2501 Aerial Center Parkway, Suite 103, Morrisville, N.C.
877.997.7742 · www.pria.us

Electronic Recording Security Considerations

http://www.pria.us/Security_WG.htm

PRIA Copyright Notice, Disclaimer and End-User License
Version 1.1 November 2003 (the "PRIA License" or the "License")

Subject to this License, Licensor hereby grants any user of this document or software ("Licensee") a worldwide, royalty-free, irrevocable, perpetual, non-exclusive license to reproduce the Work in copies, to prepare proprietary derivative works based upon the Work, to distribute copies of the Work to the public by sale or other transfer of ownership, and to display the Work publicly.

If the Work is software published by PRIA as codes in source and binary form, the License includes the right for Licensee to distribute copies of, and use, the codes in source and binary forms, with or without modification.

Any distribution of copies of the Work, or of a derivative work based upon the Work, shall reproduce verbatim the above copyright notice, the entire text of this License and the entire disclaimer below under the following header: "This document includes works developed by PRIA and some of its contributors, subject to PRIA License, Version 1.1 November 2003 published at www.pria.us/license.htm or any subsequent applicable version of such License." Any software application developed by Licensee based upon the Work shall include the following notice in its end user documentation and in its codes: "This software product includes software or other works developed by PRIA and some of its contributors, subject to PRIA License, Version 1.1 November 2003 published at www.pria.us/license.htm or any subsequent applicable version of such License." Upon publication of a derivative work, Licensee shall inform PRIA of such publication and address to PRIA a copy of Licensee's derivative work and any relevant documentation.

"PRIA" is a trade name of the "Property Records Industry Association." No derivative work or altered versions of a Work by Licensee may be trademarked or labeled in reference to PRIA or any of its trademark(s) or service mark(s) without PRIA's prior written approval. No reference to PRIA or any of its trademarks by Licensee shall imply endorsement of Licensee's activities and products.

DISCLAIMER: THIS WORK IS PROVIDED "AS IS." PRIA, THE COPYRIGHT HOLDER, THE AUTHORS OF THIS WORK AND ANY STANDARD -SETTING BODY CONTRIBUTORS TO THIS WORK MAKE NO REPRESENTATIONS OR WARRANTIES (i) EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NONINFRINGEMENT; (ii) THAT THE CONTENTS OF SUCH WORK ARE FREE FROM ERROR OR SUITABLE FOR ANY PURPOSE; NOR THAT IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. IN NO EVENT WILL PRIA, THE COPYRIGHT HOLDER. ANY AUTHOR OF THIS WORK, OR THE STANDARD-SETTING BODY CONTRIBUTORS TO THIS WORK BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS WORK, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA ON YOUR INFORMATION HANDLING SYSTEM OR OTHERWISE, EVEN IF PRIA, THE COPYRIGHT HOLDER AND/OR ANY AUTHORS AND/OR ANY STANDARD-SETTING BODY CONTRIBUTORS TO THIS WORK ARE EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

1. Introduction

Throughout the electronic recording process documents and information are:

- collected (submitted)
- processed
- transferred
- stored
- disposed

Each of these critical areas in handling information presents issues that need to be addressed and resolved by submitters, delivery & receiving vendors and recording agencies to ensure that systems and information are being protected adequately and in accordance with applicable legislation.

Within each of these areas, organizations need to understand

- the applicable threats and vulnerabilities that can lead to loss or damage as a result of security breeches;
- the policies, procedures and technologies that can be implemented to protect against the security breeches; and
- in the event a breech does occur, the incident response plans that an organization can follow to mitigate the overall risk for the security breech.

The PRIA Security Workgroup also strongly recommends that property records industry institutions implement programs that educate employees on the importance of protecting personal information, and the important role that each employee has in performing his/her duties to ensure that documents and information are submitted (collected), processed, transferred, stored and disposed in a secure manner.

2. Purpose and Scope

Because security issues vary widely between organizations based on numerous factors, this document is not intended to provide a blanket analysis that can be utilized without further effort. Rather it is intended to provide guidance as to the types of issues that need to be considered as part of a comprehensive security analysis. It also attempts to provide a sample methodology that can be utilized by organizations as a self-assessment tool.

