Florida Courts Technology Commission Report

to the

Supreme Court of Florida

regarding

Court Technology Continuity and Disaster Recovery Planning

December 23,2002

TABLE OF CONTENTS

APPENDICES

I. BACKGROUND

On October **25,** 2002 the Florida Courts Technology Commission convened and acted upon several critical issues in a manner which will play a vital role in the Judicial Branch over the next several years. The Commission, in addition to adopting a Judicial Information Strategic Plan, considered the need to ensure the security of information and systems critical to court operations.

The issue of securing court information came before the Commission as a result of a request by the Supreme Court to consider several recommendations of the Court's Work Group on Emergency Preparedness. The Work Group was directed by the Court to develop recommendations that would ensure the safety of court employees and visitors while allowing the state's courthouse doors to remain open during emergencies. The final report submitted to the Court by the Work Group contained several recommendations related to technology. Noting this, the Court referred the final Emergency Preparedness Report to the Florida Courts Technology Commission for consideration.

Specifically, the Court has asked the Commission to report on the feasibility and advisability of the Work Group's technology recommendations and to include a fiscal impact analysis and proposed implementation timetable for the recommendations. The Court further requested that the Commission report back no later than December **3**1,2002.

There were twenty-three recommendations in the Emergency Preparedness Report that were referred to the Commission for consideration. The Commission, after review and consideration, observed that, although all of the recommendations appear individually sound, many of them reach beyond the scope of keeping the state's courthouse doors open during times of emergency. A categorized listing of the recommendations referred to the Commission can be found in APPENDIX A of this report.

Thus, at its meeting on October 25,2002 the Commission concluded that the Emergency Preparedness Report identified and raised a much broader issue that should be addressed by the Commission and the Judicial Branch. That issue is the need to maintain the security of court information regardless of situations that may be classified as emergencies.

As a first step in fulfilling the objective of addressing court information security, the Commission established Court Information Security Committee ("CISC") with an overall charge of developing and recommending a comprehensive Information Security Program for the Judicial Branch.

Upon establishing the CISC, Commission appointed the following individuals to the Committee:

The Honorable Manuel Menendez, Jr., Chair
Circuit Judge, Thirteenth Judicial Circuit

The Honorable James R. Jorgenson
Judge, Third District Court of Appeal

Ms. Sharon Abrams, Court Technology Officer
Eleventh Judicial Circuit

Mr. Matt Benefiel, Trial Court Administrator
Ninth Judicial Circuit

Ms. Jannet Lewis, Court Technology Officer
Tenth Judicial Circuit

Mr. Jon Lin, Court Technology Officer
Fifth Judicial Circuit

The Honorable Barbara T. Scott
Clerk of the Circuit Court, Charlotte County

Mr. Grant Slayden, Trial Court Administrator
Second Judicial Circuit

The Honorable Cheryl Strickland
Clerk of the Circuit Court, St. Johns County

In addition to charging the CISC with developing and recommending a comprehensive Information Security Program for the Judicial Branch, the Commission instructed the CISC to ensure that its recommendations will integrate with the Judicial Information Strategic Plan that was approved by the Commission on October **25, 2002.**

In this regard, Initiative 8 of the Strategic Plan is most pertinent which reads as follows:

> " 5.2.8 Strategic Initiative 8 - Establish a plan for Information Security for trial courts in the context of the enterprise judicial information environment.
>
> The ability to access and share information from participating agencies through a judicial information environment introduces a need to plan for and implement appropriate security measures to ensure integrity, availability and confidentiality of information. This includes but is not limited to business continuity and disaster recovery processes.
>
> 5.2.8.1 Strategy 8a - Establish a Security Program for information under immediate control of the Court.
>
> 5.2.8.2 Strategy 8b - Evaluate programs in participating agencies to ensure adequate information security safeguards and controls are in place."

The CISC has been further instructed to consider the Judicial Branch functional and technical standards that were approved on October 25, 2002 by the Commission. These standards are contained within documents entitled "Functional Requirements" and "Integration and Interoperability" – both of which are supporting documents to the "Judicial Information Strategic Plan."

In order to provide the CISC with an appropriate timeframe in which to complete the critical task of developing a comprehensive Judicial Branch Information Security Program, the CISC has been requested to submit a report to the Commission for review prior to June 1, 2003. Upon the Commission's review of the CISC's report, it is anticipated that the Commission will submit to the Supreme Court a comprehensive set of recommendations related to the security of Judicial Branch information.

11. SUMMARY

As a single and specific objective within the much broader goal of developing a comprehensive Judicial Branch Information Security Program, the Florida Courts Technology Commission tasked its Court Information Security Committee to draft a response regarding the emergency preparedness recommendations that were referred to the Commission by the Supreme Court.

In referring the matter to the CISC, the Commission identified and approved six of the twenty-three recommendations in the Emergency Preparedness Report as directly and specifically relating to emergency preparedness. These recommendations were acknowledged by the Commission as recommended interim guidelines for Court Emergency Preparedness Plans.

