computer systems by an appropriate security method." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   ☑ "Agencies shall establish and use appropriate authentication methods to ensure each user is identified prior to granting access to computerized information resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

2. Each user should be assigned a unique identifier and

password. Identifiers and passwords should not be used more than once within a system. Use of access scripts with embedded passwords should be limited and controlled.

Did You Know:

☑ "Authorized users of computerized information resources shall not disclose their means of authentication." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/ handbook/standard/standard.html]

Consider This:

➥ Upon successful log-in, users should be notified of date and time of last successful log-in, location of last log-in, and each unsuccessful log-in attempt on user identifier since last successful entry.

➥ Where identification codes in human-readable form are considered too great a security liability, other forms should be employed such as encoded security cards or biometric-based devices.

3. Password rules should include standard practices such as minimum password length, expiration dates, and a limited number of log-on attempts. System administrators should determine what level and frequency of log-on error constitutes a misuse problem which, in turn, would trigger the notification of security personnel.

4. Users should be restricted to only the level of access necessary to perform their job duties.

5. Permission to alter disposition/retention codes, and/or to create, modify, and delete records should be granted only to authorized users with proper

clearance. Modification of record identifiers is not allowed.

6. Access to private keys for digital signatures should be limited to authorized individuals.

Did You Know:

☑ "Each agency that chooses to use digital signature technology must establish a digital signature implementation and use policy." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/ handbook/standard/standard.html]

☑ "An individual must protect and not disclose or make available his or her digital signature private key or password to other persons, including fellow state employees, managers, and supervisors." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/ handbook/standard/standard.html]

☑ "When conducting State business, an employee must only use a digital signature key pair and certificate purchased with state funds. Employees must not use a State digital signature key pair for personal business." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/ handbook/standard/standard.html]

☑ "The agency must revoke the ex officio digital signature key pair whenever there is a change in the person occupying the office." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

7. Lists of all current and past authorized users along with their privileges and responsibilities should be maintained. The current list should be reviewed on a regular schedule to ensure the timely removal of authorizations for former employees, and the adjustment of clearances for workers with new job duties.

8. Personnel duties and access restrictions should be arranged such that no individual with an interest in record content will be responsible for administering system security, quality controls, audits, or integrity-testing functions. No individual should have the ability to single-handedly compromise the system's security and operations.

2B. Internal System Security

1. Access to system documentation should be controlled and monitored.

2. Access to output and storage devices should be controlled and monitored.

3. Controls should be in place to ensure proper security levels of data when archiving, purging, or moving from system to system. Controls should be in place for the transportation or mailing of media or printed output.

4. Procedures should be implemented to ensure the complete sanitization and secure disposal of hardware, software, and storage media when outdated or supplanted by newer versions, units, etc. Documentation should include date, equipment

identifiers, methods, and personnel names.

5. Insecurity-detection mechanisms should be constantly monitoring the system. Failsafes and processes to minimize the failure of primary security measures should be in place at all times.

6. Security procedures and rules should be reviewed on a routine basis to maintain currency.

7. Measures should be in place to guard the system's physical security. Items to consider include:
   a. access to rooms with terminals, servers, wiring, backup media
   b. data interception
   c. mobile/portable units such as laptops
   d. structural integrity of building
   e. fire safety
   f. supporting services such as electricity, heat, air conditioning, water, sewage, etc.

8. Security administration personnel should undergo training to ensure full understanding of the security system's operation.

2C. External System Security

1. In cases of remote access to the system, especially through public telephone lines, additional security measures should be employed. Possible action could include the use of input device checks, caller identification checks (phone caller identification), call backs, and security cards.

2. For records originating outside the system, the system should be capable of verifying their origin and integrity. At a minimum, the system should:
   a. verify the identity of the sender or source
   b. verify the integrity of, or detect errors in, the transmission or informational content of the record
   c. detect changes in the record since the time of its creation or the application of a digital signature
   d. detect any viruses or worms present

Did You Know:

☑ "Organizations conducting business over the Internet need robust security controls to ensure data integrity, data confidentiality, and system availability. Data integrity controls help protect the accuracy and completeness of data, both in storage and while in transit. Confidentiality controls help ensure that sensitive data, such as credit card numbers, cannot be seen by unauthorized individuals. Finally, system availability controls help minimize the amount of time when citizens cannot use the system to conduct business." (Office of the Legislative Auditor, *Financial-Related Audit: Department of Public Safety, Web-Based Motor Vehicle Registration Renewal System as of April 2001*. August 2001, Report No. 01-43.) [http://www.auditor.leg.state.mn.us/]

☑ "It is a sad reality that unscrupulous individuals discover new discover new security exploits daily and use that knowledge to penetrate organizations with many layers of preventative defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. Since time is of the essence when under attack, every organization must also have decisive incident response procedures. Those that do not may fail to discover that they are completely unsecured until extensive damage has been done." (Office of the Legislative Auditor, *Financial-Related Audit: Department of Public Safety, Web-Based Motor Vehicle Registration Renewal System as of April 2001*. August 2001, Report No. 01-43.) [http://www.auditor.leg.state.mn.us/]

☑ "Agencies shall take appropriate preventative actions to protect their computer information from corruption by viruses." (Minnesota Department of Administration, Office of Technology, *Computerized Information*

Resources Security Standards for State Agencies. IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "Agencies shall monitor and evaluate, on an ongoing basis, the effectiveness of security tools and virus protection being used within their agency. Security tools and virus protection systems which are not found to be effective shall be updated in a timely manner." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

Criteria Group 3: System administrators should establish audit trails that are maintained separately and independently from the operating system.

Questions to Ask

- Who can access audit data? Alter? Delete? Add?
- How can the audit logs be read? Who can do this?
- What tools are available to output audit information? What are the formats? Who can do this?
- What mechanisms are available to designate which activities are audited? Who can do this?
- How are audit logs protected?

3A. General characteristics of audit trails include:

1. Audit trail software and mechanisms should be subject to strict access controls and protected from unauthorized modification or circumvention.

2. Audit trails should be backed up onto removable media periodically to ensure minimal data loss in case of system failure.

3. System should automatically notify system administrators when audit storage media is nearing capacity and response should be documented. When the storage media containing the audit trail is physically removed from the system, the media should be physically secured as required by the highest sensitivity level of data it holds.

Consider This:
↪ If audit trails are encoded to conserve space, the decode mechanism must always accompany the data.

3B. A system should be in place to track password usage and changes. Recorded events and information should include:

1. user identifier
2. successful and unsuccessful log-ins
3. use of password changing procedures
4. user ID lock-out record
5. date
6. time
7. physical location

3C. A system should be in place to log and track users and their online actions. Audit information might include:

1. details of log-in (date, time, physical location, etc.)
2. creation of files/records
3. accessed file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/ security level)
4. accessed device identifiers
5. software use
6. production of printed output
7. overriding of human-readable output markings (including overwrite of sensitivity label markings and turning off of labeling mechanisms) on printed output
8. output to storage devices

Did You Know:

☑ "The agency head shall ensure that users are aware that their use of computerized information resources is traceable." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "Agencies shall ensure that computer access points to systems connected to the state network require and access control process that can be audited." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "Where appropriate, agencies shall log access to data in such a way as to permit an agency to audit its access to computerized information resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ ot_files/handbook/standard/standard.html]

☑ Users must be supplied with the Tennessen Warning when collecting confidential, private data by any means. (Minnesota. *Chapter 13 (Government Data Practices, 13.04, subdivision 2). Statutes*. 1998.) [http://www.revisor.leg.state.mn.us/stats/13/]

3D. For each record, audit trails should log, at a minimum, the following information:

1. record identifier
2. user identifier
3. date
4. time
5. usage (e.g., creation, capture, retrieval, modification, deletion)

Criteria Group 4: System administrators should establish comprehensive disaster and security incident recovery plans.

4A. Disaster and security incident recovery plans should be periodically reviewed for currency and tested for efficiency.

Did You Know:

☑ “Agencies shall ensure the backup, transport, storage, and recovery of their computerized information resources.” (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ “Agency heads shall ensure that security policies are included in their Disaster Recovery Plans.” (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

4B. Security incident recovery plans.

1. Hazards include:
   a. hardware failure or malfunction
   b. software failure or malfunction
   c. network failure or malfunction
   d. human error
   e. unauthorized access and activity

2. Government agencies should contact the Minnesota Department of Administration, InterTechnologies Group for assistance with incident-handling procedures and support.
   a. Information regarding the Minnesota Computer Emergency Response Team (MNCert) is available from James Johnson (651.296.6364; james.johnson@state.mn.us) and Arik Nelson (651-296-6361).

3. Related resources include :
    a. CERT Coordination Center
       [http://www.cert.org]

4C. Disaster recovery plans.

1. Hazards include:
    a. fire and/or explosion
    b. water or flood
    c. wind or tornado
    d. lightening
    e. power outage
    f. rodents
    g. insects
    h. human error
    i. violence and/or terrorism

2. Government agencies should contact the Minnesota Department of Administration, InterTechnologies Group, Business Continuation Management (BCM) Unit.
    a. The BCM can assist with:
        1. business impact analysis
        2. recovery strategy development
        3. plan development
        4. training
        5. plan test coordination
        6. plan maintenance
    b. Information regarding the BCM and ts services is available at: [http://www.mainserver.state.mn.us/bcm/]

3. Related resources include:
    a. Minnesota State Archives' record storage and disaster preparedness guidelines available at: [http://www.mnhs.org/preserve/records/recser.html#guides]

    b. Federal Emergency Management Agency (FEMA), emergency response and recovery guidelines available at: [http://www.fema.gov/r-n-r/ers_wl.htm#]

Criteria Group 5: Each record and/or record series should have an associated set of metadata.

QUESTIONS TO ASK

- What are the components of a complete or final record of a transaction?
- What are the minimum components necessary to provide evidence of a transaction? If you went to court, what would be the minimum information you would need?
- Are there any laws, regulations, or professional best practices that specify the structure (including medium, format, relationships) of the record of a transaction or any of its components?
- What information is necessary to interpret the contents of a record?
- During which agency business processes might you have to access a record?
- Who are the external secondary users of your records?
- What are the rules, laws, and regulations that restrict or open access to these records to external secondary users?
- What are the procedures for reproducing records for use by secondary users? What are the reproduction formats?
- Is there a mechanism to indicate sensitivity level on hardcopies? Who can enable/disable this function?
- What are your industry's standards for records retention?

Did You Know:

☑ The *Minnesota Recordkeeping Metadata Standard* is administered by the Minnesota Department of Administration, Office of Technology, as IRM Standard 20. The standard is geared to Minnesota government entities at any level of government. It includes both mandatory and optional elements, and may be applied at either the record or record series level. The standard is referenced in the *Minnesota Enterprise Technical Architecture* under Chapter 4, "Data and Records Management Architecture." [http://www.ot.state.mn.us]. For a complete discussion of the standard's purpose, structure, and requirements, see [http://www.mnhs.org/preserve/records/metadatastandard.html].

5A. The Minnesota Recordkeeping Metadata Standard includes twenty elements. Each is listed below along with associated sub-elements and the obligation for implementation.

1. **Agent** (** mandatory)
Definition: An agency or organizational unit responsible for some action on or usage of a record. An individual who performs some action on a record, or who uses a record in some way.
    1.1 Agent Type (mandatory)
    1.2 Jurisdiction (mandatory)
    1.3 Entity Name (mandatory)
    1.4 Entity ID (optional)
    1.5 Person ID (optional)
    1.6 Personal Name (optional)
    1.7 Organization Unit (optional)
    1.8 Position Title (optional)
    1.9 Contact Details (optional)
    1.10 E-mail (optional)
    1.11 Digital Signature (optional)

2. **Rights Management** (** mandatory)
Definition: Legislation, policies, and caveats which

- What is the records disposition plan?
- Who is responsible for authorizing the disposition of records?
- Who is responsible for changes to the records disposition plan?
- How does the system accommodate integration of records from other systems?
- Who can access record metadata? Alter? Delete? Add?

SPECIAL QUESTIONS FOR DATA WAREHOUSES

- Do you gather extraction metadata?
- Do you cleanse the data? Do you document the procedure? Do you gather cleansing metadata?
- Do you transform the metadata? Do you document the procedure? Do you gather transformation metadata?
- What metadata and/or documentation do you offer users?
- Who can access metadata? Alter? Delete? Add?
- What are the legal liabilities regarding data ownership and custodial responsibilities? Where do data custody responsibilities reside – with the source systems, the warehouse system, or both?
- Are there records retention schedules and policies for warehouse data? Is retention of warehouse data coordinated with retention for data extracted from the source systems?

govern or restrict access to or use of records.

2.1 MGDPA Classification (mandatory)
2.2 Other Access Condition (optional)
2.3 Usage Condition (optional)
2.4 Encryption Details (optional)

3. **Title** (** mandatory)
Definition: The names given to the record.

3.1 Official Title (mandatory)
3.2 Alternative Title (optional)

4. **Subject** (** mandatory)
Definition: The subject matter or topic of a record.

4.1 First Subject Term (mandatory)
4.2 Enhanced Subject Term (optional)

5. **Description** (optional)
Definition: An account, in free text prose, of the content and/or purpose of the record.

6. **Language** (optional)
Definition: The language of the content of the record.

7. **Relation** (optional)
Definition: A link between one record and another, or between various aggregations of records. A link between a record and another information resource.

7.1 Related Item ID (mandatory)
7.2 Relation Type (mandatory)
7.3 Relation Description (optional)

8. **Coverage** (optional)
Definition: The jurisdictional, spatial, and/or temporal characteristics of the content of the record.

8.1 Coverage Type (mandatory)
8.2 Coverage Name (optional)

9. **Function** (optional)
Definition: The general or agency-specific business function(s) and activities which are documented by the record.

10. **Date** (** mandatory)
Definition: The dates and times at which such fundamental recordkeeping actions as the record's or records series' creation and transaction occur.

10.1 Date/Time Created (mandatory)
10.2 Other Date/Time (optional)

11. **Type** (optional)
Definition: The recognized form or genre a record takes, which governs its internal structure.

12. **Aggregation Level** (** mandatory)
Definition: The level at which the record(s) is/are being described and controlled. The level of aggregation of the unit of description (i.e., record or record series).

13. **Format** (optional)
Definition: The logical form (content medium and data format) and physical form (storage medium and extent) of the record.
13.1 Content Medium (mandatory)
13.2 Data Format (mandatory)
13.3 Storage Medium (mandatory)
13.4 Extent (optional)

14. **Record Identifier** (** mandatory)
Definition: A unique code for the record.

Did You Know:
☑ Under the Minnesota standard, modified records are considered new records and are thus assigned new identifiers.

15. **Management History** (** mandatory)
Definition: The dates and descriptions of all records management actions performed on a record from its registration into a recordkeeping system until its disposal.
15.1 Event Date/Time (mandatory)
15.2 Event Type (mandatory)
15.3 Event Description (mandatory)

16. **Use History** (optional)
Definition: The dates and descriptions of both legal and illegal attempts to access and use a record, from the time of its registration into a recordkeeping system until its disposal.
16.1 Use Date/Time (mandatory)
16.2 Use Type (mandatory)
16.3 Use Description (optional)

17. **Preservation History** (optional)
Definition: The dates and descriptions of all actions performed on a record after its registration into a recordkeeping system which ensure that the record remains readable (renderable) and accessible for as long as it has value to the agency and to the community at large.

17.1 Action Date/Time (mandatory)
17.2 Action Type (mandatory)
17.3 Action Description (mandatory)
17.4 Next Action (optional)
17.5 Next Action Due Date (optional)

18. **Location** (** mandatory)
Definition: The current (physical or system) location of the record. Details about the location where the record usually resides.

18.1 Current Location (mandatory)
18.2 Home Location Details (mandatory)
18.3 Home Storage Details (mandatory)
18.4 Recordkeeping System (optional)

19. **Disposal** (**mandatory)
Definition: Information about policies and conditions which pertain to or control the authorized disposal of records. Information about the current retention schedule and disposal actions to which the record is subject.

19.1 Retention Schedule (mandatory)
19.2 Retention Period (mandatory)
19.3 Disposal Action (mandatory)
19.4 Disposal Due Date (mandatory)

20. **Mandate** (optional)
Definition: A source of recordkeeping requirements. For example, a piece of legislation, formal directive, policy, standard, guideline, set of procedures, or community expectation which (explicitly or implicitly) imposes a requirement to create, keep, dispose of, or control access to and use of a record.

20.1 Mandate Type (mandatory)
20.2 Refers To (mandatory)
20.3 Mandate Name (mandatory)
20.4 Mandate Reference (optional)
20.5 Requirement (optional)

Consider This:

- ➥ Where records are not individually authenticated, record series metadata may include the name or title of the individual responsible for validating or confirming the data within the record series, and for confirming that the particular series was produced in accordance with standard procedures.

Section 10: Glossary

Note: Definition sources are indicated by letters and listed at the end.

Term **Definition**

Accountability . . . . .

1. The quality of being responsible, answerable; the obligation to report, explain, or justify an event or situation.

Archival Value . . . . .

1. "The values, evidential and/or informational that justify the continuing retention of records as archives." (l)

Archiving . . . . .

1. "The process of creating a backup copy of computer files, especially for long-term storage." (i)

Asymmetric Encryption . . . . .

1. "A form of cryptosystem in which encryption and decryption are performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key. Also known as public-key encryption." (a)

Audit Trail . . . . .

1. "A record showing who has accessed a computer system and what operations he or she has performed during a given period of time." (b)

Authenticity . . . . .

1. Authenticity is a function of a record's preservation and is a measure of a record's reliability over time.

Authentication . . . . .

1. "A process used to verify the integrity of transmitted data, especially a message." (a)
2. "The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization,

Term **Definition**

which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.” (b)

3. “The process of confirming an asserted identity with a specified, or understood, level of confidence. The mechanism can be based on something the user knows, such as a password, something the user possesses, such as a ‘smart card,’ something intrinsic to the person, such as a fingerprint, or a combination of two or more of these.” (h)

Back-up . . . . .

1. “To copy files to a second medium . . . as a precaution in case the first medium fails.” (b)

Backup . . . . .

1. “A substitute or alternative. The term backup usually refers to a disk or tape that contains a copy of data.” (b)

Biometric-based Device . . . . .

1. An authentication technique relying on measurable physical characteristics of the user that can be automatically checked. An example is a fingerprint scanner. (b)

Data . . . . .

1. “Symbols, or representations, of facts or ideas that can be communicated, interpreted, or processed by manual or automated means.” (i)
2. Minnesota “government data” is defined, by statute, to mean “all data collected, created, received, maintained or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media or conditions of use.” (k)

Data Model . . . . .

1. A diagram that shows the various subjects about which information is stored, and the relationships between those subjects.

Term **Definition**

Data Warehouse . . . . .

1. A computer-based information system that is home for "secondhand" data that originated from either another application or from an external system or source. A data warehouse is a read-only, integrated database designed to answer comparative and "what if" questions. Unlike operational databases that are set up to handle transactions and that are kept up to date as of the last transaction, a data warehouse is analytical, subject-oriented, and structured to aggregate transactions as a snapshot in time.

DIG-IT . . . . .

1. Data Issues Group for Information Technology. A Minnesota state government group formed in 1997 as a subcommittee of the Information Policy Council (IPC). Comprised of staff from state agencies and related organizations with an interest in data administration, data modeling, and database administration, DIG-IT's goal is promoting the importance of data as a vital state asset requiring management of its creation, use, storage, dissemination, documentation, and disposition by sharing collective experiences and expertise. Its web site is at < http://www.data.state.mn.us/ >

Digital . . . . .

1. "Describes any system based on discontinuous data or events. Computers are digital machines because at their most basic level they can distinguish between just two values, 0 and 1, or off and on. There is no simple way to represent all the values in between, such as 0.25. All data that a computer processes must be encoded digitally, as a series of zeroes and ones." (b)

Digital Signature . . . . .

1. "An authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature guarantees the source and integrity of the message." (a)
2. "In Minnesota, a digital signature is defined to be an

Term **Definition**

asymmetric cryptosystem. . . . A digital signature is a reliable electronic method of signing electronic documents that provides the recipient with a way to verify the sender, determine that the content of the document has not been altered since it was signed, and prevent the sender from repudiating that fact that he or she signed and sent the electronic document. A digital signature is made up of a key pair consisting of a private key and a public key. . . . A signature looks like a random series of numbers and alphabetical characters. Each signature is unique because it uses the content of the electronic document to create the character string." (c)

Disaster . . . . .

1. "An unexpected occurrence inflicting widespread destruction and distress and having long-term adverse effects on agency operations. Each agency defines what a long-term adverse effect is in relation to its most critical program." (i)

Documentation . . . . .