This document generally applies to issues relating to the processing of electronic documents. It does not attempt to address general courthouse security nor the security of physical records (i.e.: paper & microfilm) on file in a recording agency's office. Any references to physical security are generally limited to the security of areas and devices utilized when processing electronic records. While there is clearly some overlap between electronic recording systems which facilitate delivery of electronic documents and legacy land records management systems which are used to index documents for storage and retrieval, these recommendations are primarily focused on the electronic recording process.

Additionally this document is limited to securing the electronic recording process from the recording agency perspective. When addressing the security concerns of submitters this document does so from the vantage point of how those issues may impact a recording agency's operations.

3. Definitions

3.1. Basic Security Terms

Some basic security terms are used throughout this document and are defined as follows:

1. **Authentication** — Is the process of establishing confidence in user identities.[1]

   Trading partners must perform authentication to establish a degree of confidence in the identity with whom they are in communication. Trading partners must deploy a reliable mechanism to assert their identity as well as validate their partner's identity.

   Authentication can take many forms: login string, passwords, account numbers or digital certificates. Some forms are more secure than others. Account numbers or passwords that are clear-text strings and contain no embedded protection to provide privacy require confidentiality to be applied when they are used.

2. **Confidentiality** — Is reserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

   Confidentiality and privacy are often used synonymously. There are several methods to achieve privacy for information from strong access controls to encryption. For electronic recording transactions (data-in-motion) between trading partners, encryption is the preferred solution. As a general rule, private or sensitive data-in-motion should be encrypted, regardless of internal (enterprise) or external transports. Restated, any sensitive data that is transferred over public networks (e.g.::, internal eMail/IM) or stored in portable storage media (e.g.::, laptops, flash/USB drives) should be encrypted to protect it from unauthorized access or disclosure.

3. **Non-repudiation** — Can provide various levels of assurance to the sender of information that their message is delivered and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.[2]

   Historically, "repudiate" is a legal term for the ability to deny or reject validity or authority. In the world of eCommerce, the goal of non-repudiation is to prevent repudiation of valid transactions, which is critical to the success of eCommerce. The ability to prevent an entity from denying a particular act must be supported to ensure intent.

   Appropriate policies and procedures, along with the security principles of authentication and integrity are combined into a single principle. This helps to ensure the identity of the entity and integrity of the associated transaction, which provides evidence

[1] NIST SP 800-63
[2] NIST SP 800-53, Revision 1

against modification. A commonly used method for non-repudiation is XML digital signature.

4. **Integrity** — Involves guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

   Integrity comprises timely, accurate, complete, and consistent data. The information must not be manipulated in any way, either through electronic errors or human intention. Hashing functions and digital signatures are very common in many system applications to provide data integrity services. A strong hashing function ensures that data modification does not go undetected. Moreover, by digitally signing the hash value, one can ensure that the hash can be trusted.

5. **Authorization** — Or ***rights-based access control*** is the enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.[3]

   Access controls or authorization are based on rights granted between trading partners, therefore specific access control recommendations are outside the scope of this document. However, access control is an important component of any effective security regimen and should be carefully considered from the outset of any eRecording initiative.

3.2. Threats, Vulnerabilities and Risks

For the purposes of this paper, the following definitions are used for **threats, vulnerabilities and risks**:

3.2.1. Threat

Something that is the source for causing danger or harm. For example, a hacker is a threat to a company's computer system.

The following threats are identified in the risk assessment spreadsheet in Attachment A:

1. **Rogue Submitter** — An entity posing to be a legitimate submitter.
2. **Rogue Web Site** — A web site that poses to be a legitimate web site (i.e., a real on-line county recording system) for the purposes of collecting documents or information (e.g.::, phishing, pharming).
3. **Rogue Recording Entity** — An entity that poses to be a legitimate recording-related entity for the purposes of recording documents.
4. **Hacker** — An entity purposely attempting to gain unauthorized access to computer systems.