Specifically, the six recommendations that were adopted by the Commission are as follows:

> "41(i). All courts and judicial branch entities should ... Develop and implement a document.disaster recovery plan to address information technology resources, and paper records, which will be reviewed and tested on an annual basis. The plan will include temporary manual procedures for operating without power and automated systems."
>
> "42. The chief judges of the districts and circuits and all judicial branch entities should implement methods to back **up** electronic information in a manner that will preserve the information, and allow for recovery and restoration of information."
>
> **"5** 1. The chief judges of the districts and circuits and all judicial branch entities should conduct a study regarding which records are stored in electronic format, paper format or both."

"52. Alternate technology and facility planning should be a part of the overall disaster recovery plan."

"53. In the event of extended power outages and inability to access automated systems; a temporary manual system may be necessary. In order to accomplish this **task,** chief judges of the districts and circuits must identify essential forms required to sustain court operations if electrical power or automated systems are unavailable."

"54. Each judicial branch entity responsible for judicial records should prepare a records recovery plan to establish specific procedures for personnel to follow in the event that an emergency or disaster occurs."

While the CISC was directed by the Commission to consider the remaining seventeen Emergency Preparedness Report technology recommendations in addressing its longer-term goal of developing an overall Judicial Branch Information Security Program, the CISC's immediate task has been to focus on assessing the feasibility, advisability, implementation schedule and fiscal impact associated with the six recommendations listed above. A list of all twenty-three recommendations referred by the Court, as categorized by the Commission can be found in APPENDIX **A.**

Also as directed by the Commission, the CISC considered several other relevant issues including whether there are additional emergency preparedness issues relating to technology that are not addressed in the Emergency Preparedness Report. In addition, the CISC's analysis and recommendations regarding emergency preparedness have been derived in such a manner as to ensure that they will fit within the ultimate work product of a recommended comprehensive court information security program. To achieve this objective, consideration has been given to

appropriate security measures aimed at preventing or minimizing the events that are disruptive to court information technology. Such security measures, which should ultimately be incorporated in a comprehensive information security program, and their interrelationships to tasks directly and specifically pertaining to emergency preparedness are listed in APPENDIX B.

Consideration has also been. given to ensure that the analysis and recommendations regarding emergency preparedness mesh with Security Standards contained within Integration and Interoperability Document approved by the FCTC. These specific standards are included as APPENDIX C. Further, the analysis and recommendations are aimed at laying out an effective and efficient planning method for technology continuity and disaster recovery by mapping to the "Functional Requirements Document" approved by the FCTC. This framework, which is recommended for use in identifying critical court functions and inventorying court records is included as APPENDIX D.

Finally, the proposed actions in this report are aimed at integrating and coinciding with the overall emergency planning efforts that are currently underway. To this end, draft court emergency preparedness reports are anticipated to be completed in March of 2003 by each district and circuit Court Emergency Management Group.

The overall results of the analyses shows value afforded by realizing statewide standards relating to court information technology that can only be achieved through a concerted effort of

many **players** and a common vision. To this end, recommendations to the Court can be found in the CONCLUSION of this report.

11. ANALYSIS and RECOMMENDATIONS

The following section lists the six recommendations of the Emergency Preparedness Report that are deemed pertinent, and provides analysis and recommendations as related to each recommendation's feasibility, advisability, proposed timetable and fiscal impact. As a general recommendation applicable to all of the recommendations in the Emergency Preparedness Report, there should be clarification provided for the term, "judicial branch entities." Specifically, many to these recommendations must be adhered to by entities outside of the courts as there are many independent constitutional officers that bear custodial responsibility for records required by the courts. Circuit Clerks of Court are the primary example, but are not the only entities outside of the courts proper that bear such responsibilities. The courts will need to work closely and in conjunction with Clerks of Court and other such entities to ensure its requirements for continuity of operations and disaster recovery can be met.

Analysis and recommendations regarding the six recommendations adopted by the Florida Courts Technology Commission are as follows:

A. Emergency Preparedness Report Recommendation 41(i)

> "All courts and judicial branch entities should **...** (i) Develop and implement a document disaster recovery plan to address information technology resources, and paper records, which will be reviewed and tested on an annual basis. The plan will include temporary manual procedures for operating without power and automated systems."

1. ***Feasibility:*** In order to develop a plan for recovering records, a study aimed at inventorying records must first be conducted (as suggested in Emergency Preparedness Report Recommendation 51 addressed later herein). An effective plan for disaster recovery cannot be developed without first understanding what information supports each critical court function, where that information resides, who has custodial responsibility for the information, in what format the information exists (paper or electronic) and what technology infrastructure houses and delivers the information (for information that is in electronic format). After first compiling the requisite inventory of information assets, a plan could be rather easily implemented and annually reviewed, tested *and updated* as necessary.

In developing these plans, it would generally be feasible to include temporary manual procedures as a contingency for records that are accessible via automated systems; however, there may be some instances in which manual contingencies are not sufficient. Instances in which manual procedures may not be feasible involve: a) an inability to institute fully operational manual procedures within the maximum acceptable restoration time and b) situations in which manual contingencies are not sustainable for the duration of a disruptive event. More importantly, there are some jurisdictions in which certain records reside in electronic format only and thus manual procedures may not be feasible. In these instances, a more appropriate approach may include alternate power and/or alternate equipment.