1. "The act or process of substantiating by recording actions and/or decisions." (i)
2. "Records required to plan, develop, operate, maintain, and use electronic records. Included are systems specifications, file specifications, codebooks, file layouts, user guides, and output specifications." (i)

Dynamic . . . . .

1. "Refers to actions that take place at the moment they are needed rather than in advance." (b)

Electronic . . . . .

1. "Of, or relating to, technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." (e)

Electronic Document . . . . .

1. "An electronic document is any document generated or stored on a computer. An electronic document may be an e-mail message, a contract, a purchase order, a letter or some other type of document. An electronic document can also be an image such as a

Term — **Definition**

blueprint, survey plat, drawing or photograph." (c)

2. "Recorded information that is recorded in a form that requires a computer or other machine to process it. Includes word processing documents; electronic mail messages; . . . Internet and intranet postings; numerical and textual spreadsheets and databases; electronic files; optical images; software; and information systems." (i)

Electronic Record . . . . .

1. "A record created, generated, sent, communicated, received, or stored by electronic means." (e)

Firewall . . . . .

1. "A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria." (b)

Format . . . . .

1. "The shape, size, style, and general makeup of a particular record." (i)

Hard Copy . . . . .

1. "A printout of data stored in a computer. It is considered hard because it exists physically on paper, whereas a soft copy exists only electronically." (b)

Information . . . . .

1. Data, text, images, sounds, codes, computer programs, software, databases, etc. (e)

Information Policy Council (IPC) . . . . .

1. Organized by statute, the IPC is charged with encouraging "cooperation and collaboration among state and local governments in developing intergovernmental communication and information

Term	**Definition**
	systems” in Minnesota (Chapter 202, Article 3, Section 7, Subdivision 3, 1997). Its membership consists of commissioner-level staff and Chief Information Officers of state agencies and constitutional offices. Its web site is at < http://www.state.mn.us/intergov/ipc/ >
Information System	1. “An electronic system for creating, generating, sending, receiving, storing, displaying, or otherwise processing information.” (e) 2. “The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. . . . Most often refers to a system containing electronic records, which involves input or source documents, records on electronic media, and output records, along with related documentation and any indexes.” (i)
Input Device	1. Any apparatus, such as a keyboard, that allows data to be fed or entered into a computer. (b)
Internet	1. A decentralized global network connecting millions of computers.
Intranet	1. “A network . . .belonging to an organization . . . accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.” (b)
Legacy System	1. “An application in which a company or organization has already invested considerable time and money.” (b)
Log-in	1. To enter information before gaining access to a

Term **Definition**

computer system. At the minimum, log-in typically requires a username and password.

Metadata . . . . .

1. Data about data.
2. “The description of the data resources, its characteristics, location, usage, and so on. Metadata is used to identify, describe, and define user data.” (i)

Microform . . . . .

1. “Any form containing greatly reduced images, or microimages, usually on microfilm. Roll, or generally serialized, microforms include microfilm on reels, cartridges, and cassettes. Flat, or generally unitized, microforms include microfiche, microfilm jackets, aperture cards, and microcards, or micro-opaques.” (i)

Migration . . . . .

1. The process of moving computer files from one information system or medium to another.

Official Record . . . . .

1. “In disposal scheduling, the copy of the record held by the office of record. Any other copies of the record can then be destroyed whenever they are no longer required.” (l)

Output Device . . . . .

1. Any machine capable of representing information from a computer, including display screens, printers, plotters, and synthesizers. (b)

Password . . . . .

1. “A character string used to authenticate an identity. Knowledge of the password and its associated user ID is considered proof of authorization to use the capabilities associated with that user ID.” (a)

Permanent Value . . . . .

See **Archival Value**

Private Key . . . . .

1. “The private key is the part of the key pair that is used

Term **Definition**

by the person to sign an electronic document. It must be kept secure as it is the identity of the person in the electronic environment.” (c)

2. “One of the two keys used in an asymmetric encryption system. For secure communication, the private key should be known only to its creator.” (a)

Public Key . . . . .

1. “The public key is the part of the key pair used by the recipient of an electronic document to verify the signature. It is maintained on the certificate issued by the certification authority.” (c)
2. “One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key.” (a)

Record . . . . .

1. “Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” (e)
2. Information created or received during the course of government business that becomes part of an official transaction.
3. “All cards, correspondence, discs, maps, memoranda, microfilms, papers, photographs, recordings, reports, tapes, writings and other data, information or documentary material, regardless of physical form or characteristics, storage media or conditions of use, made or received by an officer or agency of the state and an officer or agency of a county, city, town, school district, municipal subdivision or corporation or other public authority or political entity within the state pursuant to state law or in connection with the transaction of public business by an officer or agency.” Excluding “data and information that does not become part of an official transaction, library and museum material made or acquired and kept solely or reference or exhibit purposes, extra copies of documents kept only for convenience of reference and stock of publications and processed documents, and bonds, and coupons, or other obligations or evidence of indebtedness, the destruction or other disposition

Term **Definition**

of which is governed by other laws." (g)

Reliability . . . . .

1. Reliability is the measure of a record's authority and is determined solely by the circumstances of the record's creation.

Removable Media . . . . .

1. Media, such as tapes, floppy disks, and CD ROMs, that can be physically removed from the computer environment.

Retention Period . . . . .

1. "The period of time, usually based on an estimate of the frequency of current and future use, and taking into account statutory and regulatory provisions, that records need to be retained before their final disposal." (l)

Retention Schedule . . . . .

1. A plan for the management of records including a list of record series, coverage dates, locations, formats, volume, data practices classifications, and retention periods.

Risk Analysis . . . . .

1. A component of risk management that evaluates risks (the possibility of incurring loss or injury), examining the probability of loss or injury occurring, then determining the amount of risk that is acceptable for a given situation or event; a prioritization of risks.

Spoliation . . . . .

1. The destruction of evidence.

Storage Device . . . . .

1. A device capable of storing data such as disk drives and tape drives. (b)

System Development Life Cycle . . . . .

1. "A systematic and orderly approach to solving business problems, and developing and supporting

Term **Definition**

resulting information systems." Typical phases of the system development life cycle include: Planning, Analysis, Design, Implementation, and Support. (d)

Tennessen Warning . . . . .

1. Under the Minnesota Government Data Practices Act, "an individual asked to supply private or confidential data concerning the individual shall be informed of: (a) the purpose and intended use of the requested data within the collecting state agency, political subdivision, or statewide system; (b) whether the individual may refuse or is legally required to supply the requested data; (c) any known consequence arising from supplying or refusing to supply private or confidential data; and (d) the identity of other persons or entities authorized by state or federal law to receive the data. This requirement shall not apply when an individual is asked to supply investigative data, pursuant to section 13.82, subdivision 5, to a law enforcement officer." (j)

Transaction . . . . .

1. "An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs." (f)

Trustworthy . . . . .

1. An information system that produces reliable and authentic records.

URL . . . . .

1. "Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web." (b)

Virus . . . . .

1. "Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function." (a)

World Wide Web (WWW) . . . . .

1. "A system of Internet servers that support specially

Term **Definition**

formatted documents. The documents are formatted in a language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files.” (b)

Worm . . . . .

1. “Program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.” (a)

Sources:

a. William Stallings, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River, NJ: Prentice Hall, 1999.

b. Webopedia. [http://webopedia.internet.com/]. November 1999.

c. Office of the Minnesota Secretary of State. [http://www.sos.state.mn.us/business/digital/digsig.html]. November 1999.

d. Jeffrey L. Whitten, Lonnie D. Bentley, and Victor M. Barlow, *System Analysis and Design Methods*. Burr Ridge, IL: Irwin, 1994.

e. National Conference of Commissioners on State Laws, *Draft: Uniform Electronic Transactions Act*. [http://www.law.upenn.edu/library/ulc/ulc.htm]. March 1999.

f. State of California, *Uniform Electronic Transactions Act*. [http://www.leginfo.ca.gov/pub/bill/sen/sb_0801-0850/sb_820_bill_19990916_chaptered.html]. November 1999.

g. Minnesota Statutes, Chapter 138, Section 138.17, Subdivisions 1 and 4.

h. Fred B. Schneider, ed., *Trust in Cyberspace.* Committee on Information Systems Trustworthiness, National Research Council. Washington, D.C.: National Academy Press, 1999.

i. U.S. Environmental Protection Agency, “Glossary of Common Records Management Terms.” [http://www.epa.gov/ngispgm3/nrmp/gloss/gloss01.htm#a]. November 1999.

j. Minnesota Statutes, Chapter 13, Section 13.04, Subdivision 2.

k. Minnesota Statutes, Chapter 13, Section 13.02, Subdivision 7.

l. Judith Ellis, ed., *Keeping Archives, Second Edition.* Port Melbourne, Victoria, Australia: D. W. Thorpe, in association with The Australian Society of Archivists, Inc., 1997.

Section 11: Bibliography

Minnesota: Guidelines and Reports

Office of the Secretary of State.

Digital Signature Program (including proposed “Minnesota State Agency Digital Signature Implementation and Use Standard”). 1999.
[http://www.sos.state.mn.us/business/digital/gl.html]

Office of the Legislative Auditor.

Summaries of the following reports are offered at: http://www.auditor.leg.state.mn.us/

Department of Public Safety Security Audit: Web-based Motor Vehicle Registration Renewal System. April 2005. Report No. 05-23.
{need for comprehensive security program; formal systems development standards and systems security tests; security standards for wireless technologies; periodic scans for unauthorized wireless access points; documentation of access control standards; access in line with employee duties; no sharing of accounts and passwords; use of complex passwords; procedures for promptly installing security-related patches; need to define security events to log; regular review of security logs; periodic system scans for known security weaknesses}

Minnesota Board of Podiatric Medicine, July 1, 2000 through June 30, 2003. February 2005. Report No. 05-10.
{need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

Minnesota Board of Marriage and Family Therapy, July 1, 2000 through June 30, 2003. February 2005. Report No. 05-08.
{need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

Minnesota Board of Dietetics and Nutrition Practice, July 1, 2000 through June 30, 2003. February 2005. Report No. 05-07.
{need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

Minnesota Board of Dentistry, July 1, 2000 through June 30, 2003. February 2005. Report No. 05-06.
{need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

Minnesota Board of Chiropractic Examiners, July 1, 2000 through June 30, 2003. February 2005. Report No. 05-05.
{need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

Minnesota Board of Veterinary Medicine, July 1, 2000 through June 30, 2003. January 2005. Report No. 05-04.
{need to restrict access to systems; separation of incompatible duties and security clearances; access in line with employee duties}

Minnesota Board of Nursing, July 1, 2000 through June 30, 2003. January 2005. Report No. 05-03.
{need for review of access to systems; need to restrict access to systems}

Department of Human Services, State Operated Services, July 1, 2002 through December 31, 2003. September 2004. Report No. 04-40.
{separation of incompatible duties and security clearances; access in line with employee duties}

Minnesota State Colleges and Universities: Information Technology Security Follow-Up. September 2004. Report No. 04-39.
{need for comprehensive security program}

Financial Audit Division Report: Minnesota State Colleges and Universities. September 2004. Report No. 04-37.
{access in line with employee duties; separation of incompatible duties and security clearances}

Financial Audit Division Report: Departments of Employee Relations, Finance, and Administration, SEMA4 Information Technology Audit. August 2004. Report No. 04-36.
{password management; access in line with employee duties; audit trails for individuals}

Financial Audit Division Report: Minnesota State Court System, Fourth Judicial District, Seventh Judicial District. August 2004. Report No. 04-35.
{separation of incompatible duties and security clearances; access in line with employee duties; restriction of access to private data}

Financial Audit Division Report: Department of Transportation, Fiscal Years2001 through 2003. August 2004. Report No. 04-34.
{separation of incompatible duties and security clearances}

Financial Audit Division Report: Minnesota State Colleges and Universities Data Warehouse Controls Information Technology Audit. July 2004. Report No. 04-29.

{development and documentation of formal data extraction standards and procedures; periodic information technology risk assessments; development of detailed system security baselines; independent assessment of security controls; separation of incompatible duties and security clearances}

Financial Audit Division Report: Minnesota State Colleges and Universities, Degree Audit Reporting and Course Applicability Systems Information Technology Audit. July 2004. Report No. 04-28.
{need for comprehensive security infrastructure; active management of systems; periodic testing and validation of controls; separation of incompatible duties and security clearances; access to data from uncontrolled environments and interfaces; access in line with employee duties; password management; audit trails for individuals}

Financial Audit Division Report: Department of Health, Fiscal Years 2001 through 2003. June 2004. Report No. 04-26.
{separation of incompatible duties and security clearances}

Financial Audit Division Report: Department of Agriculture, Fiscal Years 2001 through 2003. June 2004. Report No. 04-24.
{periodic review of appropriateness of security clearances}

Financial Audit Division Report: Perpich Center for Arts Education, Fiscal Years 2001 through 2003. June 2004. Report No. 04-23.
{need for records retention schedule}

Financial Audit Division Report: State Agricultural Society, Year Ended October 21, 2003. May 2004. Report No. 04-20.
{need for comprehensive security infrastructure addressing current information technology risks}

Information Technology Audit: Department of Revenue, Selected Individual Income Tax Processing Controls. March 2004. Report No. 04-16.
{need for periodic information technology risk assessments; need to develop detailed system security baselines; independent assessment of security controls; need to develop standard access request protocols; timely review of security clearances; password management; audit trails for individuals; access in line with employee duties; control of network access points; review systems for unnecessary and insecure services; prompt installation of security-related patches; ongoing monitoring of systems for security-related events}

Management Letter: Department of Administration, Fiscal Year Ended June 30, 2003. March 2004. Report No. 04-14.
{access controls for computer program libraries}

Management Letter: Department of Human Services, Fiscal Year Ended June 30, 2003. March 2004. Report No. 04-11.
{password and account management; access controls for computer program libraries}

Information Technology Audit: Department of Finance, Information Warehouse Data Integrity Audit. February 2004. Report No. 04-07.
{No major weaknesses were identified.}

Financial-Related Audit: Minnesota State Colleges and Universities, SCUPPS Information Technology Audit. June 2003. Report No. 03-33.
{timely review of security clearances; access in line with employee duties; formal standards and procedures for access; access controls for mission-critical systems; password management; monitoring of security-related events; encryption during file transmission}

Financial-Related Audit: Saint Paul College, July 1, 1999 – June 30, 2002. May 2003. Report No. 03-31.
{timely review of security clearances; access in line with employee duties; unique user accounts}

Financial-Related Audit: Anoka Ramsey Community College, July 1, 2000 – June 30, 2002. June 2003. Report No. 03-28.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Anoka-Hennepin Technical College, July 1, 2000 – June 30, 2002. May 2003. Report No. 03-24.
{timely review of security clearances; access in line with employee duties; unique user accounts}

Management Letter: Department of Finance, Fiscal Year Ended June 30, 2002. March 2003. Report No. 03-17.
{timely review of security clearances; access in line with employee duties; unique user accounts; password control}

Management Letter: Department of Children, Families & Learning, Fiscal Year Ended June 30, 2002. March 2003. Report No. 03-15.
{documentation of system design; cross-training of computer staff}

Financial-Related Audit: Department of Finance, MAPS Interface Controls. November 2002. Report No. 02-68.
{timely review of security clearances; access in line with employee duties; password control and encryption; encryption of data over public networks; data quality checks}

Financial-Related Audit: Department of Natural Resources, July 1, 1999, through June 30, 2002. October 2002. Report No. 02-65.
{timely review of security clearances; access in line with employee duties; procedures; written documentation}

Financial-Related Audit: Public Employees Retirement Association. September 2002. Report No. 02-62.
{lack of comprehensive security program leading to numerous weaknesses}

Financial-Related Audit: Minnesota Veterans Homes Board, July 1, 1997, through June 30, 2002. September 2002. Report No. 02-61.
{access in line with employee duties}

Financial-Related Audit: Minnesota Housing Finance Agency, July 1, 1997, through June 30, 2002. September 2002. Report No. 02-59.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Metropolitan State University, July 1, 1999, through June 30, 2001. September 2002. Report No. 02-58.
{timely review of security clearances; access in line with employee duties; procedures; written documentation}

Financial-Related Audit: Department of Employee Relations, Department of Finance SEMA4 Information Technology Audit. August 2002. Report No. 02-57.
{access in line with employee duties; encryption during file transmission}

Financial-Related Audit: Department of Human Services MAXIS Data Integrity Audit. August 2002. Report No. 02-53.
{access in line with employee duties; access controls to mission-critical programs; information technology risk assessment}

Financial-Related Audit: Hennepin Technical College, July 1, 1998, through June 30, 2001. July 2002. Report No. 02-46.
{access in line with employee duties}

Financial-Related Audit: Minnesota West Community and Technical College, July 1, 1998, through June 30, 2001. June 2002. Report No. 02-43.
{access in line with employee duties}

Financial-Related Audit: Minnesota State Colleges and Universities, Office of the Chancellor, July 1, 1998, through June 30, 2001. June 2002. Report No. 02-42.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Vermillion Community College, July 1, 1998, through June 30, 2001. June 2002. Report No. 02-37.

{timely review of security clearances; access in line with employee duties; procedures; written documentation}

Financial-Related Audit: Mesabi Range Community and Technical College, July 1, 1998, through June 30, 2001. June 2002. Report No. 02-36.
{timely review of security clearances; access in line with employee duties; procedures; written documentation}

Financial-Related Audit: Department of Administration InterTechnologies Group, System-Wide Access to Mainframe Data Follow-up. May 2002. Report No. 02-26.
{timely review of security clearances; access in line with employee duties; written documentation}

Management Letter: State Agricultural Society for the Year Ended October 31, 2001. April 2002. Report No. 02-23.
{lack of comprehensive security program; written documentation}

Management Letter: Department of Children, Families and Learning Fiscal Year Ended June 30, 2001. March 2002. Report No. 02-16.
{lack of training}

Management Letter: Department of Administration, Fiscal Year Ended June 30, 2001. January 2002. Report No. 02-05.
{access in line with employee duties}

Financial-Related Audit: Anoka-Hennepin Technical College, July 1, 1997, through June 30, 2000. October 2001. Report No. 01-50.
{access in line with employee duties; password control}

Financial-Related Audit: Inver Hills Community College, July 1, 1997, through June 30, 2000. October 2001. Report No. 01-49.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Department of Public Safety, Web-Based Motor Vehicle Registration Renewal System as of April 2001. August 2001. Report No. 01-43.
{system-development planning; formal risk assessment; timely review of security clearances; access in line with employee duties; password control; physical environment; security incident detection and response; written documentation of system, standards, policies, and procedures}

Financial-Related Audit: Perpich Center for Arts Education, July 1, 1997, through June 30, 2000. August 2001. Report No. 01-40.
{accuracy of records}

Financial-Related Audit: Rochester Community and Technical College, July 1, 1997, through June 30, 2000. July 2001. Report No. 01-37.
{periodic review of system security; timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Minnesota State College – Southeast Technical, Three Years Ended June 30, 2000. July 2001. Report No. 01-36.
{access in line with employee duties; written documentation}

Financial-Related Audit: Office of the Ombudsman for Mental Health and Mental Retardation, July 1, 1997, through June 30, 2000. June 2001. Report No. 01-32.
{access in line with employee duties; written documentation}

Financial-Related Audit: Riverland Community College, July 1, 1997, through June 30, 2000. June 2001. Report No. 01-30.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Hibbing Community College, Three Fiscal Years Ended June 30, 2000. May 2001. Report No. 01-28.
{access in line with employee duties}

Financial-Related Audit: Board of Barber Examiners, July 1, 1995, through June 30, 2000. May 2001. Report No. 01-21.
{access controls; disaster recovery plans; system backups}

Management Letter: State Agricultural Society For the Year Ended October 31, 2000. April 2001. Report No. 01-19.
{written system documentation}

Financial-Related Audit: North Hennepin Community College, July 1, 1997, through June 30, 2000. March 2001. Report No. 01-16.
{timely review of security clearances; access in line with employee duties}

Financial Audit: Minnesota Council on Disability, July 1, 1997, through June 30, 2000. February 2001. Report No. 01-03.
{access in line with employee duties}

Financial-Related Audit: Minnesota State Colleges and Universities System Access to MnSCU Data. November 2000. Report No. 00-53.
{formal risk assessment; timely review of security clearances; access in line with employee duties; security policies and procedures}

Financial-Related Audit: Ombudsman for Corrections, Three Fiscal Years Ending June 30, 2000. October 2000. Report No. 00-50.
{timely review of security clearances}

Financial-Related Audit: Department of Administration InterTechnologies Group, System-wide Access to Mainframe Data. October 2000. Report No. 00-49.
{timely review of security clearances; access in line with employee duties; written documentation}

Financial-Related Audit: Department of Finance, Information Warehouse Data Integrity as of May 2000. September 2000. Report No. 00-45.
{access in line with employee duties; password controls}