[3] www.utmb.edu/is/security/glossary.htm

5.	**Eavesdropper**	An entity that is capable of intercepting documents or information (without knowledge by the submitter or the recording agency) as it is collected by the recording agency from the submitter.
6.	**Denial of Service Attack**	An attack against a system that is designed to overload system capabilities so that legitimate services cannot be rendered until the attack is ended.
7.	**Internet-based Attack**	Worms, viruses, etc., that promulgate via the Internet and look to exploit vulnerabilities within computing networks and systems.
8.	**Insider Threat**	An employee, contractor, etc., that has internal access to organizational assets, and intends to leverage that access to perform unauthorized functions.
9.	**Uneducated Employee**	An employee (or contractor) who unknowingly performs unauthorized functions (e.g.::, emailing sensitive information over unprotected networks, screen prints of sensitive information), is susceptible to social engineering attacks that disclose sensitive information, or performs ill-advised functions due to lack of education (e.g.: poor development and testing practices, inappropriate use of documents and information in testing environments).
10.	**Un-trusted Applications**	Applications that perform functions they are not supposed to perform, or do not perform functions they are supposed to perform.
11.	**Catastrophic Events**	Unforeseen events (e.g.: natural disasters, major power outages) that cause operations to cease.

3.2.2. Vulnerabilitiy

Something that is susceptible to attack or harm. For example, an un-patched computer system is vulnerable to an attack by an Internet virus.

The following vulnerabilities are identified in the risk assessment spreadsheet in Attachment A:

1.	**Collecting Unnecessary Documents and Information**	A submitter that collects sensitive/non-public information that is not needed to support electronic recording functions or processes.
2.	**Transferring Unnecessary Sensitive Information**	A recording entity that transfers additional sensitive information that is not needed by the recipient entity.
3.	**Poor Authentication**	An inability for either the submitter or the recording entity to authenticate one another prior to executing on-line transactions.

4.	**Inadequate Network Security (Recording Entity Web Interface)**	Minimal or poor security at the web interface (e.g.: web server) that leads to exposure of documents or information as it is being collected by the submitter.
5.	**Inadequate Security (Submitter Computer)**	Minimal or poor security at the submitter's computer that leads to exposure of the submitter's document and information.
6.	**Insecure Transfer Methods**	Electronic (e.g.: Internet-based) and physical (e.g.: media) transfer methods that do not provide adequate protection of documents or information (e.g.: sensitive information is not encrypted while in transit).
7.	**Inadequate Event Logging**	Lack of event logging that can provide details on transaction history or support security incident monitoring capabilities.
8.	**Uneducated Requester/Submitter**	A requester/submitter employee who has little to no security knowledge with respect to participating in on-line transactions.
9.	**Uneducated Employee**	A staff member may fail to properly authenticate a package being received or may not properly secure their user id and password or may delete documents.
10.	**Super User**	A person with unlimited access privileges who can perform any and all operations on the computer.
11.	**Insecure Test Environment**	Test environments that use "live operational data" but have lax security capabilities compared to the operational environments.
12.	**Poor Disaster Recovery Plans and Capabilities**	Plans and capabilities that do not exist, or exist but are in such poor condition that an organization is unable to recover back to adequate operating state after a catastrophic event has occurred.
13.	**Non-Compliant Third Party Service Providers**	Recording-related entities that do not perform periodic security reviews or audits to understand the security posture of their organization.
14.	**Inadequate Physical Security**	Minimal or poor physical security to prevent unauthorized access to critical computing equipment.
15.	**Removable Media**	Media such as USB drives, PDAs, notebook computers, and other such devices that can store documents and information, and also be easily removed from the operational environment of the entity.
16.	**Stored Documents and Information in Unused Storage Devices**	Storage devices that are not in current use (e.g.: retired, being repaired/serviced, damaged) but contain sensitive information.

17.	**Improper Deletion or Destruction of Documents and Information**	Documents and information that are still resident within the system even after disposal procedures have been followed (e.g.: not wiping hard disks containing documents and information).

3.2.3. Risk

The undesired result (consequence) that occurs when a threat successfully attacks or exploits a vulnerability. For example, an Internet virus (threat) penetrates an un-patched computer system (vulnerability) and causes the computer system to disclose sensitive information in an unauthorized manner (risk). Risk is further defined as having two components: the likelihood that the consequence will occur, and the impact of the consequence.