2. ***Advisability:*** Creating a document disaster recovery plan would be an important component of each court's overall emergency preparedness planning efforts, although focusing on the recovery of paper documents should not overshadow the need to recover critical information that may not be in a traditional "document" format. For example, information contained within an electronic court docket would be a high priority for recovery not only to provide crucial information on what cases must be acted on first (in the wake of a disruptive event), but also due to the fact that docket entries would serve as a basis for recovering needed paper documents that were contained within the files of all active cases. In this regard, it is imperative that there be contingencies to recover a backup copy of critical electronic information via compatible alternate equipment in the event that the primary equipment is unavailable.

As to the consideration of contingencies entailing temporary manual procedures, this is highly advisable due to the cost associated with various contingency options. Generally, manual contingencies come at little or no cost while contingencies involving alternate technology infrastructure are quite costly. Regarding the review and testing of recovery plans, it is extremely important to ensure that recovery plans are not merely created and filed away. Without periodic review, testing, updating and dissemination of the plan, the resources expended on the creation of the plan will have been largely wasted.

*3. **Proposed Timetable:*** As suggested under "feasibility," a study aimed at inventorying records (i.e., the tasks alluded to in recommendation number **51** of the Emergency Preparedness Report) should first be accomplished before an effective document disaster recovery plan can reasonably be developed. Therefore, it is recommended that all courts develop **a** draft records recovery plan by March 31, 2003. This will allow for the requisite study to be conducted during the January-February timeframe that would then immediately thereafter be used during the February-March timeframe to develop the actual plan.

4. ***Fiscal Impact:*** At this time, it is difficult to ascertain with any level of accuracy the fiscal impact associated with implementing sufficient document disaster recovery plans; however, through an appropriate planning process as described in this report, **a** reasonably accurate fiscal impact can be derived. The key issue here is that the cost associated with recovery plans is directly dependent on the time standards and prioritization that are established for recovering any given court function. The process of establishing such requirements will be set in the early part of the planning process, which should then be used to develop plans and assess the fiscal impact associated with implementing those plans.

One can reasonably assume that the fiscal impact will be small, if attention is given to selecting the most cost-effective contingencies. In this regard, there are a three factors

that should be noted: 1) it is suggested that existing personnel within the courts and other judicial branch entities will develop, implement and maintain recovery plans, but not without workload implications. **2)** there is a chance that manual contingencies will not always be the most cost effective option, particularly for high-volume functions affecting public safety 3) offsite storage of duplicate documents for active cases may be required and can be quite costly dependent on the format of the information (i.e., paper or electronic).

Of course, the fiscal impact of recovery plans should be minimized while ensuring the ability to prevent critical court functions from being disrupted for too long a period. One difficulty here is how to define what is "too long a period" for any given court function. Once this definition is established, the most cost effective recovery plan should be developed and implemented to meet the standard set regarding maximum acceptable disruption time. The main issue here is that in catastrophic situations in which electronic information is lost, the equipment housing the information is also lost. Under such scenarios, a backup copy of electronic data is useless if there is no compatible equipment available onto which the backup copy can be restored and accessed.

In consideration of these issues, it is apparent that the most cost effective recovery plans for court records will be those which take advantage of standardization between and among different courts. An increase in standardization will naturally result in less costly

and more effective recovery plans. The appellate courts offer the best example of how standardized systems result in highly cost effective recovery plans. Namely, each appellate court has nearly identical technology which in turn can be leveraged in their respective disaster recover plans through reciprocal arrangements. Through this approach, one appellate court's backup copy of electronic information can be restored and made available via another appellate court's technology infrastructure – obviating the need for acquiring and maintaining alternate equipment. This model should be pursued in the trial courts wherever possible in order to satisfy recovery requirements while minimizing the significant fiscal impact associated with maintaining spare equipment that would be utilized only in the event of a catastrophic loss. This would be accomplished through two efforts: 1) in the short-term, identifying where compatibilities exist between different trial courts and establishing reciprocal arrangements for disaster recovery and 2) in the long-term, achieving increased standardization of information technology throughout the state's trial courts.

To aid in identifying opportunities for reciprocal arrangements in the trial courts, the result of the recent technology infrastructure survey could be used. The infrastructure survey results will provide information regarding interoperability and compatibility between various trial courts.

B. Emergency Preparedness Report Recommendation 42

"The chief judges of the districts and circuits and all judicial branch entities should implement methods to back up electronic information in a manner that will preserve the information, and allow for recovery and restoration of information."

1. ***Feasibility:*** This recommendation is highly feasible in large part because it is reasonable to assume that court and judicial branch entities generally have in place effective methods for backing up electronic information. There is arguably no procedure in the field of information technology more critical than backing up data. Less common yet equally important are adequate measures to ensure the successful recovery and effective restoration of electronic information.

The primary factors that can impede the recovery and restoration of information are easily remedied by regularly taking backup data to a secure, remote storage location and by periodically testing the restoration of electronic information. In addition, it is crucial to ensure that the right information is being backed up. These measures are also highly feasible, although may not be fully implemented in all jurisdictions.