Financial-Related Audit: Minneapolis Community and Technical College, July 1, 1996, through December 31, 1999. September 2000. Report No. 00-44.
{access in line with employee duties; unique users IDs and passwords}

Financial-Related Audit: Alexandria Technical College, July 1, 1996, through December 31, 1999. September 2000. Report No. 00-43.
{access in line with employee duties; records retention policies, documentation, and training}

Financial-Related Audit: Lake Superior College, July 1, 1996, through December 31, 1999. September 2000. Report No. 00-42.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Pine Technical College, July 1, 1996, through December 31, 1999. August 2000. Report No. 00-41.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Departments of Commerce and Public Service, July 1, 1996, through December 31, 1999. August 2000. Report No. 00-40.
{system audit trails}

Financial-Related Audit: Minnesota State University Moorhead, July 1, 1996, through December 31, 1999. August 2000. Report No. 00-37.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Dakota County Technical College, July 1, 1996, through December 31, 1999. August 2000. Report No. 00-36.
{timely review of security clearances; access in line with employee duties}

Financial-Related Audit: Normandale Community College, July 1, 1996, through December 31, 1999. August 2000. Report No. 00-35.
{access in line with employee duties; control of user IDs}

Financial-Related Audit: Public Utilities Commission, July 1, 1997, through December 31, 1999. July 2000. Report No. 00-34.
{timely review of security clearances}

Selected-Scope Financial Audit Report: Department of Corrections, Three Fiscal Years Ended June 30, 1999. July 2000. Report No. 00-32.
{timely review of security clearances}

Audit Report: Metropolitan State University, Period from July 1, 1996, through December 31, 1999. July 2000. Report No. 00-29.
{timely review of security clearances; access in line with employee duties; unique passwords}

Financial Audit: Anoka-Metro Regional Treatment Center, Three Fiscal Years Ended June 30, 1999. June 2000. Report No. 00-27.
{access in line with employee duties}

Financial Audit: Board of Architecture, Engineering, Land Surveying, Landscape Architecture, Geoscience, and Interior Design, July 1, 1996, through December 31, 1999. June 2000. Report No. 00-25.
{access control; written system documentation; user training; backup procedures and storage}

Financial Audit: Fergus Falls Community College, July 1, 1996, through December 31, 1999. June 2000. Report No. 00-24.
{timely review of security clearances}

Financial-Related Audit: Department of Economic Security Mainframe Scheduled Batch Processing and MIPS Accounting System for the Period Ending February 2000. May 2000. Report No. 00-21.
{timely review of security clearances; access in line with employee duties; quality controls; unique user accounts; password management}

Financial Audit: Winona State University, Period from July 1, 1996, through December 31, 1999. May 2000. Report No. 00-18
{timely review of security clearances; access in line with employee duties; unique passwords}

Management Letter: State Agricultural Society for Year Ended October 31, 1999. April 2000. Report No. 00-14.
{written system documentation}

Financial-Related Audit: Board of Electricity for the Period July 1, 1996, through December 31, 1999. April 2000. Report No. 00-13.
{access in line with employee duties}

Department of Economic Security: Statewide Audit—Selected Audit Areas, Fiscal Year Ended June 30, 1998. March 1999. Report No. 99-21.
{security procedures; access controls; written documentation; disaster recovery plan}

Minnesota Department of Employee Relations, Minnesota Department of Finance, SEMA4 Database Security Audit. December 1998. Report No. 98-63.
{formal risk assessment; timely review of security clearances; password control; written documentation of system, policies, and procedures}

South Central Technical College Financial Audit: For the Period July 1, 1995, Through June 30, 1997. October 1998. Report No. 98-59.
{timely review of security clearances; access in line with employee duties; unique users IDs and passwords}

Department of Finance: Information Warehouse Data Integrity Review. June 1998. Report No. 98-36.
{data integrity and security; procedures}

Minnesota Veterans Homes Board: Financial Audit—Two Years Ended June 30, 1997. April 1998. Report No. 98-23.
{timely review of security clearances}

Department of Economic Security: Financial Audit—Fiscal Year Ended June 30, 1997. March 1998. Report No. 98-19
{timely review of security clearances; access in line with employee duties; security administration; security procedures and documentation; disaster recovery plan}

Department of Children, Families and Learning, Selected Programs: Fiscal Year 1997 Statewide Audit. March 1998. Report No. 98-12.
{quality control; security administration; written documentation; user training; disaster recovery plan}

Department of Public Safety, Selected Programs: Fiscal Year 1997 Statewide Audit. February 1998. Report No. 98-10.
{transaction history files; access in line with employee duties; unique user accounts; disaster recovery plan}

Department of Labor and Industry: Financial Audit—Fiscal Year Ended June 30, 1997. February 1998. Report No. 98-5.

{timely review of security clearances; access in line with employee duties}

Minnesota Accounting and Procurement System / Minnesota Statewide Employee Management System. September 1996. Report No. 96-39.
{security administration; security policies; timely review of security clearances; access in line with employee duties; external systems}

Department of Human Services: Programs Selected for Statewide Audit for the Fiscal Year Ended June 30, 1995. June 1996. Report No. 96-22.
{access control; timely review of security clearances; access in line with employee duties; system documentation}

Department of Public Safety, Selected Programs: Fiscal Year 1995 Statewide Audit. April 1996. Report No. 96-15.
{transaction history files; access in line with employee duties; disaster recovery plan}

Department of Labor and Industry: Programs Selected for Fiscal Year 1995 Statewide Audit. February 1996. Report No. 96-8.
{access control; clearance in line with employee duties}

Minnesota Department of Administration, Office of Technology.
The following reports are available at http://www.ot.state.mn.us/standards.

Minnesota Recordkeeping Metadata Standard. IRM Standard 20, Version 1. May 2002.

Minnesota State Agency Digital Signature Implementation and Use Standard. IRM Standard 18, Version 1. November 1999.

Computerized Information Resources Security Standards for State Agencies. IRM Standard 16, Version 1. June 1998.

Management Standards for the Reproduction of Government Records Using Imaging Systems. IRM Standard 13, Version 1. February 1995.

Technical Standards for the Reproduction of Government Records Using Imaging Systems. IRM Standard 12, Version 1. February 1995.

Minnesota Historical Society, State Archives Department. Electronic Records Management Guidelines.
[http://www.mnhs.org/preserve/records/electronicrecords/erguidelines.html]

Minnesota: Laws

Rules of Evidence: Article 9 (Authentication and Identification—Rules 901 and 902). Statutes: Court Rules. 1998.
[http://www.revisor.leg.state.mn.us/]

Chapter 13 (Government Data Practices). Statutes. 1998.
[http://www.revisor.leg.state.mn.us/stats/13/]

Chapter 15.10 (Records Delivered to Department Heads). Statutes. 1998.
[http://www.revisor.leg.state.mn.us/stats/15/10.html]

Chapter 15.17 (Official Records). Statutes. 1998.
[http://www.revisor.leg.state.mn.us/stats/15/17.html]

Chapter 138.163(Preservation and Disposal of Public Records). Statutes. 1998.
[http://www.revisor.leg.state.mn.us/stats/138/163.html]

Chapter 138.17 (Government Records; Administration). Statutes. 1998.
[http://www.revisor.leg.state.mn.us/stats/138/17.html]

Chapter 325K (Minnesota Electronic Authentication Act). Statutes. 1998.
[http://www.revisor.leg.state.mn.us/stats/325K/]

Chapter 325L (Uniform Electronic Transactions Act). Statutes. 2000.
[http://www.revisor.leg.state.mn.us/forms/getstatchap.shtml]

Chapter 8130.7500, Subpart 8 (Department of Revenue, Sales and Use Taxes: Returns and Records – Electronic Data Processing Records). Rules. 1997.
[http://www.revisor.leg.state.mn.us/arule/8130/7500.html]

Chapter 8275 (Secretary of State: Electronic Authentication). Rules. 1998.
[http://www.revisor.leg.state.mn.us/arule/8275/]

Other States: Guidelines, Reports, and Laws

Delaware. Delaware Public Archives. *Model Guidelines for Electronic Records*. 20 January 1998.

New York. New York State Archives and Records Administration. *Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment*. 1994.
[ftp://ftp.sara.nysed.gov/pub/rec-pub/state-rec-pub/admiss.pdf]

Federal Government: Guidelines, Reports, and Laws

U.S. Public Law 106-229. 106th Congress, 2nd Session, 30 June 2000. *Electronic Signatures in Global and National Commerce Act*.
[http://thomas.loc.gov/]

Commodity Futures Trading Commission. *Recordkeeping*. Proposed Rule (17 CFR Part 1) in *Federal Register* (5 June 1998) vol. 63, no. 108, 30668-30675.
[http://www.gpoaccess.gov/nara/index.html]

National Archives and Records Administration. *Electronic Records Management*. *Code of Federal Regulations*, Chapter 12, Title 36, Part 1234.
[http://www.gpoaccess.gov/cfr/index.html]

U.S Department of Commerce. Patent and Trademark Office. *Checklist of Requirements for Electronic Records Management (ERM) Over the Life Cycle of Patent and Trademark Records*. Prepared by Cohasset Associates, Inc., 26 February 1999.

U.S. Department of Commerce. Technology Administration. National Institute of Standards and Technology.

CS2: Protection Profile Guidance for Near-Term COTS, (Draft Version 0.5), and *Rationale for CS2: Protection Profile Guidance for Near-Term COTS*, (Draft Version 0.5), by Gary Stoneburner. 25 March 1999. Re-titled as, and superseded by, *CSPP - Guidance for COTS Security Protection Profiles*, (Version 1.0, NISTIR 6462), January 2000.

An Introduction to Computer Security: The NIST Handbook. NIST Special Publication 800-12. October 1995.
[http://csrc.nist.gov/publications/nistpubs/index.html]

Generally Accepted Principles and Practices for Securing Information Technology Systems, by Marianne Swanson and Barbara Guttman. NIST Special Publication 800-14. September 1996.
[http://csrc.nist.gov/publications/nistpubs/index.html]

U.S. Department of Commerce. Technology Administration. National Institute of Standards and Technology, Federal Computer Security Program Managers' Forum Working Group. *Guide for Developing Security Plans for Information Technology Systems*, by Marianne Swanson. NIST Special Publication 800-18. December 1998.
[http://csrc.nist.gov/publications/nistpubs/index.html]

U.S. Department of Defense.

Design Criteria for Electronic Records Management Software. Prepared by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. DoD 5015.2-STD. November 1997, revised June 2002.
[http://jitc.fhu.disa.mil/recmgt/standards.htm]

Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200.28-STD. December 1985.
[http://www.fas.org/irp/nsa/rainbow/std001.htm]

Password Management Guideline. CSC-STD-002-85. 12 April 1985.
[http://www.fas.org/irp/nsa/rainbow/std002.htm]

U.S. Department of Defense. National Computer Security Center.

A Guide to Understanding Audit in Trusted Systems. NCSC-TG-001. 1 June 1988.
[http://www.fas.org/irp/nsa/rainbow/tg001.htm]

A Guide to Understanding Configuration Management in Trusted Systems. NCSC-TG-006-88. 28 March 1988.
[http://www.fas.org/irp/nsa/rainbow/tg006.htm]

A Guide to Understanding Identification and Authentication in Trusted Systems. NCSC-TG-017. September 1991.
[http://www.fas.org/irp/nsa/rainbow/tg017.htm]

Trusted Network Interpretation of the TCSEC (TNI). NCSC-TG-005. 31 July 1987.
[http://www.fas.org/irp/nsa/rainbow/tg005.htm]

Trusted Product Evaluation Questionnaire. 2 May 1992.
[http://www.fas.org/irp/nsa/rainbow/tg019-2.htm]

Integrity in Automated Information Systems, by Terry Mayfield, J. Eric Roskos, Stephen R. Welke, and John M. Boone. C Technical Report 79-91. September 1991.
[http://www.iwar.org.uk/comsec/resources/standards/rainbow/C-TR-79-91.htm]

U.S. Department of Defense. National Security Agency. National Telecommunications and Automated Information Systems Security Committee. *Advisory Memorandum on Office Automation Security Guidelines*. NTISSAM COMPUSEC 1-87. 1987. [http://www.iwar.org.uk/comsec/resources/standards/rainbow/N-C-1-87.htm]

U.S. Department of Energy. *Records Considerations for Electronic Information: Guidelines for Individuals and Systems Administrators*. Prepared by the Lockheed Martin Energy Systems Electronic Records Committee for the Oak Ridge National Laboratory. February 1996.

U.S. Department of Health and Human Services. *Security and Electronic Signature Standards [as related to Health Insurance Portability and Accountability Act of 1996]*. Proposed Rule (45 CFR Part 142) in *Federal Register* (12 August 1998) vol. 63, no. 155, 43241-43280.
[http://www.gpoaccess.gov/nara/index.html]

U.S. Department of Health and Human Services. Food and Drug Administration. *Electronic Records; Electronic Signatures*. *Code of Federal Regulations*, Chapter 1, Title 21, Part 11. Final Rule in *Federal Register* (20 March 1997) vol. 62, no. 54, 13430-13466.
[http://www.gpoaccess.gov/nara/index.html]

U.S. Department of Justice. *National Criminal Background Check System Regulations*. Proposed Rule (28 CFR Part 25) in *Federal Register* (4 June 1998) vol. 63, no. 107, 30430-30438.
[http://www.gpoaccess.gov/nara/index.html]

U.S. Department of Treasury. Customs Service. *Recordkeeping Requirements*. *Code of Federal Regulations*, Chapter 1, Title 19, Parts 19, 24, 111, 113, 143, 162, 163, 178, and 181. Final Rule in *Federal Register* (16 June 1998) vol. 63, no. 115, 32916-32955.
[http://www.gpoaccess.gov/nara/index.html]

U.S. Department of Treasury. Internal Revenue Service.
Revenue Procedure 98-25. 1998.

“Retention of Books and Records: Section 4—Electronic Storage System Requirements.” *Revenue Procedure 97-22*. 1997.

International Government: Guidelines, Reports, and Laws

Australia. Australian Archives (National Archives of Australia). *Keeping Electronic Records: Policy for Electronic Recordkeeping in the Commonwealth Government*. September 1995. Now part of NAA's expanded online offerings for the Commonwealth Recordkeeping Program.
[http://www.naa.gov.au/recordkeeping/overview/summary.html]

Australia. Defence Signals Directorate.

Australian Communications—Electronic Security Instructions 33 (ACSI 33): Security Guidelines for Australian Government IT Systems. April 1998. Updates issued periodically.
[http://www.dsd.gov.au/library/infosec/acsi33.html]

Australian Communications—Electronic Security Instructions 38 (ACSI 38): Australian Government Standards for the Protection of Electronic Business Systems and Internet Delivery Mechanisms. 9 February 1999.

Great Britain. Public Record Office.

Management, Appraisal and Preservation of Electronic Records—Vol. I: Principles. 1999.
[http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm]

Management, Appraisal and Preservation of Electronic Records—Vol. II: Procedures. 1999.
[http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm]

National Organizations: Guidelines and Reports

American Bar Association, Internal Security Committee, Electronic Commerce and Information Technology Division, Section of Science and Technology. *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*. 1 August 1996.
[http://www.abanet.org/scitech/ec/isc/dsgfree.html]

Association for Information and Image Management.
The following reports are available for purchase at: http://www.aiim.org

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems—Part I: Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence. AIIM Report No. TR31-1992. 1992.

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems—Part II: Performance Guideline for the Acceptance by Government Agencies of Records Produced by Information Technology Systems. ANSI/AIIM Report No. TR31-1993. 1993.

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems—Part III: Implementation of the Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems. ANSI/AIIM Report No. TR31-1994. 1994.

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems—Part IV: Model Act and Rule. ANSI/AIIM Report No. TR31-1994. 1994.

Information Systems Audit and Control Association and Foundation. *COBIT: Control Objectives for Information and Related Technology*. 1998.
[http://www.isaca.org/cobit.htm]

International Federation of Accountants, Information Technology Committee. *International Information Technology Guideline: Managing Security of Information*. January 1998.

National Conference of Commissioners on Uniform State Laws. *Draft: Uniform Electronic Transactions Act*. 19 March 1999.
[http://www.law.upenn.edu/bll/ulc/ulc_frame.htm]

Nuclear Information and Records Management Association.
The following reports are available at: http://www.nirma.org

Authentication of Records and Media (Report No. TG11-1998). 1998.

Electronic Records Protection and Restoration (Report No. TG21-1998). 1998.

Management of Electronic Records (Report No. TG15-1998). 1998.

Software Configuration Management and Quality Assurance (Report No. TG16-1998). 1998.

Electronic Records Projects and Studies

Center for Technology in Government (Albany, New York). *Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation*. 1998.
[http://www.ctg.albany.edu/projects/er/ermn.html]

Duranti, Luciana, Terry Eastwood, and Heather MacNeil. *The Preservation of the Integrity of Electronic Records*. 1997.
[http://www.interpares.org/UBCProject/index.htm]

Indiana University Archives. *Indiana University Electronic Records Project, 1995-1997: Final Report to the National Historical Publications and Records Commission (NHPRC)*. April 1998.
[http://www.indiana.edu/~libarch/ER/]

University of Pittsburgh, School of Information Sciences. *Functional Requirements for Evidence in Recordkeeping*. 1996.

Appendices

The following appendices complement the material found in the main body of the *Handbook*:

Appendix A
Citation of the *Trustworthy Information Systems Handbook*

Appendix B
Background of the Trustworthy Information Systems Project

Appendix C
Trustworthy Information Systems Project Methodology

Appendix D
Minnesota Laws and Policies Relating to Electronic Records

Appendix E
Legal Issues Affecting Electronic Records Management

Appendix F
Project Field Test Results

- *Data Warehouse: Operational (Minnesota Department of Finance)*
- *Web-Enabled Data Repository: Test Phase (Minnesota Department of Children, Families, and Learning)*
- *Web-Enabled Electronic Bidding System: Test Phase (Minnesota Department of Transportation)*
- *Transactional System: Analysis Stage of Development (Minnesota Housing Finance Agency)*
- *Transactional System: Transition to Different Platform (City of Minneapolis)*

Appendix G
Tools for Assisting in the Application of the Trustworthy Information Systems Criteria

Appendix A:
Citation of the *Trustworthy Information Systems Handbook*

Users should be aware of the following information as they refer to the *Trustworthy Information Systems Handbook*:

- Versions are identified by number.

- New versions will be released as substantive changes are made to sections **other than** the bibliography (which changes on a continual basis). The most current version will always be online.

- Past versions will be kept in PDF format by the Minnesota State Archives for five years and will be made available by request. **Users concerned about ongoing access to a particular version (e.g., for audit purposes) should download and maintain within their own agency the PDF of the entire handbook.**

    - Version 1 (December 1999 through July 2000). Note: the HTML and PDF forms of this version carry no identifying number.

    - Version 2 (released in August 2000).
        - Section 2, Section 4, Section 9, and Section 11 revised.

    - Version 3 (released in September 2001).
        - Substantive changes to Section 2, Section 8, Section 9, Section 11, Appendix A, and Appendix D.

    - Version 4 (released in July 2002).
        - Substantive changes to Section 9 (Criteria Group 5), Section 11, and Appendix A.

Users wishing to cite the *Handbook* should use the following format:

> Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.

Appendix B: Background of the Trustworthy Information Systems Project

The Trustworthy Information Systems (TIS) project grew out of a grant to the Minnesota State Archives from the National Historical Publications and Records Commission to establish an electronic records program. The funding was used, in part, to hire an additional staff person, and work got underway in March 1998.

Support was solicited from state government organizations, and partnerships were formed with two key groups: the Information Policy Council (IPC) and the Data Issues Group for Information Technology (DIG-IT). Organized by statute, the IPC is charged with encouraging "cooperation and collaboration among state and local governments in developing intergovernmental communication and information systems" in Minnesota (Chapter 202, Article 3, Section 7, Subdivision 3, 1997). Its membership consists of commissioner-level staff and Chief Information Officers of state agencies and constitutional offices. A subcommittee of the IPC, DIG-IT is open to any state employee with an interest in such topics as database administration, data modeling, and data administration. The group's activities center around promoting the importance of data as a vital state asset and facilitating data sharing, data security, and data access within the state.

The first two phases of the project involved developing the criteria set and testing it for practicality against actual government information systems (refer to Appendix F). State Archives staff promoted the TIS project and sought collaborators by giving talks to government entities and by offering an informational brochure. By October 1999, the State Archives had worked with the following agencies: the Minnesota Housing Finance Agency; the Minnesota Department of Finance; the Minnesota Department of Children, Families and Learning; the Minnesota Department of Transportation; and the City of Minneapolis.