3.3. Electronic Recording Process

3.3.1. Process

The following definitions are used in reference to the electronic recording process:

Collection/Submission	Collection/Submission is the initial gathering of documents and information by a submitter to support an electronic recording function or process. In other words, a settlement agent (e.g.: lawyer, title agent, escrow agent) is responsible for sending recording documents and information to a recording agency for the purpose of fulfilling the recording function (i.e., submission of a document for recording).
Processing	Processing of documents and information is a recorder's internal use of those elements, by its employee(s) or computing environment, to execute an electronic recording workflow activity. Processing includes electronic computer processing as well as human review of electronic documents and information. Processing is assumed to be performed within the boundaries of a recording or delivery entity, and within a local operational network.[4] If a high level function (e.g.: statewide eRecording portal) involves multiple entities working together to process documents and information, a B2B (business-to-business) transfer of documents and information is required to transfer documents and information to each recording entity. It is important to note this distinction between internal processing and B2B transfers because it helps a recording entity define boundaries for when documents and information exist within the recording entity, and when it does not, for the purpose of fulfilling an electronic recording function.

[4] Local operational network is a notational term. A recording entity needs to determine within its own working boundaries what constitutes a local operational network (e.g.: LAN, WAN) where *processing* occurs, vs. *transferring documents and information* to other operational networks (either internally within the organization or to other recording entities).

Transferring

Transferring of documents and information is the sending and receiving of documents and information between two governmental entities (e.g.:: recording agency & county treasurer or recording agency and state department of revenue)

Transferring is assumed to be performed after documents and information have been initially collected/submitted from the submitter, and in support of processing and storing documents and information. That is, transferring of documents and information is not considered a stand-alone function. It is performed as part of a general processing or storing function. Disposing of documents and information is considered to be a local matter within a recording entity; therefore, it is not necessary to transfer documents and information to another entity for the purpose of disposing them.

Storing

Storing of documents and information is the placement of documents and information into either temporary or long term containers. Temporary containers (e.g.: workflow applications) are used to support real-time execution of an electronic recording process or function. Long term containers (e.g.: eVault or archive) are used to support historical record keeping and maintenance of electronic recording transactions.

Storing documents and information is assumed to occur after some local processing of documents and information is complete. For example, documents and information can be stored temporarily as part of processing a recordable document from a submitter, stored long term in a local environment as part of an online repository of recorded documents and indices, and stored long term in a remote environment as part of an offline archive of recorded documents (e.g.: eVault). Note in this last example that the documents and information are transferred to the remote entity, processed by that remote entity, and then stored by that remote entity.

Disposing

Disposing documents and information are the deletion or discarding of documents and information that are no longer needed within an electronic recording process or function. Documents and information can be deleted or discarded from both temporary and long term containers.

Disposing may also include the destruction of physical media so that its former contents cannot be read or effectively reconstructed. Such physical destruction will likely be needed to ensure uncompromised elimination of sensitive data at the end of its lifecycle.

Disposal activities also need to consider and be performed in accordance with approved retention schedules established by various governing agencies. Technology implementations must be designed in keeping with applicable policy decisions that govern electronic records.

3.3.2. Participants

Defining the parties and roles played by various actors in an electronic recording transaction has been a long standing challenge to the industry. While electronic message exchanges typically occur between a submitter and receiver(s), the business transactions which comprise the electronic recording process frequently involves more than two parties. Clearly, the mortgage finance transaction involves numerous service providers.

Nomenclature and process varies from one jurisdiction to the next. Sometimes a person's understanding is shaped by the role they play and the place at which they begin their participation in the transaction. And there are numerous scenarios wherein a single entity performs multiple roles in a transaction.

The following is an attempt to break the electronic recording transaction into its basic components so that the reader can then determine which party is performing which function(s) within a specific electronic recording implementation. These components are intentionally broad and examples are provided to help the reader understand the application of the definitions provided.