Most questionable regarding the recovery and restoration measures, is the ability to recover and restore electronic information after a catastrophic event that entails the loss of both the primary copy of information as well as the equipment that houses it. **As** indicated previously in this report, recovery and restoration can oftentimes be dependent upon whether compatible alternate equipment is in place – a measure that

can be costly if inter-court technology standardization is not sufficient to support feasible reciprocal arrangements between courts.

2. ***Advisability:*** With regards to information technology in the courts, there is no task more important than ensuring effective methods for backing up, recovering and restoring critical information.

3. ***Proposed Timetable;*** All court and judicial branch entities should take immediate action to ensure compliance with these recommendations. No later than March 31, 2003, critical court information that is stored electronically should be verified as having in place effective backup methods that are complete and consist of, at a minimum, regular remote storage and periodic restoration testing. Also by March 31, the opportunity for reciprocal arrangements should be identified in order to increase cost effectiveness in addressing alternative equipment contingencies.

4. ***Fiscal Impact:*** Since it is assumed that due care is being practiced by all entities bearing custodial responsibilities for court records, by backing up those records which are in electronic format, the impact associated with doing so should be deemed negligible. The only potentially significant fiscal impact associated with this recommendation involves providing for alternative equipment upon which backup data can be restored. It is important to note; however, that such fiscal impact will

decrease over time as trial courts statewide move towards a greater level of technology standardization and interoperability (as advocated by the Florida Courts Technology Commission through its Judicial Information Strategic Plan).

C. Emergency Preparedness Report Recommendation 51

"The chief judges of the districts and circuits and all judicial branch entities should conduct a study regarding which records are stored in electronic format, paper format .or both."

1. ***Feasibility:*** Without appropriate direction, conducting such a study could prove to be daunting and less-than-worthwhile. In order for this task to be achievable, it should be undertaken with the specific goal of creating an inventory of records required to support critical court functions. Considering records beyond those that are required to support critical court functions may result in a task that **is** too burdensome to be effectively completed. Further, in order for the study to be worthwhile, the result should be an inventory that includes: record type, court function(s) requiring the record, format(s) in which the record is stored, location(s) the record is stored, primary custodian of the record and method of accessing the record in order to fulfill critical court work. **As** an aid in completing this inventory in the trial courts, it is strongly suggested that the Functional Requirements Document approved by the Commission be used as a framework (see APPENDIX D).

*2. **Advisability:*** Conducting a study of records, as described above, is not only an essential task to be performed, but it is recommended as a critical first step in the process of developing effective continuity and recovery plans for court information.

*3. **Proposed Timetable:*** It is suggested that an inventory of critical court records be completed in February of 2003 so that it can be used in developing continuity and recovery plans that would in turn be incorporated into draft court emergency preparedness plans by March 31,2003.

4. ***Fiscal Impact:*** The impact associated with conducting a records study as described would be minimal, short of moderate workload implications on existing court personnel.

D. Emergency Preparedness Report Recommendation 52

"Alternate technology and facility planning should be a part of the overall disaster recovery plan."

1. ***Feasibility:*** Due to a lack of specificity, this recommendation is feasible at face value but may be highly infeasible if interpreted in an extreme fashion. What is needed is further guidance regarding the instances in which alternate technology and facilities would be deemed necessary components of a disaster recovery plan. As described previously herein, this issue relates the cost associated ensuring the

availability of alternate computing equipment that would provide sufficient compatibility for restoring backup copies of critical electronic information.

Continuity and disaster recovery planning as pertaining to technology, like all other areas of information security, is based on risk management fundamentals. In this regard, it is important to understand the basic method for effectively managing risk. Risk is derived by assessing factors such asset value and the probability of losing assets. Controls to mitigate risk are then selected through a cost-benefit analysis that compares the derived level of risk to the cost of applicable safeguards. This is pertinent to disaster recovery plans because the benefit received from alternate technology cannot often justify its cost. Therefore, it is suggested that alternate technology is only necessary as a component of a court disaster preparedness plan when manual procedures are insufficient in meeting critical court restoration requirements.

2. ***Advisability:*** It is advisable to include alternate technology as a part of a courts overall disaster recovery plan only under circumstances in which it is impossible to implement adequate manual procedures that can be fully operational within the maximum tolerable restoration time or under circumstances in which manual contingencies are not sustainable for the duration of a disruptive event. Due to the

cost, alternate technologies need not be utilized if manual processes are sufficient and cost-effective contingencies.

*3. **Proposed Timetable:*** A component of the overall emergency planning process is to identify the critical court functions, prioritize them and assign a maximum acceptable time for resumption. This task must first be completed before any reasonable effort can be made in identifying a need for alternate technology (in lieu of manual contingencies). Since it is anticipated that courts will have identified this prioritization in the draft plans by March 31 of 2003, it **is** suggested that necessary contingencies involving alternate technology be identified and added to each court's disaster recovery plan in April of 2003.