Phases three and four of the project are implementation and education. Implementation centers around web-enabled delivery of TIS products. Early on, a general discussion of trustworthy information systems, the criteria set, and the bibliography were made available on the State Archives' World Wide Web site. With sponsorship from the IPC and in consultation with Signorelli & Associates, Inc., a Saint Paul-based technical writing firm, these items were enhanced and re-worked into the present handbook for wide distribution to government agencies.

Given the rapid rate of technological change and the consequences for both archival preservation and routine government operation, education has been, and will continue to be, a major component of the project. This educational effort will be two-fold. State Archives staff will seek to stay abreast of pertinent topics and methods through such means as taking classes, remaining active participants in groups like DIG-IT, and collaborating with consultants and the academic community. One result will be periodic updates to this handbook to maintain its currency. As well, the staff will help inform others by giving presentations at conferences, speaking to interested organizations, and meeting with representatives from government agencies. Other means of education will include hosting workshops and focus groups on specific topics, issues, and technologies (e.g., data warehousing and metadata), and posting informational pieces on the State Archives web site (e.g., lists of online resources).

Appendix C: Trustworthy Information Systems Project Methodology

Work on the Trustworthy Information Systems project got fully underway in March 1998 and advanced in two stages, culminating in the production of this handbook.

The first phase consisted of researching and compiling the criteria set. A wide range of sources concerned with legal, audit, records management, and archival requirements and standards were surveyed (refer to Section 11, *Bibliography*). Common items of concern in each area came together in the criteria set, which stands within the particular framework of Minnesota's laws and policies.

Once the criteria set was in draft form, attention turned to field testing with respect to actual government information systems (refer to *Appendix F*). Over the course of the testing phase, the set was applied to five different systems. In each case, State Archives staff met with agency personnel knowledgeable about the particular system under scrutiny and led the examination process. One State Archives staff member walked the group, item-by-item, through the criteria while another transcribed the interview information into a chart on a laptop computer. Participants were queried as to whether each criterion was considered important and whether it was currently implemented or planned for future implementation. With each system, the criteria set was supplemented with general questions relevant to that particular function and/or agency. Results were shared with each agency for review and comment as well as for its own internal use.

The findings from the testing phase formed the basis for the formalized process for determining the trustworthiness of information systems presented in this handbook. As the criteria set is applied to more systems, State Archives staff anticipate that the examination process will be refined and that new versions of the handbook will be released as necessary. Additionally, the criteria set will be revised and updated as appropriate to maintain its currency. With the Handbook online, State Archives staff will cease to take such an active role in the examination process, although they will continue to be available for consultation.

Appendix D:
Minnesota Laws and Policies Relating to Electronic Records

To ensure that records are properly created, maintained, and disposed, record keeping responsibilities of state and local government officials are well-defined in Minnesota's Statutes (M.S.) and Rules (M.R.):

- M.S. Chapter 13
- M.S. Chapter 15
- M.S. Chapter 138
- M.R. Chapter 1205
- M.S. Chapter 325L

Official Records Law

Under Minnesota law

> all officers and agencies of the state, counties, cities, towns, school districts, municipal subdivisions or corporations, or other public authorities or political entities with the state, … shall make and preserve all records necessary to a full and accurate knowledge of their official activities (M.S. 15.17).

The chief administrative officer of each government agency has the responsibility to protect records and deliver them to successors to assure smooth transition and continuity (M.S. 15.17). When the functions, powers, and duties of a department or agency are assigned or transferred to another department or agency, all records must be transferred to the successor department or agency (M.S. 15.10).

Records Management Law

The term "government records" is defined in M.S. 138.17, Subdivision 1 as

> state and local records, including all cards, correspondence, discs, maps, memoranda, microfilms, papers, photographs, recordings, reports, tapes, writings and other data, information or documentary material, regardless of physical form or characteristics, storage media or conditions of use, made or received by an officer or agency of the state and an officer or agency of a county, city, town, school district, municipal subdivision or corporation or other public authority or political entity within the state pursuant to state law or in connection with the transaction of public business by an officer or agency.

Although agencies must keep records, this does not mean all records must be retained permanently. In fact, government employees have a mandated responsibility to dispose of data determined to be unnecessary (M.R. 1205.1500 and M.S. 13.07).

M.S. 138.163 addresses the preservation and disposal of public records, governing the disposition of virtually all records of state and local governmental units in Minnesota except those of the Supreme Court and the University of Minnesota.

M.S. 138.17 outlines the procedures that must be followed to dispose of records that no longer have value to an agency. The statute creates the Records Disposition Panel whose members are the Attorney General, the Legislative Auditor (for state agency records), the State Auditor (for local government records), and the Director of the Minnesota Historical Society. The members of the Panel have the authority to determine retention periods for records, to approve their destruction, or to direct that records of long-term legal, fiscal, administrative, or historical value be preserved by the governmental unit or at the State Archives. A records management program is administered by the state commissioner of administration according to M.S. 138.17, Subdivision 7. The Minnesota State Archives was created pursuant to M.S. 138.161.

Occasionally, special statutes state how long certain records must be retained. However, M.S. 138.17 takes precedence over any such law unless records are specifically exempted from M.S. 138.17. That is, unless a statute says that a record is exempt from M.S. 138.17, the retention period listed serves only as a guideline. The Records Disposition Panel has the sole authority to approve a records retention period.

Minnesota Government Data Practices Act

All Minnesota government employees should be acquainted with the major provisions of the Minnesota Government Data Practices Act (M.S. 13). The only governmental units exempt from the requirements of the statute are townships.

The Act balances the often conflicting interests of government efficiency, individuals' right to privacy, openness in government, and freedom of information for the public and the media. Except in special instances, the Act does not govern data handling in the private sector.

The Act establishes a "data classification system." Eight categories classify and label government data in terms of who is authorized to gain access (M.S. 13.02). Unless specifically noted otherwise, all government data is accessible to the public for any reason (M.S. 13.03).

As defined by the Act, the responsible authority is an individual in each governmental agency who is required to perform the duties necessary to implement and administer the Act. M.S. 13.05 details most of these responsibilities.

M.S. 13.04 guarantees certain rights to individuals on whom the government maintains data. M.S. 13.04, Subdivision 2 discusses the requirements of what is known as the "Tennessen Warning," a notification statement supplied to individuals when private or confidential information is being asked of them. M.S. 13.08 offers protection in the form of civil remedies to individuals who feel that a government agency is violating or not properly administering the provisions of the Act.

M.S. 13.03, Subdivision 3 explains the procedure that government agencies must follow when receiving a request for records from the public. The responsible authority of the agency must provide copies of public data to a requester in a timely manner. Costs for this service may not exceed the actual costs of searching for and retrieving the records and may not include charges for separating public from not-public data. If the request is denied, a citation to the specific statutory section, temporary classification, or federal law must be given. Upon receipt of such denial, the requester may file court action to compel the release of the data.

Access and Security Laws and Policies

Under the Minnesota Government Data Practices Act (M.S. 13) and the Department of Administration's rules (M.R. 1205), all data collected, created, received, maintained, or disseminated by any government agency (e.g., state agency, political subdivision, or statewide system) must be made accessible to the public unless the data is classified as inaccessible by state statute, federal statute or temporary classification. Agencies must establish written procedures to assure properly controlled access to private and confidential data (M.R. 1205.0400, Subpart 3 and M.R. 12.0600, Subpart 3).

M.S. 13.05, Subdivision 5 addresses the protection of data, stipulating that the responsible authority shall

> (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; and (2) establish appropriate security safeguards for all records containing data on individuals.

Moving beyond the simple establishment of procedures, agencies must prepare and distribute directives requiring compliance and provide related training to staff (M.R. 1205.1300, Subpart 5).

Uniform Electronic Transactions Act

Enacted in 2000, the Minnesota Uniform Electronic Transactions Act (UETA) (M.S. 325L) facilitates electronic commerce and electronic government services by legally placing electronic records and signatures on equal footing with their paper counterparts. The law does not require the use of electronic records and signatures but, rather, allows for them where agreed upon by all involved parties. While technology neutral, the law stipulates that all such records and signatures must remain trustworthy and accessible for as long as required. Along a similar vein, the federal Electronic Signatures in Global and National Commerce (E-Sign) Act (U.S. Public Law 106-229) also encourages the use of electronic documents and signatures, although it goes further to provide some guidelines regarding standards and formats.

Other Relevant Statutes and Rules

Article 9 of Rules of Evidence (Authentication and Verification), Minnesota Statutes: Court Rules, 1998.

M.S. 325K (Secretary of State Administrative Rule: Electronic Authentication).

Chapter 8130.7500, Subpart 8 (Department of Revenue, Sales and Use Taxes: Returns and Records—Electronic Data Processing Records). Rules. 1997.

Appendix E:
Legal Issues Affecting Electronic Records Management

DISCLAIMER:
This is a summary tool. It is not intended to be a substitute for individualized legal advice. Consult an attorney for assistance with specific concerns or for advice.

There are a number of legal issues that affect electronic records management. This memorandum summarizes a few such issues, including: destruction of records/spoliation, discovery of electronic records, electronic records as evidence, privacy of e-mail, liability for records/information contained on a web site, personal jurisdiction via electronic records, and the Uniform Electronic Transactions Act.

I. Destruction of Records/Spoliation

A. Destruction in General

In Armstrong v. Executive Office of the President, 1 F.3d 1274 (DC Cir 1993), a group of researchers and nonprofit organizations sought to prevent the deletion of e-mail records created during the Reagan administration, arguing that e-mail records should receive the same protection as paper-based records under the Federal Records Act (FRA). The DC Circuit agreed, holding that substantive e-mail communications are included in the FRA definition of "records" and so e-mail records, including transmittal information, should be stored. Often electronic records contain more information than their hard copy counterparts (such as multiple drafts in word processing). Machine-readable data contains original information that never existed in paper documents.

In Public Citizen v. Carlin, the Federal Court of Appeals overturned a lower court's holding that the federal government's General Record Schedule 20 (GRS 20) was invalid. GRS 20 governed the federal agencies' destruction and storage of certain electronic records. Specifically, the challenged portion of GRS 20 was the provision that authorized the disposal of word processing and electronic mail files that were copied to an agency record keeping system from a personal computer.

The lower court had held that GRS 20 exceeded the statutory authority because (1) it did not analyze the content of the records (it includes "program" records as well as "housekeeping" or administrative records); and (2) it did not set a specific time period for the retention of records before destruction (which is required by the statute). It also stated that hard-copy records are not satisfactory replacements for electronic records and may impair the research value of the records, since hard copies cannot be searched, manipulated, and indexed in the same way as electronic records, and are not as complete as electronic records (such as information about revisions).

The Court of Appeals held that the statute required a record to be scheduled according to the physical attributes of the record rather than its content. In addition, GRS 20 only authorizes disposal of records after they are copied into an agency record keeping system. There is no risk that the information will be lost to future users, since a record must first be copied before it can be destroyed under GRS 20. GRS 20 does not authorize the disposal of electronic records per se. The National Archivist still has to assess the "administrative, legal, research, or other value" of a record before authorizing its disposal. The Court also held that GRS 20 did state a time for disposal of records, which was after they have been transferred to a record keeping system. The Court of Appeals agreed with the lower court that electronic record keeping has advantages over paper record keeping, but acknowledges that not all agencies have established an electronic record keeping system and that the Archivist does not have to require every such agency to create an electronic record keeping system. Finally, the paper copies of electronic records will be complete, because GRS 20 required retention of hidden information or comments.

A defendant organization may seek to have a lawsuit dismissed for prejudice, if the plaintiff delayed in filing the lawsuit, and if before such filing the organization destroyed relevant records pursuant to its reasonable record retention policy. Minnesota courts are hesitant to impose sanctions for the destruction of documents prior to the initiation of litigation. Capellupo v. FMC Corp., 126 FRD 545 (D MN 1989). Courts in other states do not hesitate to impose such sanctions, however. For example, in Peskin v. Liberty Mutual Insurance Company (530 A.2d 822 (1987)), Peskin filed a claim for insurance coverage 9 ½ years after a fire. Liberty Mutual no longer possessed all the records necessary to establish the parameters of coverage. The records were destroyed by Liberty Mutual pursuant to its records destruction schedule before it received notice of the fire. The court remanded the case to determine whether Liberty Mutual's record retention policies comported with industry standards of practice and were otherwise reasonable.

The duty to preserve evidence starts when the litigant knows, or reasonably should know, that information is relevant in an action or reasonably calculated to lead to discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is subject of pending discovery request. (See Souza v. Fred Carries Contracts, Inc., 955 P2d 3 (AZ App Div 2 1997) and Fayemi v. Hambrecht and Quist, Inc., 174 FRD 319 (SDNY 1997)). For example, according to Hunter v. Ark Restaurants Corp., 3 F. Supp 2d 9 (DDC 1998), a court can dismiss a case for destruction of evidence when the litigant is on notice that documents are relevant to potential litigation and destroys such documents, depriving the party of the opportunity to present critical evidence on key claims. The obligation to preserve evidence even arises prior to the filing of a complaint where a party is on notice that litigation is likely to be commenced. Capellupo v. FMC Corp., 126 FRD at 550; Alliance to End Repression v. Rochford, 75 FRD 438 (ND IL 1976). If, however, there is no hint of litigation nor any other reason to retain certain documents, then a litigant's destruction of such documents does not warrant sanction or dismissal of the claim.

Each state has its own rules regarding destruction of evidence. For example, New York has a high standard for spoliation of evidence. Under its "Spoliator Beware" standard, the negligent, non-willful destruction of crucial and dispositive evidence in the sole possession of a party could bring severe sanctions of dismissal or summary judgment against the destroying party (even if the evidence was destroyed before a lawsuit was commenced). When a party alters, loses, or destroys key evidence before it can be examined by the other party's expert, the court has discretion as to sanctions. See Conderman v. Rochester Gas & Electric Corp., 687 NYS2d 213 (Supp 1998). In Conderman, there was an accident caused by certain telephone poles falling on a car. The defendant's risk management department sent an experienced team of claims personnel to the accident site, and they did not mark, identify, preserve or test the poles. The poles were thereafter destroyed, and the plaintiff claimed spoliation of evidence. The court held that New York has a strong public policy regarding the maintenance of key evidence in connection with a lawsuit. In this case, the immediate dispatch of experienced claims personnel showed that the defendant had a high degree of awareness of the likelihood of possible litigation, and supports a finding that crucial evidence was negligently destroyed.

A majority of states do not recognize a separate tort of spoliation of evidence, but limit the remedies for spoliation to the case at hand (such as Arizona in Souza v. Fred Carries Contracts, Inc., 955 P2d 3 (AZ App Div 2, 1997); and Texas in Trevino v. Ortega, 969 SW2d 950 (TX 1998). Courts in these states hold that spoliation does not give rise to independent damages, and is better remedied within the lawsuit affected by the spoliation. Spoliation is an evidentiary concept, not a separate cause of action; the destruction only becomes relevant when someone believes that those destroyed items are instrumental to success in a lawsuit. A minority of states, however, do recognize a separate tort of spoliation of evidence (California, Florida, New Jersey, New Mexico and Ohio).

B. Destruction After Commencement of Lawsuit

Once an organization knows, or has reason to know, of the relevance of documents or information, it has an affirmative duty to preserve such information. If an organization destroys or fails to retain documents or information which it knows, or has reason to know, will be relevant in a lawsuit, it may face sanctions (at the discretion of the Court) for spoliation of evidence ranging from fines and penalties to entry of a judgment against it. See Shepherd v. American Broadcasting Companies, 151 FRD 179 (DDC 1992).

In determining whether a court should exercise its authority to impose sanctions for spoliation, a threshold question is whether a party had any obligation to preserve the evidence. Sanctions may be imposed on a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and who destroys such documents and information. While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably likely to be requested during discovery, and/or is the subject of a pending request. Wm. T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443 (CD Cal 1984). Thus, no duty to preserve arises unless the party possessing the evidence has notice of its relevance. Danna v. New York Telephone Co., 752 F. Supp. 594 (SDNY 1990). Of course, a party is on notice once it has received a discovery request. Beyond that, the complaint itself may alert a party that certain information is relevant and likely to be sought in discovery. Computer Associates International, Inc. v. American Fundware, Inc. 133 FRD 166 (D CO 1990); Teletron Inc. v. Overhead Door Corp., 116 FRD 107 (SD FA 1987).

For example, in Applied Telematics, Inc. v. Sprint Communications (1996 US Dist Lexis 14053), Sprint failed to preserve backup tapes of a computer system that routes telephone calls after receiving a request for information in connection with a patent infringement lawsuit commenced by Applied Telematics. Applied Telematics argued that Sprint knew that such information was relevant when it received the request for information. Sprint responded that, pursuant to its normal operating procedures, the computer system is backed up and saved, replacing the prior week's backup. As a result, after one week the historical information is unavailable from the computer system.

The court found that Sprint did know, or should have known, that the backup files were relevant, and failed to take steps to prevent the routine deletion of the backup files. The fact that Applied Telematics failed to ask Sprint to save the files does not relieve Sprint of its affirmative duty to do so. The court went on to find that Sprint did not destroy the backup files fraudulently or with the intent to prevent Applied Telematics from obtaining the evidence, and Applied Telematics did not suffer substantial prejudice from Sprint's actions. As a result, the court awarded Applied Telematics monetary sanctions for the destruction of evidence. The prejudice was not substantial, in part because Applied Telematics failed to pursue other means to obtain the information. The court held that it has discretion to choose an appropriate sanction upon finding improper loss or destruction of evidence, based on the willfulness of the destructive act and the prejudice suffered by the requesting party. If the spoliation or destruction of evidence was intentional and indicates fraud and a desire to suppress the truth, rather than destruction that is a matter of routine with no fraudulent intent, a sanction that has a drastic result, such as entry of judgment, may be appropriate. See also Shepherd v. American Broadcasting Companies, 151 FRD 179 (DDC 1992).

Similarly, in Turner v. Hudson Transit Lines, Inc., 142 FRD 68 (SDNY 1991), the court imposed sanctions on the defendant because it destroyed maintenance records of a bus and as a result was unable to produce them in a lawsuit regarding an injury that took place on the bus. The defendant maintained records for one year, as required by the Federal Highway Administration regulations, then destroyed the maintenance records pursuant to its documentation retention policies. The lawsuit was filed in October 1986, and the document request for maintenance records of the bus was made December 29, 1989. The defendant destroyed the documents in December 1989 and therefore could not produce them. The court held that, at least by the time the complaint was served, the defendant was on notice that maintenance records should be preserved. Even though it did not intentionally destroy evidence, its reckless conduct did result in loss of the records. The corporate managers were responsible for conveying this information to relevant employees. The defendant's management did not advise its employees of the obligation to maintain relevant documents while litigation was pending. It had an obligation to preserve the maintenance records and it failed to do so.

It is no defense for an organization to suggest that particular employees were not on notice. To hold otherwise would permit an organization to shield itself from discovery obligations by keeping its employees ignorant. See also National Association of Radiation Survivors, 115 FRD at 557; Medical Billing, Inc v. Medical Management Sciences, Inc. v. Reich, 1996 WL 219657 (ND OH 1996).

Even though a party may have destroyed evidence prior to issuance of the discovery order and thus be unable to obey, sanctions may still be appropriate if the inability to produce the records was self-inflicted. See In re Air Crash Disaster near Chicago, Illinois on May 25, 1979, 90 FRD 613 (ND IL 1981). For example, in Computer Association v. International v. Americal Fundware, Inc., 133 FRD (D CO 1990), the defendants destroyed a version of source code at issue after a copyright infringement lawsuit was filed. The defendant was sanctioned by the court because it had an obligation to preserve the code because of its knowledge of plaintiff's claims. See also National Association of Radiation Survivors v. Turnage, 115 FRD 543 (ND CA 1987); ABC Home Health Services, Inc. v. International Business Machines Corp, 158 FRD 180 (SD GA 1994); General Environmental Science Corp. v. Horsfall, 141 FRD 443 (ND OH 1992); Hirsch v. General Motors Corp., 628 A2d 1108 (NJ Super 1993); Lexis-Nexis v. Beer, 41 F Supp2d 950 (D MN 1999); Pepsi Cola Bottling Co. of Olean v. Cargill Inc., Archer-Daniels Midland Co., 1995 WL 783610 (D MN 1995).

C. Adverse Inference

If a party destroys evidence, a court may accept an inference that the evidence would be unfavorable to the position of the offending party. The concept of an adverse inference as a sanction for spoliation is based on two rationales: (1)

remedial—where evidence is destroyed, the court should restore the prejudiced party to the same position with respect to its ability to prove its case that the court would have held if there had been no spoliation; or (2) punitive—to deter parties from destroying relevant evidence before it can be introduced at trial. If a party destroyed evidence, it may accept an inference that the evidence would be unfavorable to the position of such party. The rationale is based on the observation that a party who has notice that evidence is relevant to litigation and who proceeds to destroy it is more likely to have been threatened by that evidence than is a party in the same position who does not destroy the evidence. See Schmid v. Milwaukee Electric Tool Corp., 13 F3d 76 (3rd Cir 1994).