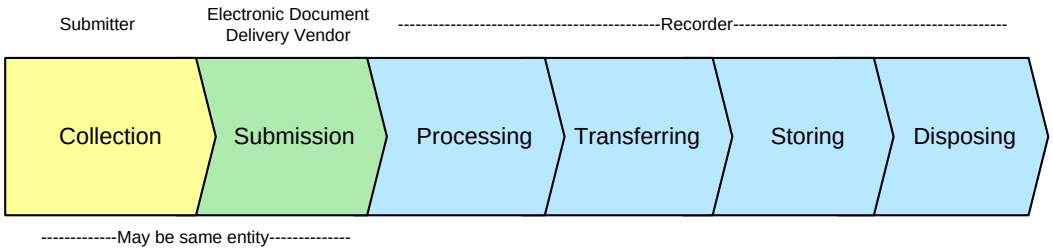
Submitter	The party who requests the document be recorded and has an interest in getting the documents recorded. This definition does not distinguish between the various steps and vendors that may be involved in pre-closing document preparation. It does not concern itself with variations on the closing event nor the agency relationship between a lender and a closing agent. While a closing agent may see itself as merely transmitting documents on behalf of a lender, the electronic recording process views them as one-and-the-same.
Delivery Vendor	A party who delivers the document to the Recording Agency or Receiving Vendor and returns the recorded document to the Submitter. This is the electronic equivalent of the USPS or other common carrier. Whoever gets the documents from the submitter to the electronic courthouse door is the Delivery Vendor. Some submitters have the capability to act as their own delivery vendor.
Receiving Vendor	A party who receives the document on behalf of the Recording Agency. This is the electronic equivalent of the courthouse mail room. This function may be performed by the Delivery Vendor or the Recording Agency's land records management system.
Recording Agency	The party who receives the document and processes it for recording (e.g.: county recorder, auditor, county clerk or clerk of the court).

A word about **portals**:

We often think of eRecording portals as having their primary relationship with Recording Agencies. In this understanding they play the role of the Receiving Vendor. In some instances they may also perform the Recording Agency function on behalf of a client county.

However, when the portal's primary relationship is with Submitters they are acting as a Delivery Vendor. Depending on county specific implementations they may or may not act as the Receiving Vendor as well.

4. Overview of the eRecording Process



4.1. Collection and Submission

The first step in the eRecording process is the collection of information that will be included in a recordable document. As a component of a real estate finance transaction, the eRecording process begins long before recordable documents are ready for submission to a recording entity. The lending process requires the gathering of a substantial amount of data regarding the parties to the transaction. While this information is critical to the lending process, very little of it is necessary for the recording process. In fact, inclusion of much of the information collected for the lending process posses potential privacy threats as part of the recording process.

The collection and maintenance of loan data is beyond the scope of this document. It is recommended however that Submitters and Delivery & Receiving Vendors exercise appropriate care when transferring data between trading partners prior to and as a part of the eRecording process.

4.2. Packaging and Delivery

Once the necessary information and images have been assembled and executed by the Submitter to create a recordable document, the Delivery Vendor will create an electronic package which is based on the PRIA eRecording XML standards and meets the requirements of the Recording Agency. This may include encoding of digital images, associating indexing data with scanned images, applying pre-determined business rules to check for recordability requirements, facilitating the payment of recording fees and other administrative functions relative to the recording process. Documents are then delivered to the Recording Agency.

4.3. Processing and Returning

Whether or not the Submitter and Delivery Vendor are the same party or are trading partners engaged in a service provider context, this document is focused on the collection and submission of data required to place a recordable document into the public record. Care should be exercised so as not to include data that is not required for the recording process in recordable electronic documents.

At the recording agency, electronic documents are reviewed for recordability. This may be an automated process, a manual process or combination of the two. Assuming the document(s) meets all applicable recordability requirements, unique recording information is associated with the document. The recorded document is then returned to the Delivery Vendor.

4.4. Transferring

Depending on the jurisdiction, additional functions may be performed on some documents. For example, deed or mortgage taxes that were collected at the time of recording may need to be transferred to another county agency or a state department of revenue. This requires the recording agency to transfer data outside of their processing system.

Whether or not a transfer of data to another agency occurs, electronic documents are stored in a land records management system. This usually includes managing indexing data and images of the documents.

Data and images that are the components of the land records management system should be archived in accordance with applicable state and local regulations and prudent industry recommendations. Multiple copies of back-up archives are recommended to be maintained in physically disparate locations so as to mitigate against the risk of loss through theft, tampering or natural catastrophes.

4.5. Disposing

While land records are usually regarded as permanent public records that are never disposed of and are intended for public consumption, some information that accompanies these records is neither permanent nor public. For example, payment account information may be included in the electronic delivery package. Care needs to be taken when disposing of this information to insure that it does not become available to unauthorized parties.

Additionally, proper care should be taken when disposing of the electronic storage media used to process and store electronic records. Simply deleting data does not necessarily eliminate it from being reconstructed via electronic forensic means. Physical destruction of the media may be an appropriate action to consider as a normal course of action.

5. eRecording Risk Categories

The PRIA Security Workgroup identified a number of threats, vulnerabilities and risks across the eRecording process (see attachment "A"). During this exercise, the following observations became evident:.

Threats Not surprisingly, threats that were most frequently rated with high combinations of likelihood and impact came from Internet based attacks and Insider threats. Thus, securing network assets and monitoring employee activities become obvious areas of attention.

Vulnerabilities Logically following, the vulnerabilities that ranked high for concern included Inadequate Network Security and Poor Authentication. Also high on the list were the Untrusted and Uneducated Employees.

Risks As a result, the following risk categories were identified as useful to organize similar and/or repetitive elements.

Unintended or Misuse of Access

This includes poor authentication, insider threats, insecure test environment, etc.

Introduction of Malicious Code or Software

This includes backdoor access, introduction of worms & viruses, etc.

Corruption of Data

This includes manipulation of data [intentional or inadvertent], receiving incorrect data, etc.

Recovery Issues

This includes poor back-up procedures, catastrophic events, etc.

6. eRecording Risk Ratings

The spreadsheet presented in attachment "A" is the result of the workgroup undertaking a generalized assessment effort. Along the way the workgroup realized that due to wide variations between counties in a number of critical areas that determine the level of risk presented by any given scenario, it is difficult to provide a blanket risk assessment that is appropriate for every recording agency. Thus it is recommended that the spreadsheet included as attachment "B" be utilized as a self-assessment tool to determine the specific level of risk faced by each agency.

The workgroup used a scale of 1 = low, 2 = medium and 3 = high to rate the likelihood and impact of the various combinations of threats, vulnerabilities and risks. The items that will be addressed in the mitigation recommendations presented in the following section are based on the generalized assessment presented in attachment "A". Your assessment may identify other areas that need to be addressed in your specific environment.

7. eRecording Risk Mitigation Recommendations

Because there is no single fool-proof system, security risks are most effectively mitigated by implementing multiple layers of various techniques. The examples that follow address the risks identified in Section 5. In isolation, any of these techniques can be thwarted. When implemented together as part of a comprehensive security program they can combine to provide a higher degree of protection.

7.1. Unintended or Misuse of Access

These risks stem from three key areas – poor authentication, insider threats and insecure test environments.

7.1.1. Authentication

Regarding authentication, it is recommended that strong authentication practices be implemented that define the acceptable identity credentials or account access information to be used by authorized individuals and can be used by system administrators to verify the identity of a user as one authorized to access the system. Examples of strong authentication would include, challenge questions and random one-time passwords in addition to user id & password combinations.

The use of multiple factors (2 or 3 factors in combination) is the preferred method of strong authentication. The banking ATM card is a good example of two factor authentication--1) the card - something you have, and 2) the Personal Identification Number (PIN)--something you know. Biometrics is the other authentication factor; however, it has some unique privacy and technology issues to overcome before it becomes more broadly accepted.

A hybrid method that has gained acceptance as a form of strong authentication is the use of a password in combination with other PINs/passwords (secret questions, selection of a favorite image, etc.). This method is not as strong as the use of multiple factors; however, its ease of implementation has gained adoption in many online financial and personally identifiable information based transaction environments.

7.1.2. Insider Threats

Regarding insider threats, two effective strategies include employee screening and network intelligence software.

As has been mentioned previously, the public nature of land records often leads organizations to mistakenly underestimate the sensitivity of the data surrounding these records and other systems that may be placed at risk from a malicious or careless insider. Payment account information is an obvious area of potential misuse. Alteration of a database, whether with the intent to change content and context or simply to vandalize, is another serious concern.

It is recommended that employee background screening be undertaken, minimally at the time of hiring or transfer to the recording office. Additionally, activity audits which highlight unusual and/or unauthorized patterns of conduct should be conducted on an on-going basis.

7.1.3. Insecure Test Environment

Another area of concern that was identified by the workgroup in this category was an insecure test environment. Test environments that are not properly established and maintained can provide access leading to various forms of attacks. Access controls, segregation of test systems from production systems and the use of sample data rather than live data are examples of procedures that should be implemented to reduce risks in this area.

While the documents associated with electronic recording are predominately public records and therefore do not pose a great concern if they are made available to "unauthorized parties" via an insecure test environment, security concerns need to be elevated when testing payment information or documents that contain other confidential information.

7.2. Introduction of Malicious Code or Software

There are a number of ways that malicious software can be introduced to a system. Often it can be a simple "social engineering" attack where an uneducated party is "tricked" into accepting a worm or virus while believing their actions are benign.

Another tool that can be useful in this regard is proper use of administrative control over software downloads and installation. Restricting the ability to download and install programs to system administrators reduces the likelihood of malicious code being introduced by unwitting users.

It is recommended that anti-virus and malware detection software be installed that can pro-actively identify such threats before they are accepted into a system. Since these threats are constantly evolving, it is vitally important to maintain current updates for detection software.

An additional recommendation is to utilize Transport Layer Security (TLS) or Secure Sockets Layer (SSL) technology for transactions with outside parties or transactions that involve sensitive information. These technologies are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet.

In an electronic recording environment there is usually the ability to filter incoming files by file type. Most recording agencies specify the acceptable file format(s) for their submissions. Filtering by file type (TIFF, PDF, etc vs. .exe) provides an opportunity for review of an unrecognized or potentially harmful file before it invades a system.

As was mentioned in regards to insecure test environments, the segregation of various systems (email, web access, eRecording , land records management, etc) can help reduce the impact of malicious code by slowing or preventing its spread to other systems in the event that such malware is introduced to a system.

7.3. Corruption of Data

This risk represents both the intentional manipulation of data as well as the accidental corruption of data due to storage media failure.

As was recommended previously in this document, access controls and activity audits can be deployed to combat the manipulation of data by unauthorized users. Limiting the number of parties who have the writeable access to data obviously reduces the risks in this area and monitoring the activity of authorized users can provide early detection of suspicious activities that could be detrimental to an organization.

Periodically scheduled quality assurance checking of back-ups and live data is recommended to help insure the reliability of storage media and the information stored on the media. Additionally, the use of encrypted hash values can provide a relatively low overhead means of checking data integrity.

7.4. Recovery Issues

Recommendations regarding a comprehensive disaster recovery plan are beyond the scope of this document but it is strongly recommended that a plan which identifies the assets of an organization, the location of those assets, the back-up and storage procedures utilized in regular operations and a future looking plan to restore normal operations in the event of a disaster be developed and periodically updated.

Another important aspect of a recovery plan is actually testing the plan before it is needed. This can be done on a limited scale in a test environment or on a full operational scale when deploying new systems. Testing a plan can reveal items overlooked or not adequately accounted for when drafting a written recovery plan before those oversights impact mission critical assets.

The PRIA Archive, Back-up and Disaster Recovery Workgroup is working on additional guidance for recording offices in this regard. Please refer to the Workgroup's website for additional details.

8. Conclusion

While the information contained in recordable documents is considered public information, the importance of security topics should not be neglected. Denial of service, nefarious alteration of the public record and access to non-public data held by recording agencies are all matters of serious concern.

As was stated at the outset, security issues vary from one organization to another based on a variety of factors. This document and the accompanying self-assessment tool are intended to provide a springboard to a broader consideration of security issues during the implementation of an electronic recording system. Depending on the resources available, it may be prudent to retain the services of a security consultant who can assist with a security analysis.

9. References

National Institute of Standards & Technology: "Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." (from the NIST website) http://www.nist.gov/