4. ***Fiscal Impact:*** There is a possibility for significant fiscal impact, which will be determined in the Spring of **2003.**

E. Emergency Preparedness Report Recommendation 53

"In the event of extended power outages and inability to access automated systems; a temporary manual system may be necessary. In order to accomplish this task, chief judges of the districts and circuits must identify essential forms required to sustain court operations if electrical power or automated systems are unavailable."

1. ***Feasibility:*** There is a slight possibility of isolated situations wherein a temporary manual system may not be feasible. This situation would be due to either an inability

for a manual system to be made fully operational within the maximum tolerable downtime of the automated system or an inability to sustain a manual system for the entire time the automated system is unavailable. If such situations exist, continuity plans should include fail-over and/or redundant power and technology infrastructure.

With respect to the need to identify essential forms required to sustain court operations, it is recommended that a single set of standardized forms be developed for statewide use. This will serve to ensure that all jurisdictions are capable of meeting the same minimum standard for continuity and recovery. It further would aid in the long term objective of standardized systems as described previously herein.

2. Advisability: For reasons indicated previously herein, contingencies that entail manual systems are strongly suggested.

3. Proposed Timetable: Manual systems necessary to support critical court functions in the event of an automated system disruption should be described and included in draft court emergency preparedness reports by March 31 of 2003.

4. *Fiscal Impact:* The fiscal impact of identifying and documenting necessary manual systems will be minimal, short of a moderate workload impact on existing personnel of the courts and other judicial branch entities.

F. Emergency Preparedness Report Recommendation 54

"Each judicial branch entity responsible for judicial records should prepare a records recovery plan to establish specific procedures for personnel to follow in the event that an emergency or disaster occurs."

1. ***Feasibility:*** Specific procedures for recovering records should be developed; however, this should be in accordance with the recovery plans developed per the many pertinent recommendations described in this report. In this regard, it should be noted that, as per the recommendations in the overall Emergency Preparedness Report, procedures relating to continuity and disaster recovery for information technology should address both response as well as recovery – which is best fulfilled by separating these two tasks.

2. Advisability: Procedures should be established in support of recovering all records, but with an emphasis on quickly recovering records required to fulfill critical court functions in priority order.

3. Proposed Timetable: Specific procedures, such as those addressing records recovering should be established immediately after the governing continuity and disaster recovery plans have been drafted, thus such procedures should be finalized and communicated to personnel prior to July 1, 2003.

4. ***Fiscal Impact:*** The fiscal impact of establishing records recovery procedures will be minimal.

IV. CONCLUSION

In light of the issues described in the preceding "ANALYSIS and RECOMMENDATIONS" section of this report, the following recommendations are respectfully submitted for the Court's consideration:

A. The Supreme Court should adopt Recommendations 41(i), 42, 51, 52, 53 and 54 of the Emergency Preparedness Report as generally feasible and advisable, but with the additional guidance and clarification contained within this report.

B. It is respectfully suggested to the Supreme Court that the fiscal impact associated with implementing these recommendations cannot be reasonably assessed until after the proper planning process is undertaken. In this regard, it is recommended that the planning process described herein take place statewide by March 31, 2003. This timeframe coincides with the broader emergency preparedness planning that is currently underway. Immediately thereafter, a reasonable fiscal impact assessment relative to technology can be accomplished.

C. The Supreme Court should establish statewide standards regarding the maximum period of interruption of each critical court function throughout the state. Doing so would serve well to ensure that public safety and court accessibility is no more threatened in one jurisdiction than in another. The Court could consider this issue in April of 2003 upon having reviewed and aggregate of draft emergency preparedness plans from throughout the state.

D. In order to minimize the long-term fiscal impact associated with information technology continuity and disaster recovery, the Supreme Court should support, at every opportunity, statewide court information technology standardization as described in the Florida Court Technology Commission's Judicial Information Strategic Plan. Further, because disaster recovery requirements are much more effectively met in a paperless environment, the Supreme Court should support, at every opportunity, relevant technology initiatives such as document imaging and electronic filing.

E. For each County and Circuit Court, the Court Administrator should complete the planning process described in APPENDIX E of this report. These tasks should be performed at the direction of each Circuit Chief Judge and in close conjunction with custodial entities such as the Clerks of Court. A similar process should be completed in the Appellate Courts at the direction of the Appellate Court Technology Committee.

F. For court continuity and disaster recovery requirements in which the custodian is not the court (as identified through the planning process described in APPENDIX E), the use of Service Level Agreements between the court and the custodial entity should be utilized. For example, agreements between Circuit Clerk of Courts and Chief Judges should by executed by way of memoranda of understanding indicating the Clerk has continuity and disaster

recovery measures in place capable of fulfilling the court's requirements related to maximum acceptable interruption time in the event of a disruptive event.

***G*. A** single, comprehensive set of uniform forms should be developed for statewide use in fulfilling mission essential court functions in the event of a disruptive emergency requiring such contingencies be executed. This effort could provide many benefits beyond merely achieving a standardized component of emergency preparedness plans. It is the natural next step to follow the Technology Commission having documented statewide court functional requirements.

In closing, the Florida Courts Technology Commission and its Court Information Security Committee looks forward to the Court's action in response to this report. There is much to be done in support of fulfilling court information technology needs and securing court information such that the Branch can most effectively serve the citizens of Florida.