When an adverse inference is made, the party may have sanctions imposed, and/or the evidence can be admitted against it. The key considerations in determining whether such a sanction is appropriate are: (1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future. See Kronisch v. U.S., 150 F3d 112 (2nd Cir 1998); Dillon v, Nissan Motor Co., Ltd., 986 F.2d 263 (8th Cir 1993); SDI Operating Partnership LB v. Neuwirth, 973 F.2d 652 (8th Cir 1992).

The state of mind of a party that destroys evidence is a major factor in determining whether an adverse inference is an appropriate sanction. If the party acted in bad faith or intended to prevent the use of the evidence in litigation, then an adverse inference is required; if the party acted willfully, it may be appropriate to draw an adverse inference. See Alexander v. National Farmers Organization, 687 F 2d 1173 (8th Cir 1982). Before an adverse inference is made, the party seeking the destroyed evidence must show that the destroyed evidence would have been otherwise unattainable by the party seeking such destroyed evidence. In order to remedy the evidentiary imbalance created by the destruction of evidence, an adverse inference may be appropriate even in the absence of a showing that the spoliator acted in bad faith. However, where the destruction was negligent rather than willful, special caution must be exercised to ensure that the adverse inference is commensurate with information that was reasonably likely to have been contained in the destroyed evidence.

For example, in Brewer v. Quaker State Oil Refining Corp., 72 F3d 326 (3rd Cir 1995), the court stated that if the contents of a document are relevant to the issue in a case, the trier of fact generally may receive the fact that the document cannot be produced as evidence that the party who has prevented production did so out of well-founded fear that the contents would harm him or her if discovered. On the other hand, no unfavorable inference arises when circumstances indicate that the document or article in question has been lost or accidentally destroyed, or where failure to produce the document is otherwise accounted for. For example, when a company cannot produce an employee's personnel file because the employer's inhouse attorney died of a terminal illness after taking possession of the file and the employer cannot find the file after continually looking for it.

D. Inefficient Record Keeping System: Unable to Locate Records

An organization may face liability if it creates a record keeping and indexing system that makes it difficult or costly to locate and produce documents on request. For example, in Kozlowski v. Sears (73 FRD 73, 1976), the plaintiff was burned when pajamas manufactured and marketed by the defendant ignited. The plaintiff asked for a record of all complaints and communications concerning personal injuries or death allegedly caused by the burning of children's nightwear manufactured or marketed by the defendant. The defendant refused to produce such documents, stating that there is no practical way for anyone to determine whether there are any such records, because it has a longstanding practice of indexing claims alphabetically by name of applicant, rather than by type of product. The court stated that the defendant may not excuse itself from compliance with the discovery request because it "utilizes a system of record keeping which conceals rather than discloses relevant records or makes it unduly difficult to identify or locate them, thus rendering the production of the documents an excessively burdensome and costly expedition. To allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purpose of the discovery rules." See also Continental Illinois National Bank & Trust Company of Chicago v. Caton, 136 FRD 682 (D KS 1991);Baine v. General Motors Corp., 141 FRD 328 (MD AL 1991); Fagan v. District of Columbia, 136 FRD 5 (DDC 1991); Control Data Corporation Securities Litigation, 1988 WL 92085, Fed Sec L Rep 93,720 (D MN 1988); Bowman v. Consolidated Rail Corp., 110 FRD 525 (ND Ind 1986); US v. ACB Sales & Service, Inc. 95 FRD 316 (1982); Dunn v. Midwestern Indemnity, 99 FRD 191 (SD OH 1980); Webb v. Westinghouse Electric Corp., 81 FRD 431 (ED PA 1978).

E. Requirement to Follow Internal Document Retention Policies

If a corporation has a documentation retention policy or other corporate policy that applies, it creates a standard that it is required to follow. For example, in Gillispie v. Rank Video Services America, (1997 US Dist LEXIS 13183), the court found that the defendant violated its own policy by not promoting the plaintiff, and this violation may constitute evidence of discrimination.

II. Discovery of Electronic Records

Today it is well established that computerized data and electronic records (as well as documentation of the computer system itself) are discoverable if relevant during discovery (the information-gathering process of a lawsuit). See FRCP 34(a); Adams v.

Dan River Mills Inc., 54 FRD 220 (WD VA 1972). Courts have stated that information which is stored, used, or transmitted in new forms should be available through discovery with the same openness as traditional forms. It would be dangerous if new techniques for using information became a hindrance to discovery in litigation. Specifically, a defendant's deleted files on its computer hard drive may be discoverable if they are still recoverable. See Gates Rubber Co. v. Bando Chemical Indus. Ltd., 167 FRD 90 (D CO 1996); Strausser v. Yalamachi, 699 So2d 1142 (FA App 1996) Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 USLEXIS 6355 (SDNY 1995); Seattle Audobon Society v. Lyons, 871 F. Supp. 1291 (WD WA 1994); Easley, McCaleb & Associates, Inc. v. Perry, No. E-2663 (Ga. Super. Cit. July 13, 1994); PHE, Inc. v. Department of Justice, No. 96-2840(PLF) (DDC 1991); Pearl Brewing Co. v. Joseph Schlitz Brewing Co., 415 F. Supp 1122 (SD Tex 1976); Greyhound Computer Corp., Inc. v. IBM, (3 Computer L Serv Rep 138 D. MN 1971). When computerized data is produced, it must be in a form reasonably useable by the other party. If a party suspects that the other party is not producing all relevant information or has destroyed records, the party may request access to the other party's computer system, or visit the other party's site.

The proliferation of e-mail has changed discovery greatly. The Federal Rules of Civil Procedure do not explicitly allow for discovery of e-mail, but state more generally that electronically stored data is discoverable. Many courts have upheld e-mail discovery requests, making e-mail messages a fodder for legal action. Most e-mail systems can create a complex record of communication, capturing the exact text that users send and receive, as well as storing information regarding their transmission and receipt. Destroying e-mail is difficult; even if a user deletes a message from his or her machine, most e-mail systems store messages on a centralized backup file for an indefinite period of time. It is relatively easy to retrieve deleted e-mails from most computer databases and these deleted e-mails are generally discoverable. See In re Brand Name Prescription Drug Antitrust Litigation (94-C-87, MDL 997 (ND IL 1995)).

Note, however, that the attorney-client privilege can extend to computer files. If legal counsel's advice or opinion was conveyed through electronic mail, then that message is privileged, except to the extent it contains information meant to be distributed to persons other than the corporate client. See IBM v. Comdisco, Inc. (91-C-67-1992 Del Super LEXIS 67 March 11, 1992). As a result, e-mail communications received from legal counsel should not be forwarded to any party within the organization, unless such party has a need to know such information. In addition, security measures should be in place to ensure that other employees at an organization do not have access to each other’s e-mail, including any e-mail communication from the organization’s legal counsel.

III. Electronic Records as Evidence

Computer-generated records cannot be admitted into evidence unless the proper foundation has been laid. For example, in Illinois v. Bovio (455 NE2d 829, 1983), the court ordered a new trial because the state prosecutor did not lay the proper foundation for admitting computer-generated bank records into evidence, which supported a necessary element of the charge of theft by deception. In Illinois, it must be shown that the computer equipment is standard, that the entries are made in the regular course of business at or reasonably near the time of the happening of the event recorded, and that the sources of information and the method and time of preparation are such as to indicate trustworthiness and justify admission. There was no testimony to show how transaction information was entered into, and processed through, the computer system which would verify the accuracy of the output. Systems which perform calculations must be scrutinized more thoroughly than systems which merely retrieve information. The state needed to show that the computer program was standard, unmodified, and operated according to its instructions.

Other states have more liberal rules regarding the admissibility of electronic records into evidence. For example, the California Uniform Electronic Evidence Act (Act) defines "electronic record" and "electronic records system" and provides a series of rules and presumptions relating to the admissibility of electronic records. The key to the Act is the presumption of integrity given to electronic records when it is established that (a) at all material times the computer system was operating properly or the fact that it was not operating properly did not affect the integrity of the electronic records; and that (b) there are no reasonable grounds to doubt the integrity of the electronic records system.

One way in which to admit electronic records into evidence in federal court is by defining them as “business records” under the Federal Rules of Civil Procedure, therefore excepting them from hearsay. The business records exception relies on trustworthiness and necessity. It consists of five elements: (1) the records must be kept in the ordinary course of business; (2) the particular record at issue must be one that is regularly kept; (3) the record must be made by, or from, information transmitted by a person with knowledge of the source; (4) the record must be made contemporaneously; and (5) the record must be accompanied by foundation testimony by a custodian of the record. All such elements must be met to be admissible. Critical to admissibility of computer records is the foundation testimony regarding the above requirements, including the reason that the message was prepared and sent. See U.S. v. Catabran, 836 F.2d 453 (9th Cir 1988); Rosenberg v. Collins. See also Quality Auto Service v. Fiesta Lincoln-Mercury Dodge Inc., No. 04-96-00967-CV 1997 WL 563176 (TX App Sept 10, 1997); U.S. v. Kim, 595 F2d 755 (DC Cir 1979).

Electronic records and computer printouts of accounting and other bookkeeping records that are entered into the computer on a monthly basis are generally admissible in court as business records. See Midfirst Bank SSB v. CW Haynes & Co., 893 F. Supp 1304 (DSC 1994); U.S. v. Goodchild, 25 F3d 55 (1st Cir 1994). Electronic records reveal more information than their paper counterparts, since they more easily show inconsistencies among documents, contain multiple drafts of documents, contain the history of a document (including who revised the document, in what manner, and when), may contain unprinted annotations, and show the names of documents and other filenames. Electronic data thought to be lost or erased is usually accessible. In addition, there are usually multiple drafts of documents and many different places within a network or computer they may be stored. Data is routinely backed up over and over, and exists in many different places and formats. Users are adverse to destroying data, people use a lower standard of care when writing e-mail, and computers routinely save many copies of documents in various ways. This makes it very expensive, time consuming, and burdensome to find and produce electronic records. In addition, if you do not produce the records, your adversary may gain access to your computer system.

The admissibility of e-mail is not so clear, however. Although e-mail is obtainable through discovery, there is no guarantee that it will be admissible in federal court. Courts are concerned about whether e-mail satisfies the "regular practice" of the exception, and the casual nature of the messages raises trustworthiness questions. See Aviles v. McKenzie; Strauss v. Microsoft Corp.; Allen v. State; U.S. v. Kim 595 F2d 755 (DC Cir 1979); Plymouth Police Brotherhood v. Labor Relations Commission; Monotype Corporation PLC v. International Typeface Corporation, 43 F.3d 443 (1994).

As of 1996, no federal court had applied the business records exception to e-mail messages. Since then, some courts have held it is admissible, while others have held that it does not meet the requirements of the business records exception in the Federal Rules of Evidence (Rule 803(6)). For example, in Monotype Corporation PLC v. International Typeface Corporation, 43 F.3d 443 (1994), the court excluded an e-mail transmission as evidence to support the defendant's defense. The defendant moved to admit an e-mail transmission under the business records exception to support its defense that it did not copy Monotype's typefaces. The court held that e-mail is far less of a systematic business activity than a monthly inventory printout or other computer-generated printout. E-mail is an on-going electronic message and retrieval system, whereas an electronic inventory recording system is a regular, systematic function of a bookkeeper prepared in the course of business. See also Michaels v. Michaels; Monotype Corporation PLC v. International Typeface Corporation, 43 F.3d 443 (1994); U.S. v. Catabran, 836 F.2d 453 (9th Cir 1988); U.S. v. Kim 595 F2d 755 (DC Cir 1979).

A survey of recent federal cases, however, shows that e-mail has found its way into the courtroom. For example, in Knox v. State of Indiana, 93 F3d 1327 (7th Cir 1996) e-mail messages in which a supervisor repeatedly asked an employee for sex were admissible in a harassment case. See also Harley v. McCoach, 928 F. Supp. 533 (ED PA 1996); Wesley College v. Pitts, 874 F.Supp 375 (D DE 1997).

IV. Privacy of E-Mail

An employee has no reasonable expectation of privacy in e-mail communications voluntarily made over the company e-mail system to another company employee, notwithstanding assurances that such communications would not be intercepted by management. For example, in Smythe v. The Pillsbury Company (914 FSupp 97, 1996), the court held that Smythe could be fired for communications made to his supervisor which were forwarded to Pillsbury management. The court found that such a firing does not violate Pennsylvania public policy, and that monitoring and interception of the contents of e-mail communications made over the company e-mail system by an employer does not invade an employee's privacy interests.

See also Bourke v. Nissan Motor Corp., No. B068705 (CA Ct App, July 26, 1993), which stated that employees had no reasonable expectation of privacy in their work place e-mail when (a) they were aware for some time prior to being terminated that their e-mail was read by the company; and (b) they signed a statement agreeing to restrict their use of company-owned hardware and software to company business.

V. Liability for Records/Information Contained on Web Site

A. Copyright

Web sites have been held liable for intellectual property infringement and other harms caused by their users. A single bad user could cause liability ranging into the millions of dollars. The potential legal risks inherent in owning and maintaining a web site are copyright infringement (direct, contributory, or vicarious) and defamation. Web sites planning to permit users to exchange content should implement a number of techniques to manage their potential risk. In addition, a president, officer, and shareholder in a defendant corporation may be personally liable for the activities of the company, since he or she is active in the day to day operations of the company. See Religious Technology Center v. Netcom On-Line Comm, 907 F. Supp 1361 (ND Cal 1995).

For example, in Comedy III Productions, Inc. et al v. Class Publications, Inc. et al (1996 US Dist LEXIS 5710 April 30, 1996), the defendant violated plaintiff's trademarks in the Three Stooges by selling unauthorized products on its Internet web site. In addition, Playboy Enterprises has initiated a number of lawsuits against web sites that post its copyrighted pictures, or that allow a subscriber to the web site to upload such pictures to the web site. For example, in Playboy Enterprises, Inc. v. George Frena, 839 F Supp 1552 (1993), the defendant operated a subscription computer bulletin board service, which distributed unauthorized copies of plaintiff's photographs. On the web site, subscribers could log-on and browse and download pictures and store them on their personal computers. In addition, subscribers could upload material to the web site so that all other subscribers could view the material. The defendant admitted that the pictures were displayed on his web site, but claimed that he did not place them there; they were uploaded by a subscriber. The defendant did not know about the pictures until he was served complaint papers, at which time he removed the photographs and began monitoring the web site to prevent additional photographs from being uploaded. The court held that the defendant is responsible for material that is on his web site and infringes on another’s copyright, even if the defendant did not place the material on the web site and did not have knowledge that such material so infringed. See also Playboy Enterprises, Inc. v. Webbworld, Inc., 991 F Supp 543 (ND Tex 1997); Christopher Scanlon v. Gil Kessler et al, No

97 Civ 1140, 1998 US Dist Lexis 10201 (SDNY July 10, 1998). Further, an operator of a computer bulletin board service may become liable for copyright infringement if it takes affirmative steps to cause copies to be made. For example, if a bulletin board service encourages people to upload documents, and it screens all documents and moves them to the appropriate generally available files, it may be held liable for things posted on its web site by others. See Playboy Enterprises Inc v. Russ Hardenburgh, Inc., 982 F. Supp 503 (ND Ohio 1997).

The Digital Millennium Copyright Act (("DMCA") (17 U.S.C § 1201 et seq; passed by Congress in 1998) makes changes in United States copyright law to address our current digitally networked environment. The DMCA provides for a limitation on "online service providers" liability for monetary damages and injunctive relief with respect to copyright infringement in certain circumstances. It adds a safe harbor to the current United States copyright law. Online service providers are defined as those entities that link users to the Internet and facilitate the transmission of digital data that is translated into another party's copyrighted work. The DMCA provides a safe harbor from liability for online service providers if their online system complies with the procedures and certain requirements set forth in the DMCA, which include the following: (1) the organization meets the definition of an online service provider, (2) the organization engaged in covered activities, and (3) the organization meets the conditions in the DMCA for material, parties to transmission, and procedures. To qualify for the limitation, the material that is transmitted online must be made available by someone other than the online service provider, and the online service provider cannot modify the material. In addition, the online service provider cannot have actual knowledge of any copyright infringement and must cooperate with the processes to disable access and limit harm to the copyright owner in the event of infringement. The safe harbor does not apply to copyrighted material the online service provider may place online itself or through independent contractors, such as on its home page; such material is subject to a traditional copyright analysis under current law.

B. Defamation

In general, courts have been reluctant to hold web site owners liable to defamatory statements made by others on its web site, such as statements made in chat rooms and other interactive medium. The Communications Decency Act, passed in 1996, states that no provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider. To date, courts have treated this language as a nearly complete bar against liability for users' defamatory postings. The safe harbor only applies to information provided by another organization or person, however, and does not apply to information put on the web site by the defendant itself.

As a result, in general computer bulletin board services are not liable when people post things without authorization and the web site operator does not create or control the content of the information available to its subscribers, but merely provides access to the Internet. In Cubby, Inc. v. Compuserve, Inc., No. 90 Civ 6571 (SDNY 1991). Cubby was suing Compuserve for libel, unfair competition, and business disparagement based on allegedly defamatory statements made in a publication included in a computerized database. The court found that Compuserve had no opportunity to review the allegedly defamatory information before it was uploaded into computer banks, from which it is immediately available to subscribers. In addition, Compuserve received no part of the fees charged for access to the relevant database; it has just one main subscription fee. The court found that Compuserve acted as a distributor, and not a publisher, of the statement and cannot be held liable for the statement because it did not know and had no reason to know of the statements. Once Compuserve decides to carry a publication, it has little or no editorial control over that publication's contents. In this situation, Compuserve is like a bookstore, library, or news stand.

On the other hand, an operator may become liable if it takes affirmative steps to cause copies to be made. For example, if a bulletin board service encourages people to upload documents, and it screens all documents and moves them to the appropriate generally available files, it may be considered to have "republished" the material. One who repeats or otherwise republishes defamatory matter is liable as if he or she had originally published it. But, vendors and distributors of such matter are not liable unless they knew or had reason to know about it. In Stratton Oakmont, Inc. v. Prodigy Services Company, Supreme Court, State of New York Index No 31063/94, Stratton is suing Prodigy for libel based on allegedly defamatory statements made in on Prodigy's "Money Talk" computer bulletin board. Prodigy held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition, and expressly likening itself to a newspaper. It has a series of "content guidelines" and enforced them through an automatic software screening program. Prodigy actively utilized technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and bad taste, Prodigy is clearly making decisions as to content and such decisions constitute editorial control. As a result, Prodigy is a publisher rather than a distributor and can be sued for libel. Prodigy's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than other computer networks that make no such choice (such as Compuserve, above).

C. Risk Management

The following are suggestions for a web site to take to minimize its risk regarding potential copyright infringement and defamation liability:

1. Do not actively monitor the web site. Active monitoring of the web site will give the web site actual or putative knowledge of user conduct and content. Thus it creates the possibility that a web site will be liable for all user harms except those preempted by the safe harbor described above.

2. Consider empowering independent contractors to monitor your site and give them the authority necessary to resolve problems.

3. Respond to complaints promptly.

4. Review your user agreement(s). Provisions enabling the web site to blacklist subscribers or edit content on subjective or arbitrary standards provide strong evidence of the web site's right and ability to control its users and their content. User agreements should only prohibit users from engaging in conduct that is illegal or tortuous.

5. All employees who interact with the web site can take legally significant actions that could undermine a risk management strategy; thus the web site's risk management strategy should be explained to all employees, and employees responsible for dealing with web site problems should be given special training on how to implement strategies.

VI. Personal Jurisdiction via Electronic Records

The minimum contacts required for personal jurisdiction in another state can be electronic. As a result, an organization that posts advertisements on the Internet through its web site may be subject to jurisdiction in all states in which such information can be accessed. For example, in Inset Systems Inc. v. Instruction Set, Inc. (937 F. Supp. 161, 1996), the court found that ISI was subject to Connecticut jurisdiction because it had a toll-free telephone number and an Internet web site on which it posted advertisements. There are at least 10,000 Internet-connected computer users in Connecticut, all of which could access ISI's advertisements again and again.

In addition, a person who conducts business via electronic mail with a person in another state is subject to jurisdiction of the courts in such state. In Hall v. Laronde (666 CA Rptr 2d 399, 1997), a California court held that a person living and working in New York may be sued in California when he negotiated the purchase, and of software modification from a California resident via electronic mail and the telephone, even though the California resident reached out to the defendant first. The defendant worked with the California resident through a period of time, and made continuing royalty payments, thus creating a continuing obligation between himself and the California resident.