APPENDIX A

Emergency Preparedness Report Recommendations (41(a) - 41(i), 42, 44 - 56)

Technology Recommendations that Directly and Specifically Pertain to Disaster Preparedness and/or Continuity of Court Operations

"41. All courts and judicial branch entities should:

...

(i) Develop and implement a document disaster recovery plan to address information technology resources, and paper records, which will be reviewed and tested on an annual basis. The plan will include temporary manual procedures for operating without power and automated systems."

"42. The chief judges of the districts and circuits and all judicial branch entities should implement methods to back up electronic information in a manner that will preserve the information, and allow for recovery and restoration of information."

"51. The chief judges of the districts and circuits and all judicial branch entities should conduct a study regarding which records are stored in electronic format, paper format or both."

"52. Alternate technology and facility planning should be a part of the overall disaster recovery plan."

"53. In the event of extended power outages and inability to access automated systems; a temporary manual system may be necessary. In order to accomplish this task, chief judges of the districts and circuits must identify essential forms required to sustain court operations if electrical power or automated systems are unavailable."

"54. Each judicial branch entity responsible for judicial records should prepare a records recovery plan to establish specific procedures for personnel to follow in the event that an emergency or disaster occurs."

Technology Recommendations that Address General Information Security Issues but do not Directly or Specifically Pertain to Disaster Preparedness or Continuity Operations

"41. All courts and judicial branch entities should:

(a) Create an information technology **risk** assessment plan for each district, and circuit by county. **A** full assessment should be conducted, and then periodically updated on a regular basis. Frequency of update is based on the amount of change that occurs in the environment.

(b) Develop and implement a policy regarding the acceptable use of information technology.

(c) Develop a Security Awareness Program to educate users on their role in properly securing information technology.

(d) Implement local policies and measures to provide controlled access to information technology to ensure confidentiality, integrity and availability of information.

(e) Implement an antivirus program that ensures up to date virus definitions and virus scanning to prevent damage to court information technology, and prevent the propagation of viruses amongst justice related entities.

(f) Implement the appropriate measures to prevent unauthorized network access both from internal and external sources to preserve confidentiality, integrity and availability of information.

(g) Implement the appropriate policies and safeguards to secure access to technology resources and paper records.

(h) Implement mechanisms to monitor potentially dangerous environmental conditions to prevent damage to technology resources and paper records."

"44. An Information Technology Security Manager (ITSM) should be the Court Technology Officer or their designee within each courts' technology staff as the designated contact to communicate information about threats to technology infrastructure and information systems."

"45. The collective statewide ITSM group should devise appropriate incident reporting measures and guidelines regarding how to investigate threats, provide

comprehensive vulnerability scans, provide methods for gathering intelligence and distributing early warnings regarding new and changing threats, and have methods to determine if a law enforcement investigation is required."

"46. New systems development and upgrades of existing systems should follow a formal systems methodology, which should include risk analysis and security architecture planning as part of the process."

"47. Security management practices such as cryptography should be implemented when necessary to ensure confidentiality and integrity of information."

"48. When the integrity, availability, and confidentiality of information on a distributed network are vital, structures and methods to authenticate and secure network transmissions should be put into place."

"49. Appropriate logging and accountability mechanisms should be in place, so security incidents can be identified, and forensics can be collected in the event legal action must be taken."

"50. Regular and frequent system vulnerability analyses should be conducted."

"55. The court should require that the Judicial Management Council conduct a statewide security assessment to ascertain the level of security planning that exists regarding judicial branch records and technologies."

Other Technology Recommendations

"56. The court should require that the Court Technology Commission review and recommend means through which all judicial branch records may be received and stored electronically within the next five years."

APPENDIX B

Potential Components of a Future Judicial Branch Information Security Program Relevant to Court Technology Continuity and Disaster Recovery Planning

Information Security Management Practices

Risk Analysis

Similar to business impact analyses performed for continuity and disaster recovery planning.

Security Awareness

Activities include circulation, training, testing and drills related to continuity and disaster recovery plans.

Information Security Policies, Standards, Guidelines and Procedures

Overall information security policy should include statement of importance and top-level support relating to all aspects of information security, including continuity and disaster planning. Supporting standards, guidelines and procedures should include those directly relating to continuity and disaster recovery.

Employment Practices

Safeguards such as employee background checks, termination procedures and key personnel continuity plans should preserve the integrity of information security safeguards including continuity and disaster recovery plans.

Physical Security

Building construction, facility monitoring, power supply redundancy/backup, fire detection/suppression and physical access controls reduce or prevent disruptive events addressed by continuity and disaster recovery plans.

Network Security

Redundancy and elimination of single-points-of failure in network infrastructure and telecommunications services can reduce the impact of disruptive events addressed by continuity and disaster recovery plans.

Operations Security

Controls involving the handling and labeling of storage media (including backup media) ensure effectiveness of continuity and disaster recovery plans.

Change Control and Configuration Management

Systems documentation ensures the effectiveness of continuity and disaster recovery plans.

APPENDIX C

"Security Standards" Excerpt from *Integration and Interoperability Document*

2.2.2 Security Standards

The system security should encompass many technical and non-technical areas. This section describes the comprehensive high-level technical security architecture strategy that should be addressed when defining system requirements.

The first step in defining the required security is to perform a risk assessment to determine the sensitivity of information, level of risk, and appropriate security investment for OSCA. The risk assessment should take into consideration both state and federal laws governing justice information.

Guidelines
The security infrastructure should employ a complete set of security components to satisfy the full spectrum of system security requirements that will range from access to public information to access to highly confidential data. The security infrastructure should provide for flexibility as new security policies are introduced into the environment.

The characteristics of security include:

- Authentication is the ability to restrict users by unique identification to the system. The system security should require a single point of authentication to all judicial systems, and provide minimally invasive access to all applications and data for authorized users. Authentication can be achieved through the use of digital certificates and a certificate authority **(CA)** hierarchy.

- A Directory Access Methodology should be identified and implemented that has wide vendor support. One recommendation to accomplish this goal is LDAP. LDAP is used extensively for holding system information, such as a corporate directory, and for support of Public-key Infrastructure (PKI). This includes a user, group and organization database, and a verification mechanism.

  Key aspects of LDAP are:

  - Protocol elements are carried directly over TCP/IP and thereby it has a rather simple protocol stack.
  - Many protocol data elements are encoded as ordinary strings (for example, Distinguished Names).

- It allows LDAP servers to cooperate by use of referrals, that is, one server can return back to the user referrals to other servers that might be able to serve the user request. (X.500 has the same capability in addition to being able to chain the request directly between servers).
- It requires UTF8 encoding of the ISO 10646 character set

- Access Control is the verification and enforcement of the user's authorized access to the computer network. It also includes the definition and control of read and write authorizations for documents as well as for network resources. Access controls or ACLs should define restrictions to access or modification of applications and data by group or by individual. ACLs are stored on each server to which they control access.

- Encryption is the coding or scrambling of information so that it can only be decoded and read by someone, or something (i.e. a server), which has the correct decoding key. All applications should encrypt data and encrypt/decrypt communication without user intervention.

- Firewalls/Proxy should be used to protect a networked server from damage. The firewall technology should support network-layer security — i.e., restrict by protocol, network access control lists (TCP/IP address filtering), and TCP/IP port. In addition, application level security should provide proxy access to the judicial servers. Proxy functionality limits external users from directly accessing data on the judicial information system servers.

Security Components

The technical architecture should unt for security in the ollowin areas:

- Network - Network security encompasses preventing unauthorized access to the LANs, MAN, and WAN that will be used to access judicial services. Network security should be an integral component of the system security architecture. It is recommended that the network be developed based on the TCP/IP protocol because of its ability to interact with heterogeneous systems. Although TCP/IP can offer extensive advantages to providing universal access to all system services, it also poses potential problems for restricting unauthorized user access. To help to mitigate this problem, it is recommended that firewall technology be deployed between the hub server, each judicial location, and the MAN/WAN. In addition, unauthorized users on county and local networks that are connected to the WAN should use a firewall to protect the courts network from access. All network devices — including hubs, routers, and other backbone technologies — should be physically secured. The goal is to provide clearly defined policies and procedures for network security management and monitoring in order to limit and manage exposure from the network.

- Client/Server - Client and server security policies should be defined and implemented to reduce the risk of exposure.

  - Client - Client security should address browser vulnerabilities from WEB applications that will be developed for execution on or by workstations. The two most widely deployed web browsers today are Netscape Navigator and Microsoft Internet Explorer. Both products have a history of known security holes. These holes typically are exploited via program changes made using popular web-based programming and scripting languages (such as Java, Java Script, ActiveX, and plug-ins). The respective vendors frequently release patches and updates to correct these problems, though new holes routinely are found. Browser and development policies should be developed and implemented to protect workstations from malicious programs.

  - Server (Web, E-mail, Directory etc.) - Servers are vulnerable to security breaches from several points.

    - Authentication to the judicial information system environment should be accomplished without sending clear-text passwords over the network. This can be accomplished with the use of digital certificates.
    - Sensitive data should be encrypted to restrict interception, playback and rewrite, or modification during the transmission process. This can be accomplished using 128 bit or above encryption technology.
    - Access should be implemented using a standards based approach.
    - As part of a complete security strategy for web, e-mail, and directory servers, each server should be managed using well-documented and clearly understood policies. Some technologies that can be used to secure these servers include, digital certificates, access control lists, and secure sockets and encryption. These technologies, combined with a strong universal security policy, will provide a robust security environment.

- Legacy Systems - Security should support both "pushing" and "pulling" information from agency legacy systems. The risk for a security breach will be even greater as judicial information system servers access information from the legacy systems or as users are accessing legacy systems in real-time. ***An*** audit should be performed on each legacy system that supplies information to the judicial information system environment. Potential risks should be addressed through the use of technology, policies, and procedures.

APPENDIX D

Court Functions Identified by the Florida Courts Technology Commission

This listing is recommended to be used as the framework for court technology continuity and disaster recovery planning. For additional clarification, the complete "Functional Requirements Document" should be referenced

Administrative Functions (e.g. procurement, payroll, etc.)

Crass-Divisional Processes

Case Initiation and Indexing
Docketing and Related Record Keeping
Schedule and Case Management
Ticklers & Alerts
Document Processing
Calendaring
Hearings
Disposition
Case Closure
Accounting
Audit Trail Management
File Archival and Destruction
Document Management
Exhibit Management
Statistical Reports
Management Reports

Criminal

Arrest & Intake Offender
File Formal Charges
Sentence Offender & Monitor Post-Sentence
Manage Post-Conviction Relief
Conduct Arraignment & Adjudication

Civil

File Claim, Discovery
Manage Small Claims Case
Evaluate Petition for Extraordinary Writ & Review
Manage County/Circuit Civil Case
Manage Appeal
Dispose/Close Case
Manage Jimmy Ryce Case

Juvenile (Dependency and Delinquency)

Dependency
Conduct Pre-Hearing Investigation
Determine Custody/Shelter
Prepare Dependency Petition/Conduct Filing Hearing
Conduct Arraignment & Pre-Disposition Hearings
Conduct Disposition and Judicial Reviews

Delinquency
Determine Custody/Detention
Conduct Arraignment
Manage Juvenile Diversion/PTI
Manage Juvenile Delinquency Case

Probate

Probate, Guardianship, and Mental/Medical Health

Traffic
UTC Intake & Administration (Clerk)
Manage Civil Traffic Infractions
Manage Criminal Traffic Violations
Generate Traffic Case Management Reports

Family

Domestic Relations
Case Review
Case Management Conference
Conduct Motion Hearing
Conduct Case Management Conference
Conduct Final Hearing

Domestic Violence, Repeat Violence, & Date Violence
Conduct Ex Parte Review of Petition
Conduct Evidentiary Hearing
Conduct Disposition Hearing

Drug Court
Manage Adult Diversion Program
Manage Post-Adjudication Drug Case
Manage Juvenile Drug Case

Jury & Witness

Jury Management Processes
Produce Pool of Eligible Jurors
Select Jury Venire
Conduct Voir Dire
Pay Jurors
*Prepare **OSCA** Reports*

Witness Management Processes
Subpoena Witness
Witness Appears
Pay Witness
Prepare OSCA Reports

APPENDIX E

Court Technology Continuity and Disaster Recovery Planning Template

This template is designed for use by each Circuit and District Court Administrator, in conjunction with Clerks and Technology Officers. The purpose of this template is to ensure adequate and uniform technology components of each circuit's Emergency Preparedness Plan. A technology continuity and disaster recovery assessment should be conducted for each county, circuit and district in accordance with this template. The results of each of these assessments should be submitted by the Court Administrator to the Court Emergency Management Group (CEMG) for inclusion in the overall Emergency Preparedness Plan. In addition, copies should be provided no later than March 31, 2003 to the Court Information Security Committee of the Florida Courts Technology Commission. The OSCA Information Systems Services Division will assist in conducting such assessments by providing standardized forms, automated collection of planning information, and guidance as required by the steps described in this template. The Court Information Security Committee will use the results of this process to identify fiscal and implementation concerns as requested by the Supreme Court.

Steps to follow in completing the Technology Continuity and Disaster Recovery Assessment and Plan for each County within each Circuit Court and in each Appellate Court:

1. List each mission essential court function. For each mission essential function, list the maximum tolerable disruption time and priority. This information will be compiled by, and obtained from, each CEMG.

2. For each mission essential court function, identify those that are fulfilled through the use of information technology (IT). For consistency and to aid in completing this step, the court functions and supporting processes as listed in APPENDIX D of the Florida Courts Technology Commission Report on Technology Continuity and Disaster Recovery should be used. IT that is used in fulfilling a mission essential court function may consist of one or more of the four IT infrastructure components:

   a) Workstations (PC's, printers and other peripherals)
   b) LAN (local area network cabling, switches, etc.)
   c) WAN (wide area network telecommunications services and equipment)
   d) Centralized Computing Equipment (mainframes, database servers, files servers, etc.)
   e) Audio Visual and Other Automated Systems (items not falling into the above categories)

3. For each mission essential court function dependent upon one or more of the IT infrastructure components listed in step 2 above, identify which infrastructure components are utilized and who the custodian is for each component. Custodian may be Court Administration, a Clerk of Court, a third-party service provider or other entity.

4. For each mission essential function, identify whether a manual contingency would be sufficient (as defined per step 1 above) in the event of a loss of one or more of the supporting IT infrastructure components (as identified in step **2** above).

5. If there are any mission essential court functions supported by IT infrastructure for which a manual contingency would not be sufficient, list the following for each of these court functions:

a) relevant process(es) involved,
b) IT infrastructure component(s) supporting the relevant process(es),
c) the custodian of each supporting IT infrastructure component,
d) summary of custodian continuity/disaster recovery plan(s),
e) whether continuity/disaster recovery plan(s) meet maximum disruption requirement

6. For any continuity/disaster recovery plans identified as not meeting maximum disruption requirements (per step **5** above), indicate the resources and time required to remedy the matter.