VII. Uniform Electronic Transactions Act

The purpose of the Uniform Electronic Transactions Act (UETA) is to develop an act relating to the use of electronic communications and records in contractual transactions. The UETA governs electronic records and signatures relating to a transaction, defined as limited to business, commercial and governmental affairs. It is intended to be consistent with the Uniform Commercial Code, but not duplicative of it. As a result, the UETA is procedural and affects the underlying substantive law of a given transaction only if absolutely necessary in light of the differences in media used. Whether a record is attributed to a person, and whether an electronic signature has any effect, is left to other substantive law.

The UETA expressly validates electronic records, signatures, and contracts. It affects the medium in which information, records, and signatures may be presented under current legal requirements. It provides for the use of electronic records and information for retention purposes, providing certainty in an area with great potential in cost savings and efficiency. The UETA makes clear that the actions of machines programmed and used by people will bind the user of the machine, regardless of whether a human was involved in a particular transaction. It also specifies the standards for sending and receiving electronic records. It does not specify the standards for an electronic signature, however. Certain legal rules requiring certain writing and signatures under law are not affected by the UETA (such as wills, etc). It applies only to transactions between parties who have agreed to conduct transactions electronically; it is intended to facilitate the use of electronic means, not require the use of electronic records and signatures.

The requirements for electronic transactions are as follows:

1. Confidentiality: the contents of messages or substance of transactions must be kept secret to unauthorized parties.

2. Access control/confidentiality: the information is only available to authorized parties; the access to information is controlled, and distribution or disclosure of the records is restricted.

3. Chain of custody: the authentication of stored electronic records (this strengthens the credibility and privacy of records).

4. Message integrity: the message is not tampered with; it is accurate.

The UETA provides that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. The medium in which a record, signature, or contract is created, presented, or retained does not affect its legal significance. It also provides that electronic records and signatures do satisfy legal requirements for writings and signatures, provided the parties have the ability to retain (print or download) the information for later review. An electronic record or electronic signature is attributable to a person if it was the act of the person. It may be proven by showing the efficacy of any security procedures applied to determine the person to whom the electronic record or signature was attributable.

The UETA also governs the retention of electronic records. It states that if a law requires certain records (including checks) to be retained, that requirement is met by retaining an electronic record that accurately reflects the information and remains accessible for later reference. The requirement of continuing accessibility addresses the issue of technology obsolescence and the need to update and migrate information to developing systems. The UETA would permit parties to convert original written records to electronic records for retention, and states that electronic records can be considered originals so long as the accuracy and accessibility requirements are met. The concern focuses on the integrity of the information and not with its originality. So long as there exists reliable assurance that the electronic record accurately reproduces the information, the electronic records and paper-based records are functionally equivalent.

The UETA provides that, in a legal proceeding, evidence of an electronic record or signature may not be excluded from evidence because it is an electronic record or signature, or it is not an original. Admissibility of evidence depends upon the substance of the information rather than the media in which the information is presented.

The UETA contains provisions specific to electronic records by government agencies. It authorizes (but does not require) state agencies to use electronic records and signatures generally for intra-governmental purposes, and to convert written records and manual signatures to electronic records and signatures. It gives an option to leave the decisions to each government agency or to assign that duty to a state officer. It also authorizes the destruction of written records after conversion to electronic form. In addition, the UETA broadly authorizes (but does not require) state agencies to send and receive electronic records and signatures in dealing with non-governmental persons. The UETA requires government agencies or state officers to take account of consistency in applications and interoperability among state agencies to the extent practicable when promulgating standards. For purposes of check retention statutes, the same electronic record of the check is covered by the UETA, so that retention of an electronic image/record of a check will satisfy such retention statutes so long as certain requirements are fulfilled.

Appendix F, Section 1
Data Warehouse: Operational

Agency:
Minnesota Department of Finance

TIS Evaluation Meeting Date:
25 March 1999

State Archives staff:
Shawn Rounds, Mary Klauda

Department of Finance staff:
Ellen Schwandt, Darryl Folkens

Agency Function:
To improve the performance of state government in the area of statewide financial planning and financial resource management. Goals of the department include ensuring the integrity of the state's financial resources, providing governmental financial management leadership, accurately presenting the state's financial condition, facilitating informed decision making, and improving the accountability and the prudent use of state resources. The department offers services in business administration, information management, and analytical services.

System Name:
Information Access Data Warehouse

System Function:
The Finance Department's Information Access Data Warehouse holds general ledger, accounting, and procurement data and payroll/personnel data from state agency source systems. The warehouse converts and stores, in a common storage format, selected data that is extracted from the state's payroll/personnel system (SEMA4) and the state's general ledger, accounting, and procurement system (MAPS). At the time of the evaluation, the warehouse logged 750 users each month, drawn from virtually all state agencies. It is a critical business system for many state agency decision makers. Information about the Information Access Data Warehouse is available on the Finance Department's web site: http://www.finance.state.mn.us/index.html

System Development Phase:
In operation since 1 July 1995. Planned move from SQL Server to Oracle; target date was 16 August 1999.

Background:

The Finance Department's Information Access (IA) Department is responsible for the warehouse system as a whole; there is joint responsibility for applications with the Department of Employee Relations and the Department of Administration. System trustworthiness had been considered, to some extent, in June 1998 when the Office of the Legislative Auditor conducted a data integrity review of the warehouse. The auditors concluded that the Finance Department had controls in place to ensure the integrity of data in the warehouse and controls to protect warehouse data from unauthorized changes.

The warehouse is a repository of data extracted from the source systems, so many of the laws and regulations (e.g., data practices act, records statutes) applying to data in the source may apply to data in the warehouse.

There are legal and preservation issues that need to be addressed as the warehouse evolves. Data access issues frequently are not well thought-out in the source systems and the problems are inherited and exacerbated in the data warehouse. Even as source system agencies address their own legal issues for information systems, there is an entirely new set of issues as data from source system agencies is joined in the warehouse. There are inconsistencies between what data is retained or purged from the source systems and the source system data in the warehouse. Warehouse records retention schedules must coordinate somehow with those pertaining to the source systems. IA staff are looking at ways to develop and implement a records disposition plan.

Since the warehouse acts in a repository capacity, it does not serve as the official place of record for any of the information from the source systems. The source systems hold the official records.

System Documentation:

The IA Department has documentation in place on the procurement, installation, maintenance, and support of system's hardware, software, and communications networks. Interconnected systems are documented; some documentation on interconnected systems may not be explicit since the system is relatively small. There are some mainframe connection security issues, and the warehouse is undergoing a security review to determine system vulnerability and ways to prevent access to the system at various points.

System Documentation—Policy and Procedures:

IA staff document programming conventions and procedures, development and testing procedures, and applications and procedures for data entry and access, data modification, data duplication, data deletion, and indexing techniques.

There is documentation on warehouse system record formats and codes. There is limited documentation on source system record formats and codes. IA staff rely on the source systems to provide users with information on what codes appear in the tables.

IA staff routinely back-up the system; backups, stored off-site and off-line, are subject to periodic integrity testing. They also routinely perform quality assurance and control checks on data. For example, there are checks to ensure that data cannot be loaded more than once. New software is installed in a test mode, with nothing being put online without first going through a test environment. There are measures in place to ensure that identification devices are functioning properly and that staff with access to the warehouse system have had security checks. The warehouse has its own computer room and its locks are changed frequently. IA staff perform quality assurance and control checks of storage medium. Eventually, the system will register when hard drives and tapes fail, triggering an automatic notification.

There is documentation on plans to migrate data to new systems, but it does not include procedures for all aspects of the migration. IA will be moving warehouse data from SQL Server to Oracle in the near future. Issues remain about which data to archive. IA staff realize the importance of retaining all parts of the data sets, but they have yet to resolve how this will happen.

System Security—User Authorization:

There are documented user identification and access procedures in place. All users are authenticated before gaining access to the system, and users are assigned a unique identifier and password. Access scripts with embedded passwords are allowed for accessing source systems' batch work. There are standard password rules for minimum password length and expiration dates. There is no limit to the number of log-on attempts per session. Since access to warehouse data is read-only, there is limited risk involved. The Finance Department has staff who respond to security incidents.

System Security—System Access:

Users and IA staff are granted warehouse access only to the level necessary to perform job duties. There is a limited number of authorized staff who can create, modify, and delete records and alter their disposition codes. Users have read-only access. Only database administrators are able to modify record identifiers. The system tracks current authorized users in a database and user lists are reviewed regularly to adjust for changes in user authorization status. There is an on-going process to review staff positions for necessary security levels. The warehouse staff is small and responsibilities are fragmented among many personnel. Position responsibilities will change as the warehouse grows. Generally, staff duties and access restrictions are arranged so that no one with an interest in record content is administering system security, quality controls, audits, and integrity testing. No individual is able to compromise single-handedly warehouse security and operations.

System Security—Internal:

For internal system security, access to system disks and to the server is controlled and monitored, although access to printers is not. Because users have read-only access, there is no concern about control over the user environment. All data from source systems is treated as secure data while it is being archived, purged, or moved from system to system. Once data is loaded into the warehouse, it is subject to system security. There are procedures in place for sanitization and secure disposal of hardware, software, and storage media when no longer needed. Security procedures are reviewed on a regular basis as necessary. Measures are in place to safeguard the system's physical security. IA staff felt that internal security issues such as facility structure and heating are very important, and that they were not examined thoroughly at the beginning of system development. They are now rectifying physical structural problems that may have been avoided.

System Security—External:

System users currently access the warehouse with full password rights. IA staff are considering moving the warehouse to a web-based user environment. When that happens, it will be very important to do a risk assessment to look at all of the security implications. There is virus detection in place on desktop computers for external system data; it is not known whether that is the case with the servers.

Audit Trails:

IA staff can run trace files and do high-level usage reporting. For instance, they can determine how many people have accessed the warehouse and for what types of reports. Oracle tools may allow closer examination of usage in the future. IA staff operate under the assumption that the users are the owners of the data in the warehouse. Their interest in having audit trails is for performance and information management purposes only, not as a true auditing tool.

Disaster Recovery:

The warehouse has a database recovery function that is reviewed and tested periodically. There is no plan in place for the entire operating system. Although staff know they can recover from a disaster event, and have done so in the past, there is a need for a more complete and formal plan. IA staff still need to identify hardware, connections, and off-site hardware platforms. There is an opportunity to implement a comprehensive disaster plan when they move to Oracle.

Data Warehouse—Specific Considerations:

IA staff document procedures and gather metadata as data is extracted from the source systems and as data is cleansed and transformed for the warehouse. There is minimal data cleansing that occurs and cleansing and transforming procedures are described. In preparing for the move from SQL to Oracle, more issues on documenting and describing data transformation have come to light. Users can view all metadata and documentation including table and view definitions, element definitions, table information, indexes and elements, join keys, dictionaries, sample metadata reports, and source system information. The metadata is readable by anyone, but can be manipulated only by IA staff.

Appendix F, Section 2
Web-Enabled Data Repository: Test Phase

Agency:
Department of Children, Families and Learning (DCFL)

TIS Evaluation Meeting Date:
2 June 1999

State Archives Staff:
Mary Klauda, Shawn Rounds

DCFL staff:
Mark Manning, Theresa Mish, Mary Lillesve, Michael Riecken (Signature Software contractor)

Agency Function:
To help communities measurably improve the well-being of children through programs that focus on education, community services, prevention, and the preparation of young people for the work environment. Department efforts emphasize achieving positive results for children and their families. Its programs address family breakdown, violence, and poverty. The department strives to make accessible its educational and community resource services and encourages collaboration between state education professionals and social services advocates in order to meet the needs of Minnesota's children and families.

System Name:
Minnesota Electronic Curriculum Repository (MECR)

System Function:
The MECR is a quality-controlled database of curriculum materials that supports the implementation of the Minnesota Graduation Standards. The repository contains information on content standards, scoring criteria, large processes and concepts, state model performance packages, assessment tasks, learning activities, and other learning resources. The primary users of the MECR are teachers and other educational professionals (e.g., administrators, curriculum developers, technology specialists, counselors) seeking high-quality curriculum materials to design and deliver instruction for the standards. Other users might include parents, students, policy makers, legislators, and in-service teacher training program staff. Access primarily is web-based and available at: http://mecr.state.mn.us/home [NOTE: As of 2003, MECR and this URL are no longer active].

System Development Phase:
Operational as of 1 June 1999

Background:

DCFL is responsible for development of the MECR. The system was planned and developed as a way to better implement and disseminate information about the Minnesota Graduation Standards. The MECR also will allow for efficient and timely updates of curriculum guidelines as graduation standards are updated by the Legislature.

The MECR is available to school districts via the Internet and CD-ROM. The CD-ROM version includes Java Runtime, a mini web server, an Internet browser, the entire contents of the database, source code, documentation, and executables. There currently are no version-tracking procedures. Software will be updated as the system warrants.

Users can create assessment tasks, learning activities, and learning resources based on the MECR once user accounts are established. School districts can change the curriculum to suit individual district goals, but after having done so, districts are responsible for curriculum content and implementation. The system does not support random changes. However, new curriculum information can be submitted for approval and inclusion to the MECR.

Prior to the MECR, the official version of state curriculum guidelines existed in paper formats. Most of the data in the MECR is new content. Once the system is operational, the electronic version will be considered the official record. State models and rules that serve as background for the MECR will remain in paper formats; policy documents for the MECR are in both paper and digital formats.

The MECR is subject to Minnesota Statutes, Chapter 3501, which established the Graduation Standards. The Data Practices Act (Minnesota Statutes, Chapter 13) does not apply to the system since none of the system data is about individuals. However, since individuals set up user accounts to log on to the system, data practices issues may pertain to the log-on information. This may require further investigation.

Records retention requirements for MECR data have not been fully identified. Permanent retention of any graduation standards information has yet to be addressed. Retention may be based on graduation years and/or updates of graduation standards. Plans are in place to have snapshots of the system data for graduation standard years.

MECR staff thought it would be a good idea to retain snapshots of the web presentation of the MECR for historical purposes. The system has some capture mechanism, and CD-ROMs may be a viable means for retaining snapshots.

During the initial stages of system development, the MECR web pages were hosted by Signature Software. The site will move to DCFL soon after the system is operational.

System Documentation:

DCFL does not have an agency-wide methodology for all aspects of system documentation. For the MECR, system operating procedures currently are in development. New entries are tracked in a log that records creators, dates of creation, and whether or not the new entries are approved. Design reviews and system tests were performed and documented before the MECR went into production. Maintaining audit trails of hardware and software changes may be considered in the future. There is an archive of all software. No one is able to make changes to the system without going through a change-request procedure followed by a review process.

DCFL has documentation on the procurement and installation of MECR's hardware. Hardware is self-installed by staff and installation procedures are outlined. There have been no hardware modifications on the MECR to date, although the physical location of the system will be changing and that move will be documented. Future issues of hardware maintenance need to be addressed, specifically issues of cost and staff responsibilities. Documentation exists, or will exist, on the procurement, installation, modification, and maintenance of the system software. DCFL, as an agency, is finalizing a policy about use of agency-authorized hardware and software, and the MECR will be subject to the terms of that policy.

The MECR is connected to the communication network infrastructure at DCFL. DCFL documents all network procurement, installation, modifications, and maintenance. The Internet is the only means of external system access to the MECR, and it is the system's main connection with school districts. School districts can choose to install MECR onto their own network systems off CD-ROM through a documented installation procedure.

System Documentation—Policy and Procedures:

System documentation includes conventions and procedures for developing, programming, and testing. Periodic functional tests are performed that are basically self-testing routines for objects before they are plugged into the system; the tests are not documented thoroughly. There is user documentation on applications and associated procedures for entering and accessing data in the MECR. There is database documentation only for the initial raw data entry. There are applications and procedures for internal indexing of the database, but no indexing for external systems data. System output, namely the web user interface, is documented.

System documentation includes record formats and codes for the database and procedures for identifying when system records become official. Additions to the MECR must be approved by a review authority and new entries are considered works-in-progress while they are under review. Records become official after review, approval, and publication. This is the only quality-assurance and control-check on system data. There is a mechanism for routine performance of system backups, but documentation on this is not complete. Backups are stored in secure, off-line, off-site storage; there are no integrity tests performed on backups. Storage mediums do not regularly undergo statistical sampling in order to identify data loss and corresponding causes, however MECR staff felt that this was an important consideration for the future. System documentation does not include plans for migration of records to new systems and media. There is an installation guide designed primarily to assist school district systems administrator in installing the MECR on different systems. User documentation and training on the MECR for mid-level administrators is available.

System Security—User Authorization:

Information in the MECR is public, and DCFL wants the public to be able to easily access system data. To promote access, there is a generic user account for people who wish to access the MECR, but who do not want to identify themselves. These users have limited read-only access and can print any public data.

Some users must be authenticated prior to being given access to certain areas of the system, and identification and access procedures for these people have been established and documented. Although each user has a unique identifier and password, there is no way for DCFL to monitor sharing of identifiers and passwords. User names and user identifiers are unique; passwords are not guaranteed to be unique. There is no means to control the use of access scripts and embedded passwords on the client-side of the system. The system terminates individual user sessions after a certain time period of inactivity. Password rules include a minimum password length, but do not establish expiration dates or a maximum number of log-on attempts.

A help desk responds to any security incidents. System security administrators approve access for users. There are no formal procedures in place to ensure that user access corresponds to the level of access necessary to perform job functions. Staff positions have not been reviewed to ensure that they have been assigned appropriate security levels. MECR staff thought that there should be such procedures in the future. Permissions to create, modify, and delete records are granted only to authorized users with proper clearance. Modification of record identifiers is prohibited. Permissions are assigned to user groups rather than individual users. DCFL maintains lists of all current and past authorized users, but lists do not include corresponding privileges and responsibilities. These lists are not reviewed regularly to make adjustments for removal of former employees or clearances for workers with new job duties, but MECR staff felt that some method of review should be implemented.

System Security—Internal:

MECR staff felt that issues of access to all systems documentation need to be addressed by DCFL as an agency. For the MECR, system output and storage devices are in a locked, controlled-access facility. There are controls to ensure security while data is being archived or moved, and procedures have been established for moving system backups to off-site storage. The DCFL information systems office has procedures for, and documentation on, the sanitization and disposal of all agency software and storage media when no longer needed. There are no procedures for sanitization and disposal of obsolete hardware, nor any policies addressing re-use of software, hardware, or storage media. There currently is no online insecurity-detection mechanism, but this issue will be addressed in the future. MECR staff felt that there should be a better process to minimize failure of primary security measures and more timely review of security procedures and rules. Various safeguards maintain the MECR's physical security. Plans are underway to train security administration personnel, ensuring their complete knowledge of MECR's security system.

System Security—External:

There are security measures relating to remote access to the MECR via the Internet; there are no direct telephone connections to the MECR. Non-system records and data are not imported directly into the MECR. Verification of the sender/source, origin, and integrity of non-system records takes place through the approval process. After approval, records/data are entered into the system. There currently is no means to detect viruses on non-system records. MECR staff felt that there should be an automatic mechanism to scan the system on a routine basis.

Audit Trails:

The MECR does not have traditional audit trails. Two forms of access logs are maintained instead: access logs as a function of the web server and internal access logs in the database that includes incoming URL information. Status logs for records in the database are maintained, but they are overwritten so that only the most current status if available. Anyone with access to directories on the server can access the audit data. Ideally, this information should be available only to the database or system administrator. Access logs are backed up on the same schedule as the rest of the system. A system logs and tracks users, noting user identifiers, record identifiers, dates, times, and types of usage.

Disaster Recovery:

There is no disaster recovery plan, but there is recognition by DCFL information systems staff of the need.

Record Data:

Data in the MECR is considered an official record only after it has gone through the approval process. Components of a complete or final record depend on the record type. Generally, record components include type and identifier, creator, current status, status date, and record information. MECR data is not considered transactional. Upon approval, the original content, format, and structure are preserved, and each record can be printed or represented as it originally appeared at time of official acceptance. Record data, documents, and metadata are not accessed, displayed, and managed as a unit. MECR staff will need to define a records disposition plan for the MECR, as well as determine who is responsible for authorizing and altering that policy.

Record metadata includes unique identifiers, dates of creation, creator and documentation of creator’s authorization, date and time of modification (i.e., server date and time), modifier (individual or organization) and documentation of modifier’s authorization, and indication of authoritative version. The media type is always the network, the format is always keyed-in internally, and the location of record is always within the database.

Appendix F, Section 3
Web-Enabled Electronic Bidding System: Test Phase

Agency:
Minnesota Department of Transportation (Mn/DOT)

TIS Evaluation Meeting Date:
22 July 1999

State Archives Staff:
Mary Klauda, Shawn Rounds

Mn/DOT Staff:
Sue Dwight, Gary Ericksen, Bill Gordon, Mike Martilla, Nancy Sannes, Gus Wagner, Joel Williams, Lynn Klessig (Office of the Attorney General, attorney for Mn/DOT legal issues), Charles Engelke (InfoTech, vendor)

Agency Function:
The Transportation Department is charged with providing a balanced transportation system for the state that includes aeronautics, highways, motor carriers, ports, public transit, railroads, and pipelines. The department is the principal agency for developing, implementing, administering, consolidating, and coordinating state transportation policies, plans, and programs.

System Name:
Electronic Bidding System (EBS) — Expedite, Bid Express

System Function:
The Electronic Bidding System (Expedite) will allow Mn/DOT to distribute contract bid items to contractors who can then prepare and submit bids electronically (via Bid Express, a third-party web site, and the Internet) to Mn/DOT. Expedite is a module of TRNS-PORT, an electronic system already in place in the department. Files from Expedite that are transferred into the system are brought into TRNS-PORT. The American Association of State Highway and Transportation Officials (AASHTO) licenses TRNS-PORT; a vendor, InfoTech, is charged with maintaining, changing, and enhancing TRNS-PORT. Bid Express is not a module of TRNS-PORT and is controlled and owned by InfoTech. AASHTO has no plans to purchase Bid Express. If successful, the system will eliminate the need to retain a paper-based system of contract bids. During the pilot project, the department will continue to accept paper bids.

System Development Phase:
Test Phase: marketing and implementation of pilot project.

Background:

Mn/DOT chose to evaluate its Electronic Bidding System (EBS) for trustworthiness as the first part of a risk assessment of the system during its pilot phase. The process of distributing and submitting contract information and bids is not new to the department. However, the addition of an electronic bidding component to the existing system brings up more and new considerations on how system information is administered.

Several state and federal laws are, or will be, in place that pertain to EBS data. Of particular concern are laws governing circumstances for the use of digital signatures, since EBS will rely on digital signatures for authentication of bidders. There are no industry standards that exist for system data and data security. System security standards are being addressed agency-wide by Mn/DOT's Information Resource Management (IRM) units. The department has records retention schedules in place for agency data, but they are based on a paper system.

There are several legal issues involved with system data, particularly concerning proofs of proper execution of a bid, valid signatures and bid bonds, correct completion of bids, and proper authority for bid signatures. Existing system data is audited every two years, per statute. Auditors routinely look at procedures for accepting bids and verification of proper insurance. Some of the contract bid data is classified under the state's data practices act, but all data is public after the award of a project. None of the data contain personal information.

System Documentation:

System documentation is complex because responsibilities extend to Mn/DOT's various IRM units, to the business units involved with deploying the system, and to the vendor, InfoTech. Documentation also applies to three systems, both internal and out-sourced: Expedite, Bid Express, and TRNS-PORT. System documentation is covered by department records retention schedules. Currently, system data resides on a mainframe, and access is strictly controlled in that environment. However, a variety of access issues need to be addressed as system data is moved from the mainframe to a client-server environment. The department's central IRM unit maintains documentation on system hardware. InfoTech heavily documents its software and maintains a revision history.

System Documentation—Policy and Procedures:

Some system documentation is covered by agency-wide IRM policies and procedures. TRNS-PORT programming conventions and procedures follow the guidelines and standards of AASHTO. Staff felt that sufficient documentation exists on development and testing procedures, applications, quality assurance and control checks, and data migration for EBS and TRNS-PORT. Documentation by Mn/DOT and InfoTech specifies standard training and terms-of-use agreements for all system users and personnel, including contractors.

System Security—User Authorization:

InfoTech and Mn/DOT both are responsible for EBS system security, but at different times, depending on the time of public bid openings. InfoTech handles documentation and implementation of security measures and access permissions from the time a contractor files a bid until the time of its public opening. After the public opening, responsibilities are passed on to Mn/DOT. User authorization is important to the system's success, and it is strictly controlled and monitored. Agency-wide user authorization policies also apply to EBS.

Since InfoTech is not a Minnesota company, bonding companies serve as the authenticating parties, enabling contractors to submit bids electronically. This issue is significant and may necessitate Mn/DOT's examining the level of trustworthiness for this system as well. The Secretary of State currently recommends that identities for digital signatures be established by a person's physical appearance. It was recommended that Mn/DOT obtain an Attorney General's opinion about changing any of these established procedures and requirements.

System Security—Internal and External:

Agency-wide IRM policy controls and monitors most aspects of internal system security. Adequate controls are in place, however, certain procedures, such as software and hardware sanitization and disposal, need further review. The department follows AASHTO's fixed schedule for reviewing security procedures and rules. Moving data from Expedite to TRNS-PORT will require additional security. There are procedures in place to control and monitor external system security.

Audit Trails:

Audit trails are maintained and users online actions are monitored adequately by InfoTech while bids are open. Mn/DOT tracks any addenda to bids after the public bid opening. Authorized users can access audit data, but cannot alter, add, or delete audit data. Access to audit trail software is controlled, protected, and monitored. Audit trails are backed-up every business day.

Disaster Recovery:

InfoTech relies on backup storage in the event of a disaster or system failure and has a mechanism in place to ensure the non-stop functioning of Expedite. Mn/DOT has a disaster plan in place that is reviewed periodically. Mn/DOT staff felt that additional back-up procedures need to be established for the client-server configuration and that there needs to be better off-site storage for backups.

Record Data:

Bid files are the primary records created by EBS. The bulk of the bid files require a seven-year retention period after bid letting is complete. Portions of the successful bid files have a twenty-year retention period. The system will retain, for each record, the original content, and format, context, and structure, along with a comprehensive set of metadata. For encrypted bid files, decryption keys must be retained as well since there needs to be a way to access the files. The department is developing a migration plan for the system's permanent/historical records.

Appendix F, Section 4
Transactional System: Analysis Stage of Development

Agency:
Minnesota Housing Finance Agency (MHFA)

TIS Evaluation Meeting Date:
2 November 1998

State Archives Staff:
Mary Klauda, Shawn Rounds

MHFA Staff:
Karmel Kluender, Dave Ruch, Renata Anderson

Agency Function:
To provide affordable housing to low and moderate income Minnesotans through a number of resources. The agency has 160 employees and operates programs that provide financing for a variety of housing needs from multi-family housing complexes to home ownership and home improvement loans.

System Name:
ALPHA (existing mainframe system) and the new information system in development, based on the CORE project. The CORE project identified the process by which major business functions within MHFA need to be tracked through an enterprise-wide system. The project was called CORE because it addressed the core, or heart, of the business processes used within MHFA for meeting its mission and goals.

System Function:
The new system, based on CORE, will be an enterprise-wide information system encompassing all aspects of the agency's business as it builds programs, raises capital for and markets them, processes requests for funding (loan applications), disburses program funds, and finalizes all of the legal program documentation. The current ALPHA system does not encompass the entire enterprise. The programs that currently are the mainstay of single family loan activities (home ownership and home improvement) are processed on this system. Many other single family and multifamily programs and their associated business processes are tracked in a variety of desktop software packages or manually in some cases. The information gathered from the efforts in the CORE project will be used to determine the best approach to decide whether to purchase or build an enterprise-wide information system.

System Development Phase:
Analysis; conceptual data model and process model.

Background:

The MHFA agreed to evaluate the Trustworthy Information Systems (TIS) criteria in November 1998. It was an opportune time for the State Archives (SA) since it was soon after the criteria had been developed. The SA needed an initial test case to determine how an agency might use and implement the criteria before promoting the idea as a project to the Information Policy Council (IPC). The evaluation with MHFA essentially tested the TIS criteria as a proof of concept; it validated the criteria set and gave the SA additional credibility to pursue the TIS project with the IPC. MHFA and the SA were logical partners for two reasons: 1) The two agencies had been working together since April 1998 to develop electronic records management and archival procedures, and 2) The MHFA had a new information system, based on the CORE project, in the early stages of development.

Evaluation Session:

The session with MHFA was informally facilitated and recorded. At the time, the SA had yet to develop a methodology for carrying out the evaluation sessions. Since the analysis phase of system development had just been completed for the CORE project, comments regarding the criteria were based on both current/ALPHA system design and procedures and a future vision of how a new system should be designed, implemented, and supported. It also was an ideal time to begin examining system trustworthiness. The meeting lasted two hours.

General Reactions to TIS Criteria:

MHFA staff found the TIS criteria useful. They appreciated having the full range of information system considerations in one document, even though many of the criteria did not apply to their agency and systems at this point. Staff had considered many of the criteria during the system analysis, but never had a structured way to document how some elements would be carried out and who would be responsible for providing and maintaining the documentation. The criteria could provide that structure.

Some of the criteria addressed issues that had not been considered fully during analysis, but ones that may become important in the future, an example being the many system security and documentation implications for handling transactions over the Internet. This will be an issue in the near future. Another benefit to the approach was documenting, in a structured way, the reasons for implementing/not implementing particular criteria considerations. For example, information systems staff had an informal understanding regarding retention of system documentation, but it was not covered in the agency's records retention schedules. MHFA staff intend to examine the criteria again as the system is developed further.

Assessing risk was the most relevant factor in determining which criteria were the most important to consider. For each of the criteria, risks of not meeting the criteria were weighed against implementation. The agency's activities are primarily financial in nature and they are audited routinely, hence financial transaction applications receive the most scrutiny and pose the highest risk. For MHFA system applications dealing with money, it was important to avoid the risk of assigning system security responsibilities to staff with an interest in the transaction or record content. Therefore, the system, as it is developed, will include procedures and personnel access restrictions so that only limited staff with an interest in the record content will be responsible for administering system security, quality controls, audits, and integrity tests.

Information systems staff felt strongly that the criteria were important, but that the decision on whether to implement had to be based on policy and business rules that required agency management consideration and input. They stressed the need to educate system users and management on the ramifications of information technology and its application as it pertains to policy issues. For example, the agency needs to address whether the electronic record of a transaction is the official record and, if so, when it becomes reliable. Agency management and users, not the information systems staff, need to answer these questions.

System Documentation:

MHFA system documentation includes data on hardware and software, its procurement, installation, modifications, and maintenance, and data on its communications networks. Further documentation considerations need to be addressed if and when client interactions take place over the Internet. Documentation does not take into account whether state- or agency-approved hardware or software is installed. As remote access and telecommuting become more common, it will be virtually impossible to monitor this.

System documentation, specifications, program manuals, and user guides are not formally scheduled in the agency's records retention schedules. There is an understanding that this documentation should be in their schedules, but it currently is not. The information systems staff have an informal retention understanding that documentation should be retained until the system is no longer used and that the system data be retained or destroyed in accordance with established records schedules, if they exist.

System Documentation—Policies and Procedures:

Policy and procedure documentation includes programming conventions and procedures. Development and testing activities are recorded. Procedures for entering and accessing data; data modification, duplication, deletion; indexing techniques; and outputs are all addressed in a user manual that is external to the operating system. The identification of an official record and when it becomes reliable is something that is not within the purview of information systems staff; this needs to be addressed by users and the MHFA administration, but it currently is not.

System procedures include record formats and codes, and there are routine system back-ups. Backups are labeled and stored in a secure, off-line, off-site location, and subjected to periodic integrity testing. System staff do quality assurance and control checks and performance and reliability testing of hardware and software. They do not consult with the manufacturer. Systems do not include periodic testing of identification devices. They have addressed migration of records to new systems and media in the analysis phase. Migration issues will be considered again as CORE is developed further. Migration of records should be addressed in records retention schedules.

The agency has standard training for users and staff with access to system hardware, software, and system data.

System Security—User Authorization:

The agency allows users one password with multiple sign-ons for the various systems and platforms. Individual user passwords are the same for all systems. They found that if there are too many identifiers, users tend to forget passwords or keep them someplace that is not secure (for example, a Post-It note on a computer). They would like to go to a single identifier, and, ideally, a single sign-on for all hardware and software applications.

The agency has no password dictionary, however, it does have a list of key system identifiers and passwords. They are not associated with a single person. The list includes the level of access for system users, who are allowed access to the system only at the level necessary to perform their job duties. Expiration dates for passwords are established within the system; password re-use is not allowed.

Permissions to create, modify, update, and delete records, and permissions to alter disposition codes are controlled by the applications. The agency controls user access to applications, so in effect, permission control is achieved. Access to private keys for digital signatures is not an issue at this time, but it may be at some point if mortgage applications are taken online.

System Security—Access and Security:

Identification and access procedures are established and documented. User authorization forms are required before system access is granted. There is paperwork to back-up user identifiers. There is no system in place to log and track users and their online actions, nor does the system supply users with the Tennessen Warning when collecting confidential data. The Data Practices Act applies to only a few of their clients. Staff were not sure whether the Tennessen Warning was supplied in their manual paper-based system.

There are insecurity-detection mechanisms in place, as well as audit and security alerts. Security procedures and rules are reviewed on a routine basis to ensure currency. Measures are in place to guard the system's physical security. Security administration staff undergo training to ensure full understanding of the security system's operations.

The agency does not control and monitor access to system documentation. This was a level of security that MHFA staff felt they could forgo because it is costly and burdensome, and they can live with the limited risk involved.

There are additional security measures in place in cases of remote access to the system. However, as more business is done over the Internet, more security is needed in this area.

Audit Trails:

The agency tracks transaction information with regard to money, and there is the ability to reconstruct audit trails from log journals. The logs are kept only for a limited period of time, and they are not maintained independently from the operating system. The logs serve as a disaster recovery mechanism rather than as an audit trail. Staff view maintaining an audit trail, particularly one that is independent from the operating system, as a very high-cost proposition. They understand its importance, but cannot justify the costs for the limited risk situations.

Disaster Recovery:

There is a disaster recovery plan in place that includes hardware, software, and database procedures, but it is not comprehensive. There are procedures in place in case of loss of automation capabilities.

Records—Non-System Records:

Some MHFA data comes from a federal database at the Department of Housing and Urban Development, and the system verifies the identity of the sender and the source system. System software automatically verifies the integrity of the source and is able to detect errors in transmission and informational content.

Arrival time of data from non-system sources is considered to be the same as the creation time. There is no mechanism in place to detect changes from the time a record was created in the source system to the time that it arrives at MHFA. Staff considered this too cumbersome to administer and not cost-effective.

There is no virus detection for non-system data. However, a virus may be the cause for wrong, missing, and invalid formats, and the system detects these anomalies and will not accept the data.

Records—Transactional Data:

For MHFA's purposes, record content is important, record format and structure are not. The criteria and related considerations suggested imaging to them, which MHFA will not be undertaking.

The agency felt that all of the associated metadata prescribed for each record was worth considering, to some extent. For example, for each record, the date and time of receipt are considered the date and time of creation; these are not separate pieces of metadata. MHFA does not keep metadata on record format. The location of the records is essentially indexing metadata that indicates on which drive the record is stored. Metadata for the protection method exists, depending on the degree to which security is an issue for a particular record. MHFA staff will be considering how to determine indication of the authoritative version of a record and who has the authoritative version of the record.

The agency has had difficulty with assigning unique identifiers to each record. Though it has tried to enforce this, different and multiple identifiers get assigned by program staff for various reasons.

Appendix F, Section 5
Transactional System: Transition to a Different Platform

Agency:
City of Minneapolis

TIS Evaluation Meetings:
February through May 1999

State Archives Staff:
Mary Klauda, Shawn Rounds

Minneapolis Staff:
Sandra Allshouse, Caroline Bachun, Marsha Haagenson, Shirley Janssen, Merry Keefe, Mary Pedersen, Myron Rademacher, Carol Rogers, Bert Sletten, Craig Steiner, Linda Webster

System Name:
Human Resource Information System (HRIS) based upon PeopleSoft software

System Development Phase:
Analysis

Summary of TIS Evaluation Work:
The State Archives (SA) began collaborating with city of Minneapolis staff in February 1999 on the "authentication" (i.e., establishing the trustworthiness) of a new Human Resource Information System (HRIS) under development at that time. The HRIS Authentication Team included the HRIS administrator, the city clerk, the city records manager, a records management consultant, an assistant city attorney, and department representatives from Human Resources, Benefits, Payroll, Inspections, and Information Technology.

As a first work item, the group formalized a project rationale and developed initial team objectives (appended to this report). Several driving issues were identified, including the problem of duplicate records, difficulties in identifying the Office of Record and official records, lack of paper documentation of certain transactions, and questions as to the trustworthiness and acceptance of HRIS electronic records. Team objectives fell into two main areas: establishment of the trustworthiness of the HRIS with respect to team-determined levels of risk, and the development of a model for future authentication projects, including mechanisms for oversight, approval, and continued audits. Meeting these objectives, the group anticipated, would not only help to ensure the integrity of the city's electronic records, but would also begin paving the way for the acceptance of the city's electronic records in legal and audit situations. Furthermore, establishing a framework for future authentication projects and then following through with consistent application would have the broad effect of boosting user confidence in the city's computer systems.

The team asked for assistance in applying the criteria for trustworthy information systems developed by the SA. To this end, SA staff members attended several team meetings, leading members through the criteria on an item-by-item basis, and asking whether each was relevant, already in place, or planned for future inclusion. Responses were recorded in chart form and shared with group members to elicit feedback and facilitate the HRIS development and authentication process.

During the early team meetings, the issue of whether and how risk should be included in the process was discussed. All members agreed that it was important to consider the potential exposure that the city could face if a computer system and the records it produces are considered untrustworthy. The group created and analyzed several risk models prior to selecting one for use.

The initial risk model proposed utilized a high-level decision-assessment process to determine the level of effort required to authenticate a system. The first step of the decision process questions whether the system is unique. If the system is unique, it receives the strictest examination. If the system is not unique and not used by others as trustworthy, it receives slightly less rigorous scrutiny. If it is not unique and is used by others as trustworthy, then it undergoes the least examination. The team created a preliminary model of the decision process to test the validity of the approach. Although they ultimately abandoned this model because non-uniqueness and usage are not true indicators of trustworthiness, the team acknowledged the usefulness of the exercise for raising important issues.

After review and discussion, the team decided to adopt a more complex and detailed approach to risk during the examination process. Tools were created to identify, document, and track decisions. The team began by altering the SA chart, first moving the broad considerations into a second, separate table. Then, the format of the main table was altered. Whereas the form was originally keyed to the criteria set, the team re-numbered the items so that each could be referred to by a unique identifier. Criteria deemed not applicable to the HRIS were removed and those remaining were grouped into the following categories: Documentation, Security, Audits and Audit Trails, Disaster Recovery Planning, Record Content and Metadata, and Records Management and Data Practices.

Columns were added for “Risk” and “Responsibility.” “Risk” was sub-divided into “Category” and “Level,” while “Responsibility” was broken down by “Human Resources,” “Benefits,” “Payroll,” “Information Technology,” and “Records Management.” The risk categories were: Health and Safety (associated with physical injury or property damage); Security/Sensitivity of Data (associated with exposure of private or confidential information); Legal Liability and Regulatory (associated with increase and loss of legal cases and violations of laws and/or regulations); Fiduciary Responsibility (associated with failing to meet responsibilities and obligations to employees, residents, and taxpayers); Financial (associated with direct and indirect financial loss).

The team undertook a two-pronged approach to risk assessment. First, members determined for what areas the system would be the system of record. In consultation with staff from the city’s Risk Management Unit, they then began identifying system-associated risks, liabilities, and special concerns with the understanding that unacceptably high levels of risk would demand further examination of the corresponding parts of the system. Next, team members looked at each of the criteria, assigned it a general risk area, and examined it with respect to the likelihood of the risk occurring given the present system controls. Criteria were assigned a “Low” categorization if it is unlikely that the risk would happen, “Medium” if the risk could conceivably occur in some circumstances, and “High” if the risk might occur.

Continuing the assessment process, for each criterion the group determined which functional area(s) was responsible for gathering and/or maintaining the necessary supporting documentation and providing a written summary to the team. Team members from each responsible area were then asked, for each applicable criterion, to describe how the criterion was already being met or to indicate how it would be within a given time-frame. A “Status” column was added to the criteria table to track progress over the period from June to September.

A sub-group was formed to evaluate the sufficiency of the responses and documentation provided by each functional area. After determining that it lacked the expertise to make such judgements, the sub-group created a self-warrantee procedure to document compliance. It was decided that, in the future, team members representing the functional areas of the system will be asked for their signatures acknowledging that they agree to meet the SA trustworthy information system criteria, and that they have created, or are maintaining, the proposed level of documentation with respect to foreseen risks. The signed self-warrantee forms will also be sent to the department heads responsible for the HRIS system. The HRIS team felt that this two-level sign-off appropriately puts the burden of determining sufficiency of documentation on the departments involved rather than on the group. The team hopes to develop a more formal review process for future projects.

As of October 1999, the HRIS project was still underway, with work being done on the final report, general records retention schedules, procedures manuals, etc. The team identified records (selected for low risk level) within the Payroll, Benefits, and Human Resources departments that they would like to eliminate in paper form. The city attorney will be requested to issue a written opinion that the electronic form of the records are adequate. Future issues for the group include digital signature technology and the use of signatures (e.g., determination of when they are actually necessary). As well, the examination process highlighted the need to develop procedures to validate the correctness of the information being entered into the system.

The HRIS team was generally pleased with the criteria, the process they developed, and the application of risk when evaluating systems, although the group felt that prior to applying the SA examination process to other systems, it would need to streamline the risk analysis process. After final review, they hope to implement the system examination process city-wide by making it a requirement at the earliest system development phase when Requests for Proposals are sent out to vendors.

HRIS Project Rationale

The rationale for addressing the authentication of the HRIS system is primarily based on issues identified in work products created during the development of the HR portion of the City General Records Retention Schedule and the HR File Conversion Project. The issues raised during these projects are typical of issues that exist in other computer and record systems in the city. The issues identified in the HR projects include:

1. The same records are maintained in multiple locations (Service File, Central HR File, Department Personnel Files, Supervisory Files, and HRIS system records—PeopleSoft).
2. The Office of Record or Official Record could not be identified.
3. Approximately 30% or more of the records in the personnel file are input documents to the HRIS system.
4. Some departments are adding records directly to the system without creating or maintaining a paper record of the transaction.
5. An effective plan for the retention and filing of HR records could not be designed without addressing whether the HRIS records could be designated as the official record for some or most transactions (thereby eliminating the need to maintain multiple copies of paper input documents).
6. Procedures did not exist to determine whether the HRIS system was a "trustworthy system." That being the case, records produced by the system could not be deemed reliable/trustworthy for legal/evidentiary and audit purposes.

Initial Team Objectives

1. Authenticate the HRIS system and the processes /procedures used to create records to ensure reliability, trustworthiness, and acceptance of electronic records in lieu of paper. Minnesota Historical Society—Trustworthy Systems: "With electronic records, the focus should be on the system; as the information itself does not exist independently of the system, the reliability of the information will be a function of the reliability of the system. From either a legal or operational perspective, the determination of the trustworthiness of the data or electronic records will necessarily focus on the trustworthiness of the hardware, software, and procedures that produce and make them legible."
2. Document rationale/justification and selection of criteria that will be used for HRIS system authentication.
3. Identify and document definitions relating to the acceptance or meeting of criteria. Typical terms to be defined might include:
    a. what is reasonable or practical acceptance
    b. what is low risk versus high risk, etc.
    c. additional terms to be added as identified
4. Identify and document specific legal/regulatory requirements or rules that may impact the designation of the official record.
5. Review and document the system, processes, and procedures used to create and maintain records (including procedures used to create, edit, and protect the records against alteration or corruption, data practices, etc.).
6. Develop and document a framework or model that can be used for future authentication efforts for other city computer systems. The framework will include procedures that can be

used to create and maintain systems that will produce records that will meet reasonable legal/evidentiary and audit standards.

7. Develop and document a framework to direct authentication oversight and approval, including the continued audit of systems that have been previously authenticated.

An anticipated outcome of the HRIS Authentication Project will be to clearly identify the official records of HRIS, the form of the record, and where the records should be maintained. The authentication of city computer systems (in general) will increase the confidence levels of users of city computer systems, help to ensure the integrity of city electronic records, and provide documentation and guidance regarding the acceptance of electronic records in lieu of paper records for legal proceedings and audit.

Appendix G:
Tools

Tools for Assisting in the Application of the Trustworthy Information Systems Criteria

- **Examination Form**
  This form was used by State Archives staff to record information from meetings with agencies conducted during the field test phase of the Trustworthy Information Systems project. In its Microsoft Word 2000 format, the cells in the form expand automatically to accommodate any amount of text, allowing the user great freedom to record the results of the examination process as it happens.

- **Legal Risk Analysis Tool**
  This tool is keyed to the data classifications in the Minnesota Government Data Practices Act and will assist you in analyzing your agency's or department's legal risk in the area of government records management. *The Legal Risk Analysis Tool is only available online at [http://www.mnhs.org/preserve/records/tis/tis.html]*

TRUSTWORTHY INFORMATION SYSTEMS EXAMINATION FORM

Agency: ____

Form Completed By: ____

Date: ____

System: ____

Stage of Development: ______________________________________

Description of System (including data models, etc.):

CRITERIA FOR TRUSTWORTHY INFORMATION SYSTEMS

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
What laws and/or regulations (state and federal apply to the data within your system?			
What are your industry's standards for system security?			
What are your industry's standards for data security?			
What areas/records might lawyers target?			
What areas/records might auditors target?			
What data falls under the Minnesota Government Data Practices Act?			
What data is of permanent/historical value to you? To others?			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
1. System administrators should maintain complete and current documentation of the entire system			
What is the system's unique identifier and/or common name?			
What is the agency and department(s) responsible for the system?			
What is the agency and department(s) responsible for applications?			
What is the name and contact information of the person(s) responsible for system administration?			
What is the name and contact information of the person(s) responsible for system security?			
Has a formal risk assessment of the system been completed? Date? Performed by? Methodology? Findings?			
Were design reviews and system test run prior to placing the system in production? Were the tests documented?			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
Is application software properly licensed for the number of copies in use?			
If connected to external systems lacking commensurate security measures, what mitigation procedures are in place?			
What other systems might records be migrated to?			
1. System documentation (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents			
1. Unique names and identifiers should remain the same over the lifetime of the units to allow tracking			
1. If system installed at more than one site, each site should be running only an appropriate, documented, up-to-date version of the authorized configuration			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
1. Audit trails of hardware and software changes should be maintained such that earlier versions of the system can be reproduced on-demand			
1. Process in place to ensure that no individual can make changes to the system without proper review and authorization			
1.A.1 System Documentation: hardware procurement			
1.A.1 System Documentation: hardware installation			
1.A.1 System Documentation: hardware modifications			
1.A.1 System Documentation: hardware maintenance			
1.A.1 System Documentation: use of only agency-authorized hardware			
1.A.2 System Documentation: software procurement			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
1.A.2 System Documentation: software installation			
1.A.2 System Documentation: software modification			
1.A.2 System Documentation: software maintenance			
1.A.2 System Documentation: use of only agency-authorized software			
1.A.3 System Documentation: communication networks procurement			
1.A.3 System Documentation: communication networks installation			
1.A.3 System Documentation: communication networks modifications			
1.A.3 System Documentation: communication networks maintenance			
1.A.4 System Documentation: interconnected systems (including the Internet) – list			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
1.A.4 System Documentation: interconnected systems – names and unique identifiers			
1.A.4 System Documentation: interconnected systems – owners			
1.A.4 System Documentation: interconnected systems – names and titles of authorizing personnel			
1.A.4 System Documentation: interconnected systems – dates of authorization			
1.A.4 System Documentation: interconnected systems – types of connections			
1.A.4 System Documentation: interconnected systems – indication of system of record			
1.A.4 System Documentation: interconnected systems – sensitivity levels			
1.A.4 System Documentation: interconnected systems – security mechanisms, security concerns, personnel rules of behavior			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
1.B.1 System Documentation: programming conventions and procedures			
1.B.2 System Documentation: development and testing procedures, including tools			
1.B.2 System Documentation: development and testing procedures – periodic functional tests should include anomalous as well as routine conditions and be documented such that they are repeatable			
1.B.3 System Documentation: applications and associated procedures for entering and accessing data			
1.B.3 System Documentation: applications and associated procedures for data modification			
1.B.3 System Documentation: applications and associated procedures for data duplication			
1.B.3 System Documentation: applications and associated procedures for data deletion			
1.B.3 System Documentation: applications and associated procedures for indexing techniques			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
1.B.3 System Documentation: applications and associated procedures for outputs			
1.B.4 System Documentation: identification of when records become official			
1.B.5 System Documentation: record formats and codes			
1.B.6 System Documentation: routine performance of system backups – appropriate labels			
1.B.6 System Documentation: routine performance of system back-ups – secure, off-line, off-site storage			
1.B.6 System Documentation: routine performance of system back-ups – periodic integrity tests			
1.B.7 System Documentation: routine performance of quality assurance and control checks (incl. audit trails)			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
1.B.7 System Documentation: routine performance of quality assurance and control checks – identification devices (e.g., security cards) periodically checked to ensure proper functioning and correctness of identifying information and system privilege levels			
1.B.7 System Documentation: routine performance of quality assurance and control checks – storage mediums undergo regular statistical sampling following established procedures outlining sampling methods, identification of data loss and corresponding causes, and the correction of identified problems			
1.B.8 System Documentation: migration of records to new systems and media as necessary, with all record components managed as a unit throughout transfer			
1.B.9 System Documentation: standard training for all users and personnel with access to equipment			
1.B.9 System Documentation: standard training – users should sign statements agreeing to terms of use			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
Who can invoke change mechanisms for object, process, and user security levels?			
Who (creator, current owner, system administrator, etc.) can grant access permission to an object after the object is created?			
Is there a help desk or group that offers advice and can respond to security incidents in a timely manner?			
Is system performance monitoring used to analyze system performance logs in real-time to look for availability problems, including active attacks and system and network slowdowns and crashes?			
List internal and external user groups and the types of data created and accessed.			
Have all positions been reviewed with respect to appropriate security levels?			
What are the procedures for the destruction of controlled-access hardcopies?			
How is information purged from the system?			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
How is resuse of hardware, software, and storage media prevented?			
2. System administrators should establish, document, and implement security measures			
2.A.1 System Security – User Authorization: user identification and access procedures should be established and documented			
2.A.1 System Security – User Authorization: users should be authenticated prior to being granted access			
2.A.2 System Security – User Authorization: unique identifier and password for each user			
2.A.2 System Security – User Authorization: identifiers and passwords not used more than once within a system			
2.A.2 System Security – User Authorization: use of access scripts with embedded passwords limited and controlled			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
2.A.2 System Security – User Authorization: upon successful log-in, users should be notified of date and of last successful log-in, location of last log-in, and each unsuccessful log-in attempt on user identifier since last successful entry			
2.A.2 System Security: where identification codes in human-readable form are too great a security liability, use of other forms such as encoded security cards or biometric-based devices			
2.A.3 System Security – User Authorization: password rules include minimum password length, expiration dates, and limited number of log-on attempts			
2.A.3 System Security – User Authorization: determination of what level and frequency of log-on error constitutes a misuse problem which, in turn, would trigger notification of security personnel			
2.A.4 System Security – User Authorization: users restricted to only level of access necessary to perform their job duties			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
2.A.5 System Security – User Authorization: permission to alter disposition/retention codes, and/or to create, modify, and delete records granted only to authorized users with proper clearance			
2.A.5 System Security – User Authorization: modification of record identifiers prohibited			
2.A.6 System Security – User Authorization: Access to private keys for digital signatures limited to authorized personnel			
2.A.7 System Security – User Authorization: maintenance of lists of all current and past authorized users along with their privileges and responsibilities			
2.A.7 System Security – User Authorization: current list of users reviewed on a regular schedule to ensure timely removal of authorizations for former employees, and adjustment of clearances for workers with new job duties			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
2.A.8 System Security – User Authorization: personnel duties and access restrictions arranged such that no individual with an interest in record content will be responsible for administering system security, quality controls, audits, or integrity-testing functions.			
2.A.8 System Security – User Authorization: No individual should have the ability to single-handedly compromise the system's security and operations			
2.B.1 Internal System Security: access to system documentation controlled and monitored			
2.B.2 Internal System Security: access to output and storage devices controlled and monitored			
2.B.3 Internal System Security: controls in place to ensure proper security levels of data when archiving, purging, or moving from system to system			
2.B.3 Internal System Security: controls in place for the transportation or mailing of media or printed output			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of hardware when no longer needed.			
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of software when no longer needed			
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of storage media when no longer needed			
2.B.4 Internal System Security: documentation of sanitization and secure disposal should include date, equipment identifiers, methods, personnel names			
2.B.5 Internal System Security - insecurity-detection mechanisms constantly monitoring the system			
2.B.5 Internal System Security: failsafes and processes to minimize the failure of primary security measures in place at all times			
2.B.6 Internal System Security: security procedures and rules reviewed on a routine basis to maintain currency			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
2.B.7 Internal System Security – Access: measures in place to guard system's physical security			
2.B.7 Internal System Security – Access: measures in place to guard system's physical security – access to rooms with terminals, servers, wiring, backup media			
2.B.7 Internal System Security – Access: measures in place to guard system's physical security – data interception			
2.B.7 Internal System Security – Access: measures in place to guard system's physical security – mobile/portable units such as laptops			
2.B.7 Internal System Security – Access: measures in place to guard system's physical security – structural integrity of building			
2.B.7 Internal System Security – Access: measures in place to guard system's physical security – fire safety			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
2.B.7 Internal System Security – Access: measures in place to guard system's physical security – supporting services such as electricity, heat, air conditioning, water, sewage, etc.			
2.B.8 Internal System Security: security administration personnel undergo training to ensure full understanding of the security system's operation			
2.C.1 External System Security: additional security measures employed in cases of remote access, especially through public telephone lines (e.g., input device checks, caller identification checks (phone caller identification), call backs, security cards)			
2.C.2 External System Security: for records originating outside of the system, the system should be capable of verifying their origin and integrity			
2.C.2 External System Security: non-system records – verification of sender or source			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
2.C.2 External System Security: non-system records – verification of the integrity, or detection of errors in the transmission or informational content of record			
2.C.2 External System Security: non-system records – detection of changes in the record since the time of its creation or the application of a digital signature			
2.C.2 External System Security: non-system records – detection of viruses or worms			
Who can access audit data?			
Who can alter audit data?			
Who can add audit data?			
Who can delete audit data?			
How can the audit logs be read?			
Who can read audit data?			
What tools are available to output audit information? What are the formats?			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	*In Place?* *Yes / No*	*Planned?* *Yes / No*	*Rationale / Notes*
Who can output audit information?			
What mechanisms are available to designate and change activities chosen for audit?			
Who is able to designate and change activities chosen for audit?			
How are audit logs protected?			
3. System administrators should establish audit trails that are maintained separately and independently from the operating system			
3.A Audit Trails: if audit trails are encoded to conserve space, the decode mechanism must always accompany the data			
3.A.1 Audit Trails – General Characteristics: audit trail software and mechanisms subject to strict access controls			
3.A.1 Audit Trails – General Characteristics: audit trail software and mechanisms protected from unauthorized modification			
3.A.1 Audit Trails – General Characteristics: audit trails protected from circumvention			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
3.A.2 Audit Trails – General Characteristics: audit trails backed up periodically onto removable media to ensure minimal data loss in case of system failure			
3.A.3 Audit Trails – General Characteristics: system automatically notifies system administrators when audit storage media nearing capacity. Response documented			
3.A.3 Audit Trails – General Characteristics: when storage media containing audit trail is physically removed from the system, the media should be physically secured as required by the highest sensitivity level of the data it holds			
3.B Audit Trails – System to track password Usage and Changes			
3.B Audit Trails – Password Usage and Changes: user identifier			
3.B Audit Trails – Password Usage and Changes: successful and unsuccessful log-ins			
3.B Audit Trails – Password Usage and Changes: use of password-changes procedures			

Criteria	***In Place?*** ***Yes / No***	***Planned?*** ***Yes / No***	***Rationale / Notes***
3.B Audit Trails – Password Usage and Changes: user ID lock-out record			
3.B Audit Trails – Password Usage and Changes: date of password use			
3.B Audit Trails – Password Usage and Changes: time of password use			
3.B Audit Trails – Password Usage and Changes: physical location of user			
3.C Audit Trails – Users: system in place to log and track users and their online actions			
3.C Audit Trails – Users: system in place to log and track users and their online actions – details of log-in (date, time, physical location, etc.)			
3.C Audit Trails – Users: system in place to log and track users and their online actions – creation of files/records			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
3.C Audit Trails – Users: system in place to log and track users and their online actions – accessed file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/security level, etc.)			
3.C Audit Trails – Users: system in place to log and track users and their online actions – accessed device identifiers			
3.C Audit Trails – Users: system in place to log and track users and their online actions – software use			
3.C Audit Trails – Users: system in place to log and track users and their online actions – production of printed output			
3.C Audit Trails – Users: system in place to log and track users and their online actions – overriding of human-readable output markings (including overwrite of sensitivity label markings and turning-off of labeling mechanisms) on printed output			
3.C Audit Trails – Users: system in place to log and track users and their online actions – output to storage devices			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
3.C Audit Trails – Users: users made aware that their use of computerized resources is traceable			
3.C Audit Trails – Users: users supplied with Tennessen Warning when collecting confidential. Private data by any means			
3.D Audit Trails: Logged for each record by audit trails: user identifier			
3.D Audit Trails: Logged for each record by audit trails: record identifier			
3.D Audit Trails: Logged for each record by audit trails: date			
3.D Audit Trails: Logged for each record by audit trails: time			
3.D Audit Trails: Logged for each record by audit trails: usage (e.g., creation, capture, retrieval, modification, deletion)			
4. System administrators should establish a comprehensive disaster recovery plan			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
4.A Disaster Plan: periodically reviewed for currency and tested for efficiency			
What are the current components of a complete or final record of the transaction?			
What are the minimal components necessary to provide evidence of the transaction? (if you went to court, what would be the minimum information you would need?)			
Are there any laws, regulations, or professional best practices that specify the structure (including medium, format, relationships) of the record of the transaction or any of its components?			
What information is necessary to interpret the contents of the record?			
During which agency business processes might you have to access this record?			
Who are the external secondary users of the record?			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place?*** ***Yes / No***	***Planned?*** ***Yes / No***	***Rationale / Notes***
What are the rules, laws, and regulations that restrict or open access to these records to external users?			
How will the record be reproduced to meet the needs of internal and external secondary users? What are the reproduction formats?			
Is there a mechanism in place to indicate sensitivity level on hardcopies? Who can enable/disable this function?			
What are your industry's standards for records retention?			
What is the records disposition plan?			
Who is responsible for authorizing the disposition of records?			
Who is responsible for changes to the records disposition plan?			
How does the system accommodate integration of records from other systems?			
Who can access metadata?			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
Who can alter metadata?			
Who can delete metadata?			
Who can add metadata?			
Does system automatically assign unique consecutive numbers and time-date stamps to the individual units of storage media as they are written to for the first time to prevent the addition of false units or the removal of legitimate ones from the storage series?			
Does the system automatically assign new identifiers to modified records?			
If the records are not individually authenticated, does the record series metadata include the name or title of the individual responsible for validating or confirming the data within the record series and for confirming that the particular series was produced in accordance with standard procedures?			
5. Each record should have an associated set of metadata.			
5.A. 1 Record metadata: agent			
5.A. 2 Record metadata: rights management			
5.A. 3 Record metadata: title			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
5.A. 4 Record metadata: subject			
5.A. 5 Record metadata: description			
5.A. 6 Record metadata: language			
5.A. 7 Record metadata: relation			
5.A. 8 Record metadata: coverage			
5.A. 9 Record metadata: function			
5.A. 10 Record metadata: date			
5.A. 11 Record metadata: type			
5.A. 12 Record metadata: aggregation level			
5.A. 13 Record metadata: format			
5.A. 14 Record metadata: record identifier			
5.A.15 Record metadata: management history			
5.A.16 Record metadata: use history			
5.A.17 Record metadata: preservation history			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place?*** ***Yes / No***	***Planned?*** ***Yes / No***	***Rationale / Notes***
5.A.18 Record metadata: location			
5.A.19 Record metadata: disposal			
5.A.20 Record metadata: mandate			
Data Warehouses: Do you gather extraction metadata?			
Data Warehouses: Do you cleanse the data?			
Data Warehouses: Do you document the cleansing procedure?			
Data Warehouses: Do you gather cleansing metadata?			
Data Warehouses: Do you transform the data?			
Data Warehouses: Do you document the transformation procedure?			
Data Warehouses: Do you gather transformation metadata?			
Data Warehouses: What metadata / documentation do you offer users?			

Agency / Department:
System:
Form Completed By:
Date:

Criteria	***In Place? Yes / No***	***Planned? Yes / No***	***Rationale / Notes***
Data Warehouses: Who can access metadata?			
Data Warehouses: Who can alter metadata?			
Data Warehouses: Who can delete metadata?			
Data Warehouses: Who can add metadata?			
Data Warehouses: What are the legal liabilities regarding data ownership and custodial responsibilities?			
Data Warehouses: Where do data custody responsibilities reside – with the source systems, the warehouse system, or both?			
Data Warehouses: Are there records retention schedules and policies for warehouse data?			
Data Warehouses: Is retention of warehouse data coordinated with retention of data in the source systems?			

Agency / Department:
System:
Form Completed By:
Date: