

TABLE OF CONTENTS

MENUBERS OF THE WORKSHOOM ON EVER SENSY PREPARED A	2
MEMBERS OF THE WORKGROUP ON EMERGENCY PREPAREDNESS	3
CHAIRMAN'S REMARKS	5
EXECUTIVE SUMMARY	6
SUMMARY OF RECOMMENDATIONS	9
PURPOSE	16
SCOPE	16
APPLICATION, IMPLEMENTATION, AND POLICY	16
SECTION I, EMERGENCY OPERATIONS	17
TASKS DISCUSSION GUIDELINES	17 19 21
SECTION II, PERSONNEL	29
TASKS DISCUSSION GUIDELINES	29 30 31
SECTION III, SAFEGUARDING RECORDS OF THE JUDICIAL BRANCH	37
TASKS DISCUSSION GUIDELINES	37 37 44

Workgroup on Emergency Preparedness

APPENDIX A, INSTRUCTIONS FOR PREPARATION OF ADMINISTRATIVE AND EMERGENCY PROCEDURES	54
APPENDIX B, OUTLINE AND SAMPLE OF CONTINUITY OF OPERATIONS PLAN (COOP)	56
APPENDIX C, THE EMERGENCY PREPAREDNESS PROCESS	87
APPENDIX D, IMPLEMENTATION PROCESS	88
APPENDIX E, EMPLOYEE PROFILE	89
APPENDIX F, EMERGENCY CONTACT INFORMATION LOG	90
APPENDIX G, FAMILY DISASTER PLAN	91
APPENDIX H, CRITICAL FORMS	102
APPENDIX I, EMERGENCY PREPAREDNESS SURVEY	107
GLOSSARY OF TERMS	121
ACRONYMS USED IN THIS REPORT	126

MEMBERS OF THE WORKGROUP ON EMERGENCY PREPAREDNESS

Mr. J. William Lockhart Circuit Court Administrator, Sixth Judicial Circuit Chairman

Ms. Jannet Lewis Court Technology Officer, Tenth Judicial Circuit Chairman, Subcommittee on Safeguarding Court Records

Mr. Tom Long Chief of General Services, Office of the State Courts Administrator Chairman, Subcommittee on Personnel

The Honorable Emerson Thompson Chief Judge, Fifth District Court of Appeal Chairman, Subcommittee on Mission Essential Functions

Mr. Mark Weinberg Circuit Court Administrator, Seventh Judicial Circuit Chairman, Subcommittee on Emergency Operations

Mr. James Birkhold Clerk of Court, Second District Court of Appeal

The Honorable Glenn Keith Cary Circuit Judge, Twentieth Circuit

Mr. Richard M. Cheek Community Program Administrator, Division of Emergency Management

The Honorable Richard F. Conrad Circuit Judge, Ninth Judic ial Circuit

Ms. Sandy Garcia Personnel Director, Eleventh Judicial Circuit

The Honorable Lydia Gardner Clerk of the Circuit Court, Orange County

Mr. Mike McHargue Director of Executive Leadership Center Florida Department of Law Enforcement The Honorable Manuel Menendez, Jr. Chief Judge, Thirteenth Judicial Circuit

Mr. Randy Napoli Bureau Chief of Fire Standards and Training State Fire Marshall

Mr. Glen Rubin Marshal, Fourth District Court of Appeal

Mr. Grant Slayden Circuit Court Administrator, Second Judicial Circuit

Lieutenant R. Scott Stiner Pinellas County Sheriff's Office

Mr. Robert Craig Waters Public Information Officer, Supreme Court of Florida

Staff to the Workgroup:

Mr. Greg Cowan
Office of the State Courts Administrator

Ms. Michelle Leshko Senior Deputy Court Administrator Sixth Judicial Circuit

Mr. Kenneth E. Nelson Court Technology Officer Sixth Judicial Circuit

CHAIRMAN'S REMARKS

Chief Justice Charles T. Wells in his charge to the workgroup said: "Keep the courts open."

Justice Wells' remark goes to the heart of the American democracy, for without open forums for the resolution of disputes, a society cannot sustain a free way of life for its citizens. This principle is found in article 1, section 21, of the Florida Constitution, which declares: "courts **shall be open** for redress of any injury, and justice shall be administered without sale, denial or delay." [emphasis added]

The members of the workgroup constitute a multidisciplinary team, from both the executive and judic ial branches of government, who have labored together for many weeks to propose ideas that will aid judges in keeping courts open. These guidelines are a set of aspirational goals that the judiciary of Florida may find useful in future planning. Our suggested guidelines are not intended to represent requirements for the judicial branch, for we believe that our courts, as is our society, are divergent, different, and unique. We offer these guidelines as suggestions for consideration by judges whose tasks are many, and whose work is often complex and overwhelming in its enormous consequences for our people.

Key to success in preparing for emergencies is the idea that there are many who will support us and help us if we ask. Communication and cooperation are the two overriding needs for success in planning for responses to threats and emergencies; we cannot emphasize this idea enough.

Americans are a resilient people, our diversity brings us together in a special eutectic – it is the stuff that holds us together, because it is the openness of our public institutions that allow us to find satisfaction and joy in our work and leisure. During this time of national concern and resolve, we celebrate the blessings of a free society, undeterred by the threats that plague a troubled world. As with great challenges of the past, our citizens have responded with their individual talents to fashion reasonable plans through which we may preserve our public institutions. This report encompasses such an activity.

We believe that the tasks, which the chief justice has asked us to examine, are not finished but have just begun. Preparing for threats and emergencies is an ongoing and living requirement, which will outlive this workgroup, and the leadership that gave birth to its formation.

EXECUTIVE SUMMARY

These proposed guidelines apply to the judicial branch and are intended to provide courses of action for the curtailment of court proceedings and the closure of court facilities during emergencies while ensuring local autonomy in both planning and execution. These guidelines should be adopted by the Court as a policy of the judicial branch. Many of the recommendations in this report are directed to the State Courts System, however, the concepts are also applicable to all judicial branch entities.

The chief justice, and the chief judges of the districts and circuits, should establish protocols for responding to emergencies. At a minimum, these protocols should include input, coordination, and recommendations from facility security, local law enforcement, local emergency management personnel, and representatives from the county or counties within each circuit, and with federal and state agencies as appropriate.

Emergency preparedness requires that coordination be established with all agencies that may become involved in assessments and responses to threats. The courts cannot achieve a high level of preparedness without the support and cooperation of agencies in the executive branch and with local agencies and constitutional officers. Key to successful planning is the establishment of means to foster coordination of resources and the establishment of communications links that will support immediate responses to threats and emergencies.

The chief justice and each chief judge should create a Court Emergency Management Group (CEMG) that includes representatives of state and local governmental agencies, representatives of state and local emergency management agencies as applicable, justices or judges, the state attorney, the public defender, the clerk of court, the sheriff, the marshal or circuit court administrator, and representatives of judicial branch agencies, if appropriate.

The CEMG should be made responsible for the creation of the Court Emergency Preparedness Plan and the development of recommended policies regarding the curtailment of court proceedings. The Court Emergency Preparedness Plan should incorporate both Emergency and Administrative Procedures and the Continuity of Operations Plan (COOP). The COOP should identify alternate facilities that may be necessary for the conduct of court proceedings in the event of an emergency and should include provisions for security, communications, and all necessary logistical support required by the court, and the officers of the court, for continued operations. The COOP should specify how the relocation of court proceedings will be accomplished if the emergency requires that court proceedings be curtailed for more than 24 hours. The Emergency and Administrative Procedures should specify how the court will operate if alternate facilities are not required.

It is critical to the judicial branch that accurate and current information is disseminated to the chief judges and other key decision makers within the judicial branch. The Emergency Coordinating Officer (ECO) of the judicial branch should serve as the nexus through which accurate and timely information is made available about potential threats and emergencies confronting the judicial branch. Threat assessments are exempt from public disclosure under the provisions of section 281.301, Florida Statutes, and rule 2.051, Florida Rules of Judicial Administration.

The chief judge of the districts and circuits, or the circuit court administrator if appropriate, should designate a court staff member to serve as the court's Public Information Officer (PIO) on a continuing basis. The chief judge should require that all court-related contacts with the media be managed through the Public Information Officer to ensure that only accurate information is disseminated. At a minimum, the Public Information Officer should be available as media contact whenever the court's emergency preparedness plan must be activated.

The Office of the State Courts Administrator should undertake actions to assist the districts and circuits in planning for emergency operations. Likewise, the Florida Court Education Council should play a key role in developing training programs that will prepare judges, marshals, court administrators, and court personnel in responding to emergencies and threats.

It is vital to the continuity of court operations that efforts are made to ensure the protection of the public, judicial officers, and court personnel. The chief justice and the chief judges of the districts and circuits should require that evacuation procedures be practiced and understood by all users of court facilities. Efforts should be undertaken to train all in how to respond to threats and emergencies that may involve life safety. There is no greater requirement for any organization than to protect the safety and health of its members.

Protecting records of the judicial branch should be of major concern to the court. Standards for protecting paper and electronic files should be put in place among all judicial branch entities as soon as possible, and the Judicial Management Council should be required by the Court to oversee this effort. 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. This effort will assist the Court in evaluating mitigation planning that presently exists, and how best to protect judicial branch records through corrective actions that may be included in future budget processes at the local and state levels.

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. The dramatic increase in computer interconnectivity, and the popularity of the Internet have been offering Florida's courts unprecedented opportunities to improve operations. At the same time, malicious attacks on computer systems have been increasing at alarming rates, and can pose serious risks to the critical operations that support the administration of justice in Florida. Electronic information and automated systems are essential to the operations of the courts, and therefore should be appropriately safeguarded. Safeguarding judicial branch records is important to ensure the confidentiality, integrity and availability of information necessary to process and resolve disputes, decide cases, and administer justice.

The Court should require that emergency preparedness planning continue as an ongoing and living process, and should require the Judicial Management Council to provide oversight for future efforts and amendments to these proposed guidelines.

SUMMARY OF RECOMMENDATIONS

- 1. The chief justice should appoint an Emergency Coordinating Officer (ECO) and an alternate for the judicial branch who will serve, pursuant to section 252.365, Florida Statutes, as the judicial branch liaison with the State Emergency Operations Center.
- 2. The chief judge of the districts and circuits should appoint ECOs and alternates who will act as liaisons on behalf of the court with appropriate law enforcement, fire department, weather, and other disaster response authorities and with county Emergency Operations Centers.
- 3. The Judicial Branch ECO and ECOs for the districts and circuits should develop means to alert and notify chief judges, court managers, local emergency preparedness coordinators, and employees with the most current information regarding impending emergencies.
- 4. The Emergency Coordinating Officer of the judicial branch and each district and circuit ECO should participate in orientation and training sessions with the State Emergency Operations Center.
- 5. The ECO should be given the responsibility for preparing and maintaining the Court Emergency Preparedness Plan under the guidance and direction of the Court Emergency Management Group (CEMG).
- 6. The chief justice should request that the Florida Department of Law Enforcement provide access to the Criminal Justice Network (CJNET) by the ECO of the judicial branch. The ECO of the judicial branch should serve as the conduit for the dissemination of information from the CJNET and the State Emergency Operations Center to the district and circuit ECOs, the chief justice, other justices, or other key judicial branch decision makers.
- 7. The chief justice and each chief judge should create a Court Emergency Management Group (CEMG) that includes representatives of state and local governmental agencies, representatives of state and local emergency management agencies as applicable, justices or judges, the state attorney, the public defender, the clerk of court, the sheriff, the marshal or circuit court administrator, and representatives of judicial branch agencies, if appropriate.
- 8. The CEMG should be made responsible for the creation of the Court Emergency Preparedness Plan and the development of recommended policies regarding the curtailment of court proceedings.

- 9. The CEMG should develop a recommended procedure through which the chief judge, the ECO, and any other designated Safety Officer will be apprised of the credibility of a threat or emergency situation by facility security, state or local law enforcement, and state or local emergency management personnel.
- 10. The ECO of the judicial branch should serve as the nexus through which accurate and timely information is made available about potential threats and emergencies confronting the judicial branch.
- 11. The state courts administrator should assist the ECO of the judicial branch in developing, through coordination with appropriate law enforcement organizations, a protected means through which the chief judges, marshals, and circuit court administrators of the state will be informed of emergencies or threat that may affect the districts or circuits.
- 12. The CEMG should develop procedures that protect the safety of the public and court personnel if it is necessary to evacuate a court facility. The procedures should address measures to assist persons with disabilities.
- 13. The CEMG should develop Administrative and Emergency Procedures to prepare for, respond to, recover from, and mitigate from emergencies not involving the use of alternate facilities; and a COOP to prepare for, respond to, recover from, and mitigate from emergencies requiring the use of alternate facilities.
- 14. Upon receipt of the recommendations of the Court Emergency Management Group, the chief justice or chief judge should review the recommendations, approve or revise the recommendations, and publish a Court Emergency Preparedness Plan for the court.
- 15. As soon as a credible threat is known to exist, the chief justice or chief judge should immediately assemble the Court Emergency Management Group comprised of members chosen by the chief justice or chief judge who may assist in executing contingency operations.
- 16. The chief justice and each chief judge should designate by written order, the judge or court officer who has authority to decide if court proceedings will be curtailed during their absence. The chief judge should appoint a Safety Officer and alternate for each court facility within the district or circuit who will be given authority to evacuate a court facility if it is determined that a threat is imminent, and the safety of the public and court personnel requires immediate action.
- 17. Should the chief justice or chief judge decide to curtail court proceedings or close a court facility, a written order of closing should be filed with the court and the ECO of the judicial branch should be immediately notified. A copy of the order should be filed with the Supreme Court of Florida.

- 18. Should the chief judge enter an order of closing, pursuant to Florida Rule of Judicial Administration 2.030(a)(2)(B)(iv), the chief judge should request that the chief justice enter such order or orders as may be appropriate to suspend, toll, or otherwise grant relief from time deadlines imposed by applicable statutes and rules of procedure for such period as may be appropriate, including, without limitation, those affecting speedy trial procedures in criminal and juvenile proceedings, all civil process and proceedings, and all appellate time limitations.
- 19. The chief justice should designate a court staff member to serve as the Public Information Officer (PIO) of the judicial branch. This officer should work with the ECO of the judicial branch during emergencies and should be present in the State Emergency Operations Center during major emergencies.
- 20. The state courts administrator, in cooperation with the Public Information Officer of the Supreme Court of Florida and the Public Information Officer of the judicial branch, should develop a guide for use by the Public Information Officers of each court during emergencies.
- 21. Upon appointment, the court Public Information Officer should coordinate with officials responsible for providing court security and should jointly develop a plan for dealing with emergencies, including crisis communications with the media.
- 22. The designated PIO of each court should develop a brochure that can be handed out to media, members of the public, and court personnel explaining basic procedures that will be followed during emergencies.
- 23. A means for providing current and accurate information to judges and court personnel should be developed by the PIO and continuing information should be provided to them throughout the emergency. An Internet site should be prepared in advance for use during emergencies.
- 24. The designated PIO should be made responsible for ensuring that the release of public information is coordinated between all response entities.
- 25. Upon the cessation of an emergency or threat, the chief justice or the chief judge should consult with the CEMG to assess what actions may be necessary to resume court operations.
- 26. The state courts administrator should provide technical assistance to the chief judges of the courts in the development of the Court Emergency Preparedness Plan and should assist chief judges in applications for grants that may aid responses to emergencies, or in the conduct of court-specific training programs for judges and court personnel relating to emergencies.

- 27. The Florida Court Education Council should develop training programs for judges, marshals, circuit court administrators, and court personnel relating to emergency preparedness.
- 28. The judicial branch should take steps to ensure that its officers and employees are trained in emergency procedures.
- 29. The Court Emergency Preparedness Plan should:
 - (a) Delineate what procedures will be followed and what agencies will be responsible for the decontamination of personnel and court facilities exposed to hazardous materials.
 - (b) Specify an evacuation procedure for each court facility that requires an annual unannounced test that is conducted during peak business hours.
 - (c) Require that each justice, judge, and all employees of the judicial branch rehearse and understand their personal evacuation route for any court facility to which they may be assigned.
- 30. Each court facility should have a Basic Life Safety (BLS) kit and portable Automated External Defibrillator (AED) in a readily accessible location.
- 31. Emergency medical team members should be designated and should be trained in the administration of basic first aid, CPR and use of an AED.
- 32. The Court Emergency Preparedness Plan should address methodologies for responding to a variety of medical emergencies.
- 33. Each district and circuit should provide judges and court employees with information to complete a Family Disaster Plan.
- 34. The chief judges of the districts and circuits should define a process in which a disaster assessment will be made.
- 35. The chief judges of the districts and circuits should establish an Emergency Management Team that would be convened during times of emergency or impending emergencies.
- 36. The chief judges of the districts and circuits should establish and communicate to all employees a listing of all personnel that would be categorized as either essential or non-essential when a court facility is closed due to an emergency.

- 37. To ensure efficient and clear lines of communication during emergencies, the chief judge, marshal, circuit court administrator, or the ECO should immediately activate, upon knowledge of an emergency, the court's telephone tree.
- 38. The chief judges of the districts and circuits should develop an Employee Emergency Recovery Guide for use by employees following an emergency.
- 39. The Court Emergency Preparedness Plan should identify, in advance, individuals who can serve on recovery teams to assist employees with identifying and accessing the support services needed.
- 40. The Court Emergency Preparedness Plan should be disseminated to the appropriate agencies affected by the plan, and to judges and court personnel who may have responsibilities for the execution of the plan.
- 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.

- (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.
- 43. The chief judges of the districts and circuits and all judicial branch entities should implement methods to physically secure paper, monitor and control environmental factors at paper storage sites, develop emergency procedures to protect paper when disaster is imminent, and develop mitigating measures if paper is lost or destroyed.
- 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.
- 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.
- 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.
- 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.
- 57. The court should require that emergency preparedness planning continue as an ongoing and living process, and should require the Judicial Management Council with oversight for future efforts and amendments to these proposed guidelines.

Final Report Page 16

PURPOSE

Article 1, section 21 of the Florida Constitution declares that the "courts shall be open for redress of any injury, and justice shall be administered without sale, denial or delay." Consistent with article V, section 2 of the Florida Constitution and Florida Rule of Judicial Administration 2.030, the following proposed guidelines are provided in harmony with the Florida Supreme Court's priority to maintain a safe environment for visitors and employees while ensuring the operation of the Florida State Court System. In order to ensure continuing public access to the courts, the judicial branch must be prepared to manage a variety of emergency situations, including natural disasters, terrorism, and extended information systems outages. Emergency preparedness is addressed in *Horizon 2002*, *The 2000-2002* Operational Plan for the Florida Judicial Branch, which includes an objective to provide "safe, functional, dignified, and healthy court facilities and infrastructure with high quality logistical, technological, and administrative support." These guidelines are consistent with the State of Florida Continuity of Government Plan (COG). The COG program derives authority from the State's Comprehensive Emergency Management Plan (CEMP), Section VI- Continuity of Government and from the State's Survivable Crisis Management Plan (SCM).

SCOPE

These proposed guidelines apply to all entities of the judicial branch and are intended to provide courses of action for the curtailment of court proceedings and the closure of court facilities during emergencies while ensuring local autonomy in both planning and execution. Many of the recommendations in this report are directed to the State Courts System, however, the concepts are also applicable to all judicial branch entities.

APPLICATION, IMPLEMENTATION, AND POLICY

The following recommended plans and procedures shall be achievable with resources and support that exist or are likely to be available. The chief justice, and the chief judges of the districts and circuits, should establish protocols for responding to emergencies. At a minimum, these protocols should include input, coordination, and recommendations from facility security, local law enforcement, local emergency management personnel, and representatives from the county or counties within each circuit, and with federal and state agencies as appropriate.

These proposed guidelines should be adopted by the Court as a policy of the judicial branch. The Court should require that emergency preparedness planning continue as an ongoing and living process, and should require the Judicial Management Council to provide oversight for future efforts and amendments to these proposed guidelines.

SECTION I

EMERGENCY OPERATIONS

(a) Tasks

- (1) Administrative Order AOSC01-54:
 - (A) Evaluate the advisability of appointing local emergency preparedness coordinators.
 - (B) Develop guidelines for emergency preparedness and contingency planning.
 - (C) Develop guidelines for the closing or alteration of regular business hours when there is a threat of harm in the form of any weapon (e.g., biological, germ, bomb, technological, or any similar weapons), natural disaster (e.g., fire, hurricane, tornado, flood, thunderstorms, or any other similar disasters), or other possible emergency (e.g., civil/political, nuclear, information warfare, or any other similar emergencies). This task should be given priority attention by the workgroup and recommended guidelines should be submitted to the Court not later than January 31, 2002.
 - (D) Develop relationships with the appropriate law enforcement, fire department, weather, and other appropriate disaster response authorities.
 - (E) Consider the role of law enforcement agencies in establishing safety plans for court facilities.
 - (F) Develop a plan to alert and notify chief judges, court managers, local emergency preparedness coordinators, and employees of impending emergencies; provide guidance for local jurisdictions to establish their own plan.
 - (G) Develop judicial branch operational contingency plans and procedures (e.g., destroyed structures, contamination, closed courts, information systems outages, large influx of cases requiring expedited processing, etc.).
- (2) Continuity of Operations Plan (COOP):
 - (A) Review Judicial Management Council's Committee on Trial Court Performance and Accountability work products.

(B) Identify and prioritize the essential functions that enable the judicial branch to provide vital services, exercise civil authority, and maintain the safety and well being of the general populace. What functions must the courts

perform during emergency operations?

(C) Identify essential personnel required to sustain and support the court during emergency operations.

- (D) Define organizational responsibilities for ensuring continued provision of essential functions.
- (F) Review delegations of authority. To whom should the Chief Justice delegate emergency responsibilities?
- (G) Define the functions, duties, and authority of a proposed Court Emergency Preparedness Coordinator. Is such a position required?
- (H) Review lines of succession and propose needed statutory, rule, or other policy changes.
- (I) Identify needed administrative orders, rules, or statutory revisions necessary to support continuation of court operations in emergencies and review legal issues relating to the overall tasks assigned to the committee as a whole.
- (J) Develop suggested standards for, and provide examples for, a media relations program that should be implemented by chief judges of the districts and circuits during emergency operations.
- (K) Develop suggested standards for public information packets, public education materials, and press guides to be utilized by the courts during emergencies.
- (L) Develop suggested standards for court Internet pages to be activated during emergency operations.
- (M) Suggest alternatives for inter-local and mutual aid agreements, inter- and intra- circuit alternatives, and inter-court relocations of court operations during emergencies.
- (N) Consider the role of law enforcement agencies in establishing safety plans for court facilities and identify security needs for alternative locations during emergencies.

- (O) Identify required communications and data networks necessary for continued operations and propose alternatives for interoperable communications among the leadership of the judicial branch during
 - (P) Identify essential supplies, equipment and furnishings.

emergencies.

- (Q) Propose alternatives for the provision of emergency notification of chief judges, court managers, and court employees.
- (R) Identify means for providing judicial branch leaders with current intelligence information during normal and emergency operations.
- (S) Suggest a structure through which the courts should establish liaison with state and local emergency management operations centers and identify required interoperable communications with each center. Make recommendations regarding a process that should be followed prior to the closure of a court facility.
- (T) Identify and recommend how the judicial branch should interface its Court Emergency Preparedness Plan with executive branch agencies and plans and recommend standards for integration of local plans with local agencies.

(b) **Discussion**

Section I presents proposed guidelines for emergency preparedness and contingency planning, and addresses the tasks of Administrative Order AOSC01-54 relating to closure of court proceedings, and the continuation of proceedings in alternate locations. The section delineates a process through which the chief justice and the chief judges of the districts and circuits may develop Court Emergency Preparedness Plan for the courts.

The workgroup believes that it is essential that chief judges of the districts and circuits in Florida develop emergency preparedness plans that delineate the tasks and responsibilities of all entities that may become involved in threats that affect the continuation of court proceedings. Plans should be specific and detailed and each entity involved in the execution of the plan should thoroughly understand what the entity is expected to do, who will be involved in the plan, when the entity is expected to take the action, where the action will occur, why the action may be necessary, and how the plan is to be accomplished.

Emergency preparedness requires that coordination be established with all public agencies that may become involved in assessments and responses to threats. The courts cannot achieve a high level of emergency preparedness without the support and cooperation of agencies in the executive branch and with local agencies and constitutional officers. Key to successful planning is the establishment of means to foster coordination of resources and the establishment of communications links that will support immediate responses to threats and emergencies.

Likewise, such efforts will require the appointment of officers who may aid judges in the development of plans and coordinated responses to threats and emergencies. Means to communicate threats to the decision makers of the judicial branch should be put in place and efforts should be made to enhance and improve interoperable communications among all courts within the judicial branch. While the chief judges of the districts and circuits should be informed of the latest threat information, they should not duplicate the efforts of the law enforcement community but should rather work with such agencies to foster information sharing and information dissemination.

Closure of court proceedings may be necessary to protect the public, judicial officers, and court employees, however, planning may help to ensure that proceedings will continue at alternate locations. The leadership of the judicial branch should be consulted and be involved in assessing threats and in determining an appropriate response.

The public should be informed of emergencies which threaten the ability of the courts to continue operations and should be advised when proceedings will continue or what alternative locations will be used for the continuation of proceedings. Regular and coordinated media briefings should occur and one representative should speak for the courts during emergencies.

These guidelines are consistent with the State's *Comprehensive Emergency Management Plan* (CEMP), Section VI- Continuity of Government, and the State's *Survivable Crisis Management Plan* (SCM), Section III — Continuity of Government.

GUIDELINES

(a) Planning for Emergency Operations

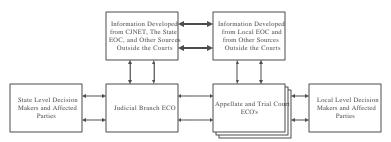
- (1) Emergency Coordinating Officer
 - (A) The chief justice should appoint an Emergency Coordinating Officer (ECO) and an alternate for the judicial branch who will serve, pursuant to section 252.365, Florida Statutes, as the judicial branch liaison with the State Emergency Operations Center.
 - (B) The chief judge of the districts and circuits should appoint ECOs and alternates who will act as liaisons on behalf of the courts with appropriate law enforcement, fire department, weather, and other disaster response authorities and with county Emergency Operations Centers.
 - (C) The names of the persons appointed by the chief justice and each chief judge and their contact information should be provided to the Emergency Coordinating Officer of the judicial branch.
 - (D) The ECO should be an individual with sufficient standing, rank, visibility, and authority to make independent decisions on behalf of the chief justice or chief judge during emergencies.
 - (E) The judicial branch ECO and ECOs for the districts and circuits should develop means to alert and notify chief judges, court managers, local emergency preparedness coordinators, and employees with the most current information regarding impending emergencies. Each district and circuit ECO should establish and maintain multiple means of communicating with the chief judge, marshal, circuit court administrator, appropriate local constitutional officers, and other local court related personnel and should coordinate with the appropriate county Emergency Operation Centers to provide for both primary and alternate lines of communication.
 - (F) The Emergency Coordinating Officer of the judicial branch and each district and circuit ECO should participate in orientation and training sessions with the State Emergency Operations Center.

(G) The ECO should be given the responsibility for preparing and maintaining the Court Emergency Preparedness Plan under the guidance and direction of the Court Emergency Management Group (CEMG). The CEMG

and the ECO should structure planned responses to emergencies, and should ensure that such plans are coordinated with federal, state, and county emergency management and law enforcement agencies and personnel.

(H) The chief justice should request that the Florida Department of Law Enforcement provide access to the Criminal Justice Network (CJNET) by the ECO of the judicial branch. The ECO of the judicial branch should serve as the conduit for the dissemination of information from the CJNET and the State Emergency Operations Center to the district and circuit ECOs, the chief justice, other justices, or other key judicial branch decision makers. The ECO of the judicial branch should receive the necessary training regarding CJNET and be authorized access to the information available on the CJNET and be given discretion and authority to interpret and disseminate intelligence information as necessary.

(I) The ECO of the judicial branch and the district and circuit ECO's should establish plans that will allow information before, during, and after emergencies to flow as follows:



- (2) Court Emergency Management Group
 - (A) The chief justice and each chief judge should create a Court Emergency Management Group (CEMG) that includes representatives of state and local governmental agencies, representatives of state and local emergency management agencies as applicable, justices or judges, the state attorney, the public defender, the clerk of court, the sheriff, the marshal or circuit court administrator, and representatives of judicial branch agencies, if appropriate.

(B) The CEMG should recommend to the chief justice or the chief judge what procedures should be used to determine if court proceedings will be curtailed due a threat of harm in the form of any weapon (e.g., biological, germ, bomb, technological, or any similar weapons), natural disaster (e.g., fire, hurricane, tornado, flood, thunderstorms, or any other similar disasters), or other possible emergency (e.g., civil/political, nuclear, information warfare, or any other similar emergencies). The group should consider what emergencies are most likely to affect the future operations of the courts by the conduct of a threat analysis and it should focus planning activities on these events. The group should also pre-determine a decision-making process that would minimize potential conflicts between agencies/constitutional officers/levels of government during emergency situations.

(C) The CEMG should be made responsible for the creation of the Court Emergency Preparedness Plan and the development of recommended policies regarding the curtailment of court proceedings. The Court Emergency Preparedness Plan should incorporate both Emergency and Administrative Procedures and the Continuity of Operations Plan (COOP) and should be regarded as confidential. The COOP should identify alternate facilities that may be necessary for the conduct of court proceedings in the event of an emergency and should include provisions for security, communications, and all necessary logistical support required by the court, and the officers of the court, for continued operations. The COOP should specify how the relocation of court proceedings will be accomplished if the emergency requires that court proceedings be curtailed for more than 24 hours. The Emergency and Administrative Procedures should specify how the court will operate if alternate facilities are not required. The CEMG should consider how the courts would operate without electrical power and what emergency forms may be necessary to conduct proceedings when electrical power is not available. The CEMG should specify what court adjunct agency personnel will be required to conduct proceedings during emergencies, including provisions for the security of the court and its officers. The CEMG should pre-identify essential personnel who will be on duty during emergencies. The CEMG should give consideration to the development of an employee emergency response plan with general information, not considered confidential, that may be distributed to all court personnel.

(D) The CEMG should develop a recommended procedure through which the chief judge, the ECO, and any other designated Safety Officer will be apprised of the credibility of a threat or emergency situation by facility security, state and local law enforcement, and state or local emergency management personnel. The procedure should allow the facility security, state and local law enforcement, or state and local emergency management personnel to review, analyze, and determine the credibility of the threat or emergency situation. These procedures should stipulate that the chief justice or chief judge, or their designees, should be provided with as much information as possible regarding the threat or emergency situation. Consideration should be given to developing a form that may be used to

record the details regarding the threat or emergency situation.

- (E) The CEMG should develop procedures that protect the safety of the public and court personnel if it is necessary to evacuate a court facility. The procedures should address measures to assist persons with disabilities. Provisions should be made for ongoing training of court personnel and judges in evacuation procedures. Procedures for responses to bomb threats, medical emergencies, fire alarms, and other emergencies should be made known to all persons occupying a court facility. Evacuation plans should be tested semiannually during peak business hours and should be subject to an after action review by the chief justice or chief judge.
- (F) The CEMG should develop Administrative and Emergency Procedures to prepare for, respond to, recover from, and mitigate from emergencies not involving the use of alternate facilities; and a COOP to prepare for, respond to, recover from, and mitigate from emergencies requiring the use of alternate facilities. Instructions for Preparation of Administrative and Emergency Procedures are provided in Appendix A. A sample outline for the COOP is shown in Appendix B together with a detailed example of a completed COOP. A depiction of the general steps associated with responding to emergency situations and how these steps relate to the parts of the Court Emergency Preparedness Plan is provided in Appendix C; and a depiction of the process for implementation of these guidelines within the judicial branch is shown in Appendix D.
- (G) The CEMG should meet on an ongoing basis to update, test, evaluate and improve the Court Emergency Preparedness Plan of the court.

Final Report Page 25

(H) Upon receipt of the recommendations of the Court Emergency Management Group, the chief justice or chief judge should review the recommendations, approve or revise the recommendations, and publish a Court Emergency Preparedness Plan for the court. The Court Emergency Preparedness Plan should be disseminated to the appropriate agencies affected by the plan, and to judges and court personnel who may have responsibilities for the execution of the plan. This plan is exempt from public disclosure under the provisions of section 281.301, Florida Statutes, and rule 2.051, Florida Rules of Judicial Administration. The Court Emergency Preparedness Plan should be updated at least annually.

(3) Suspension of Court Proceedings and Court Closures

- (A) As soon as a credible threat is known to exist, the chief justice or chief judge should immediately assemble the Court Emergency Management Group comprised of members chosen by the chief justice or chief judge who may assist in executing contingency operations. The Court Emergency Management Group should assess the threat and if necessary, recommend, and upon approval of the chief justice or chief judge, execute measures to minimize danger to life and property.
- (B) The chief justice and each chief judge should designate by written order, the judge or court officer who has authority to decide if court proceedings will be curtailed during their absence. The chief judge should appoint a Safety Officer and alternate for each court facility within the district or circuit who will be given authority to evacuate a court facility if they determine that a threat is imminent, and the safety of the public and court personnel requires immediate action.
- (C) Should the chief justice or chief judge decide to curtail court proceedings or close a court facility, a written order of closing should be filed with the court and the ECO of the judicial branch should be immediately notified. A copy of the order should be filed with the Supreme Court of Florida. The marshal or the circuit court administrator should immediately execute the order and notify the media of the intended closure. The chief justice or chief judge should ensure that measures have been implemented to notify members of the court, court personnel, and adjunct agency personnel of an intended closure.

(D) Should the chief judge enter an order of closing, pursuant to Florida Rule of Judicial Administration 2.030(a)(2)(B)(iv), the chief judge should request that the chief justice enter such order or orders as may be appropriate to suspend, toll, or otherwise grant relief from time deadlines imposed by applicable statutes and rules of procedure for such period as may be appropriate, including, without limitation, those affecting speedy trial procedures in criminal and juvenile proceedings, all civil process and proceedings, and all appellate time limitations.

(4) Dissemination of Threat Information

- (A) It is critical to the judicial branch that accurate and current information is disseminated to the chief judges. The ECO of the judicial branch should serve as the nexus through which accurate and timely information is made available about potential threats and emergencies confronting the judicial branch. Threat assessments are exempt from public disclosure under the provisions of section 281.301, Florida Statutes, and rule 2.051, Florida Rules of Judicial Administration.
- (B) The state courts administrator should assist the ECO of the judicial branch in developing through coordination with appropriate law enforcement organizations a protected means through which the chief judges, marshals, and circuit court administrators of the state will be informed of emergencies or threat that may affect the districts or circuits. The marshals and the circuit court administrators should develop a means of disseminating information to judges and court personnel regarding a potential threat or emergency.
- (C) The state courts administrator should create an Intranet site that provides links to emergency management resources, weather information, and law enforcement advisories relating to terrorism or threats that may affect the judicial branch.

(5) Public Information

The chief justice should designate a Court staff member to serve as the Public Information Officer (PIO) of the judicial branch. This officer should work with the ECO of the judicial branch during emergencies and should be present in the State Emergency Operations Center during major emergencies. The chief judge of the districts and circuits, or the circuit court administrator if appropriate, should designate a court staff member to serve as the court's PIO on a continuing basis. The chief judge should require that all court-related contacts with the media be managed through the PIO to ensure that only accurate information is disseminated. At a minimum, the PIO should be available as media contact whe never the Court Emergency Preparedness Plan must be activated.

- (A) The state courts administrator, in cooperation with the PIO of the Supreme Court of Florida and the PIO of the judicial branch, should develop a guide for use by the PIOs of each court during emergencies.
- (B) Upon appointment, the court PIO should coordinate with officials responsible for providing court security and should jointly develop a plan for dealing with emergencies, including crisis communications with the media. The plan should include the establishment of a single location where the news media may gather during the emergency. Court security personnel and the PIO should remain in constant communication for the duration of the emergency.
- (C) The designated PIO of each court should develop a brochure that can be handed out to media, members of the public, and court personnel explaining basic procedures that will be followed during emergencies.
- (D) A means for providing current and accurate information to judges and court personnel should be developed by the PIO and continuing information should be provided to them throughout the emergency. An Internet site should be prepared in advance for use during emergencies.

(E) The designated PIO should be made responsible for ensuring that the release of public information is coordinated between all response entities. The PIO may be asked to serve in a Joint Information Center under the operational control of another organization. This coordination will serve as a focal point for the coordination and provision of information to the public and media concerning the emergency response.

(b) Restoration of Court Operations

- (1) Upon the cessation of an emergency or threat, the chief justice or the chief judge should consult with the CEMG to assess what actions may be necessary to resume court operations. Should the chief justice or chief judge determine that court proceedings must be moved to alternative facilities, the COOP should be initiated.
- (2) Alteration of operational hours shall be considered whenever necessary during full or partial facility shutdown in order to continue essential court business. Alteration of operational hours may also be considered where sufficient numbers of essential personnel are unavailable or when accommodating essential functions of another court jurisdiction within the same facility. Any overtime required shall be compensated according to personnel policy. The court should establish an emergency call-out policy for this purpose. The chief judge may consider round-the-clock (24 hours a day, 7 days a week) operational hours in the event the COOP is activated for the purpose of bringing essential functions back on line at an alternative location.

(c) Assistance and Training

- (1) The Office of the State Courts Administrator should undertake actions to assist the districts and circuits in planning for emergency operations. Likewise, the Florida Court Education Council should play a key role in developing training programs that will prepare judges, marshals, court administrators, and court personnel in responding to emergencies and threats.
 - (A) The state courts administrator should provide technical assistance to the chief judges of the courts in the development of the Court Emergency Preparedness Plan and should assist chief judges in applications for grants that may aid responses to emergencies, or in the conduct of court-specific training programs for judges and court personnel relating to emergencies.
 - (B) The Florida Court Education Council should develop training programs for judges, marshals, circuit court administrators, and court personnel relating to emergency preparedness.

SECTION II

PERSONNEL MANAGEMENT

(a) Tasks

- (1) Administrative Order AOSC01-54:
 - (A) Ensure that the focus of court emergency plans and guidance is on the safety of court personnel and the public, and guaranteeing public access to the courts.
- (2) Continuity of Operations Plan (COOP):
 - (A) Identify means of personal protection for court employees during normal and emergency operations.
 - (B) Identify established medical services available to court personnel during emergencies, and develop standard protocols for the provision of medical services to court employees during emergencies.
 - (C) Develop standards for logistical support requirements of employees during emergencies.
 - (D) Suggest alternative means for the administration of payroll and other personnel functions if the infrastructure is destroyed or disabled.
 - (E) Develop operational hours, and work times, both emergency and non-emergency.
 - (F) Identify vital personnel records and suggest standards for their protection during normal operations and their availability during emergencies.
 - (G) Suggest guidelines for the identification of essential and non-essential personnel needed to sustain the courts during emergency operations.
 - (H) Suggest guidelines for the development of employee directories that would include addresses, telephone numbers and emergency contact information and means of telephonic notification such as telephone tree lists.
 - (I) Suggest guidelines for employee support following catastrophic emergencies.

(J) Review plans and procedures developed by other courts and make recommendations regarding safety of court personnel and the public.

(b) **Discussion**

In Section II, consideration is given to the needs of the public, judicial officers, and court personnel during and after threats and emergencies. Suggestions are made regarding how personnel of the judicial branch should be managed before, during, and after emergencies.

It is vital that efforts are made to protect the public, judicial officers, and court personnel during threats or emergencies. The chief justice and the chief judges of the districts and circuits should require that evacuation procedures be practiced and understood by all users of court facilities. Efforts should be undertaken to train all judicial officers and all court personnel in how to respond to threats and emergencies that may involve life safety. There is no greater requirement for any organization than to protect the safety and health of its members.

The concept of the Continuity of Operations Plan (COOP) encompasses the idea that organizations must first protect personnel from potential harm in order for the organization itself to continue its mission. Protection of personnel also involves the need to protect vital records of judicial officers and court personnel and to assist all in the development of personal plans that can be exercised during emergencies.

Judicial officers and court personnel will be required to continue their work during emergencies. Planning must include provisions for protecting judicial officers and court personnel when such emergencies require their continued service. Alternate work schedules may be required during emergencies and chief judges of the districts and circuits should have pre-identified non-essential and essential personnel necessary to continue court operations. The aftermath of an emergency may require that judicial officers and court personnel receive medical assistance or decontamination. The Court Emergency Preparedness Plan, of necessity, should address these potential needs and should require that appropriate coordination with health and emergency response agencies are in place.

Judicial officers and court personnel should be made aware of the means for their notification of emergencies or threats. It is vital that an effective system for communicating threats is established and practiced by each court. Most critical is the need to train judicial officers and court personnel in the proper responses to threats and emergencies. In particular, judges should understand and have practiced effective evacuation procedures within the court facility to which they are assigned. As public leaders, judges have a special responsibility to understand, and be able to convey to the public, proper evacuation procedures.

GUIDELINES

(a) Personnel Management

- (1) The judicial branch should take steps to ensure that its officers and employees are trained in emergency procedures and it should provide for the following:
 - (A) Each circuit COOP should address alternative procedures to ensure that county-funded court employees are paid during emergencies. Such procedures should be developed in consultation with the county entity responsible for the processing of county payrolls (county personnel office or Clerk of the Circuit Court). Sufficient payroll processing redundancy currently exists for state-funded court employees.
 - (B) All courts are encouraged to store vital personnel records in an electronic format. Duplicate electronic files should be made, periodically updated and stored in an off-site location. All employees should be encouraged to review their personnel records on an annual basis to ensure that basic personal information such as insurance beneficiaries, addresses, insurance coverage, and withholding tax, are up to date. Vital personnel records portray information about an employee that is essential for providing compensation and benefits to an employee by its employer; such as, but not limited to, employee name, address, social security number, date of hire, date of birth, rate of pay, classification, payroll deductions and tax withholdings, health, life and disability insurance provider, beneficiaries, and leave records. Vital personnel records include:
 - (i) Automated personnel database for employees and positions such as the Cooperative Personnel Employment System (COPES). If the state's personnel system is outsourced, the vendor will be required have security measures in place.
 - (ii) Employee personnel records such as employee name, address, social security number, date of birth, date of hire, citizenship status, education level, employment status, sex, and race.
 - (iii) Personnel actions such as pay changes, reclassifications, promotions, and discipline within the last year that is also retained in COPES.
 - (iv) Benefit data records such health, life and disability insurance providers and dependant and beneficiary information.

- (v) Retirement records which are maintained by the Division of Retirement, which is responsible for maintaining and backing up essential retirement records on its members.
- (vi) Personnel Regulations Manual which is currently available on diskette.
- (vii) Equal Employment Opportunity Plan and other policies that may be necessary to receive grant funding.
- (viii) Attendance and leave records indicating balances for each category.
- (ix) Employee Directories through which employees provide personal information, as well as emergency contact information, to their Personnel Office to complete an employee profile (See Appendix E). The data from these forms are to be kept in an Emergency Contact Information Log (See Appendix F) by the court's Personnel Officer or their representative and updated as necessary. Each employee is responsible for submitting an updated Employee Profile Form as soon as a change occurs.

(b) Protection of Officers and Court Employees

- (1) Decontamination and Emergency Evacuation
 - (A) The Court Emergency Preparedness Plan (CEMP) should:
 - (i) Delineate what procedures will be followed and what agencies will be responsible for the decontamination of personnel and court facilities exposed to hazardous materials.
 - (ii) Specify an evacuation procedure for each court facility that requires an annual unannounced test that is conducted during peak business hours.
 - (iii) Require that each justice, judge, and all employees of the judicial branch rehearse and understand their personal evacuation route for any court facility to which they may be assigned.

(2) Medical Services

- (A) Each court facility should have a Basic Life Safety (BLS) kit and portable Automated External Defibrillator (AED) in a readily accessible location. Additional units may be necessary depending on the court's physical layout and number of court personnel.
- (B) Emergency medical team members should be designated and should be trained in the administration of basic first aid, CPR and use of an AED.
- (C) The Court Emergency Preparedness Plan should address methodologies for responding to a variety of medical emergencies. These may include, but are not limited to, injuries from blunt force trauma, ingested poison or airborne particulates. The plan should include identifying which hospitals are prepared to respond to different emergencies as well as secondary locations. ECOs in circuits with rural counties, with a limited number of emergency and trauma certified hospitals, should consult with local officials to determine levels of care available and expected response times.
- (D) Family Disaster Plans. Each district and circuit should provide judges and court employees with information to complete the Family Disaster Plans (See Appendix G).

(c) Emergency Management Requirements

(1) Disaster Assessment - Hours of Operation

The chief judges of the districts and circuits should define a process in which a disaster assessment will be made and hours of operation (if any) are defined. Included in the process should be a determination of which functions will be performed, which functions will be delayed or continued, and which personnel will be required to work during the emergency.

(2) Emergency Management Team

- (A) The chief judges of the districts and circuits should establish an Emergency Management Team that would be convened during times of emergency or impending emergencies. Such teams should include the following individuals or their designees:
 - (i) Chief Judge
 - (ii) Marshal/Circuit Court Administrator
 - (iii) Emergency Coordinating Officer (ECO)
 - (iv) Alternate Emergency Management Coordinator (AECO)
 - (v) Court Personnel Officer
 - (vi) Court Public Information Officer
 - (vii) Court Technology Officer
 - (viii) Building Managers/Liaisons
 - (ix) Clerical Staff
- (B) Individuals on the Emergency Management Team should be added or deleted at the discretion of the chief judge. The chief judges of the districts and circuits should also predetermine what staff would be deemed non-essential when a court facility is closed due to an emergency. Those employees that are deemed essential or non-essential may change after the Emergency Management Team or chief judge makes an assessment.
- (C) The chief judges of the districts and circuits should establish and communicate to all employees a listing of all personnel that would be categorized as either essential or non-essential when a court facility is closed due to an emergency.

(3) Telephone Tree

To ensure efficient and clear lines of communication during emergencies, the chief judge, marshal, circuit court administrator, or the ECO should immediately activate, upon knowledge of an emergency, the court's telephone tree. The telephone tree represents the court's chain of command. Each individual at each level is responsible for having updated employee contact information on those who they are responsible for contacting.

(4) Employee Emergency Recovery Guide

The chief judges of the districts and circuits should develop an Employee Emergency Recovery Guide for use by employees following an emergency (See Appendix G). The Employee Emergency Recovery Guide should provide information that will assist employees to stabilize their basic human needs as well as help them return to pre-emergency conditions. The Employee Emergency Recovery Guide should:

- (A) Identify services offered by the employer such as an Employee Assistance Program and how to access the program.
- (B) Identify services offered by the employee's health insurance provider.
- (C) Identify agencies in the community such as the American Red Cross, and the County, State and Federal Emergency Management Agencies, which can provide human services, housing, financial and daycare assistance. Some of the services provided by these agencies include: Disaster Unemployment Assistance, Temporary Housing, Individual and Family Grants, Food Coupons, Disaster Related Stress Management, Individual and family Counseling, Insurance Claims Assistance, Income Tax Services and Financial Assistance.
- (D) The court should be prepared to immediately communicate to its employees any additional services that become available as a result of the emergency.

(5) Recovery Teams

The Court Emergency Preparedness Plan should identify, in advance, individuals who can serve on recovery teams to assist employees with identifying and accessing the support services needed.

(6) Training

The Court Emergency Preparedness Plan should be disseminated to the appropriate agencies affected by the plan, and to judges and court personnel who may have responsibilities for the execution of the plan. Resources should be utilized to train judges and court employees about the purpose and contents of the plan. The training process should include tests of equipment, policies and processes identified within the plan. The plan should be exercised and after action reviews conducted to ensure that essential operations and functions can be accomplished.

SECTION III

SAFEGUARDING RECORDS OF THE JUDICIAL BRANCH

(a) Tasks

(1) Administrative Order AOSC01-54:

Devise statewide policy and guidance to safeguard technology infrastructure and to back up critical information (both electronic and paper).

- (2) Continuity of Operations Plan (COOP):
 - (A) Devise statewide policy guidance to safeguard the courts' technology infrastructure and to back-up critical information (both automated and paper).
 - (B) Propose statewide policy and guidance for security of court automated records and systems.
 - (C) Propose standards for continued operations of automated systems during emergencies including reestablishment of systems on alternative machines (HOT Sites).
 - (D) Identify essential forms required to sustain court operations if electrical power or automated systems are unavailable.
 - (E) Define the vital records of the judicial branch and propose guidelines to preserve and protect court records (paper and electronic), propose mitigation measures, and review ways to recreate records that are destroyed.

(b) Discussion

Section III discusses the enormous issues associated with protecting the records of the judicial branch, whether paper or electronic, and suggests standards that should be considered for adoption by the judicial branch for their protection.

On March 7, 2002, the Court approved amendments to Rule 2.051 (b), Florida Rules of Judicial Administration, which defined the records of the judicial branch:

- **(b) Definitions**. Judicial records for this rule refer to documents, exhibits in the custody of the clerk, papers, letters, maps, books, tapes, photographs, films, recordings, data processing software of other material created by any entity within the judicial branch, regardless of physical form, characteristics, or means of transmission, that are made or received pursuant to court rule, law or ordinance, or in connection with the transaction of official business by any court or court agency.
 - (1)"Records of the judicial branch" are all records, regardless of physical form, characteristics, or means of transmission, made or received in connection with the transaction of official business by any judicial branch entity and consist of:
 - (A) "court records," which are the contents of the court file, including the progress docket and other similar records generated to document activity in a case, transcripts filed with the clerk, documentary exhibits in the custody of the clerk, and electronic records, videotapes, or stenographic tapes of depositions or other proceedings filed with the clerk, and electronic records, videotapes, or stenographic tapes of court proceedings; and
 - (B) "administrative records," which are all other records made or received pursuant to court rule, law, or ordinance, or in connection with the transaction of official business by any judicial branch entity.
 - (2) "Judicial branch" means the judicial branch of government, which includes the state courts system, the clerk of court when acting as an arm of the court, The Florida Bar, the Florida Board of Bar Examiners, the Judicial Qualifications Commission, and all other entities established by or operating under the authority of the Supreme Court or the chief justice.

In this opinion, the Court made clear its authority to provide oversight and control of such records.

The Court has said: "We conclude that the clerks of the circuit courts, when acting under the authority of their article V powers concerning judicial records and other matters relating to the administrative operation of the courts, are an arm of the judicial branch and are subject to the oversight and control of the Supreme Court of Florida, rather than the legislative branch." Times Publishing Company v. Ake, 660 So 2d 255 (Fla. 1995).

As the overseer of judicial branch records, it follows, that the Court may impose standards regarding how such records are protected and maintained. The Judicial Management Council and the Court Technology Commission should examine the guidelines proposed herein and should make recommendations to the Court for mandatory standards to be followed by all entities of the judicial branch.

The dramatic increase in computer interconnectivity, and the popularity of the Internet have been offering Florida's courts unprecedented opportunities to improve operations. At the same time, malicious attacks on computer systems have been increasing at alarming rates, and can pose serious risks to the critical operations that support the administration of justice in Florida. Electronic information and automated systems are essential to the operations of the courts, and therefore should be appropriately safeguarded. Safeguarding court records is important to ensure the confidentiality, integrity and availability of information.

The Florida State Court System relies heavily on the availability of court records both paper and electronic to process cases. These records are the official demonstration of the outcome of hearings and decisions made by the courts. Plans must be put in place to protect court records from harm, make court records available at alternate locations due to an emergency situation, and to recover records if destroyed or damaged.

Maintaining offsite duplicates of paper records is the greatest security to overcome losses of paper records from emergencies or disasters. This can be accomplished by the photocopying of all paper records, which is prohibitively expensive in terms of labor and storage, and is not a feasible recommendation based upon the charge that this plan be undertaken under existing budgetary restraints. Likewise, duplication of paper records by scanning or microfiche, while presenting less of a storage obstacle, involves the investment of labor and technology that is likewise cost prohibitive. Thus, preservation and protection of the records of the judicial branch within existing budgetary restraints requires these prophylactic measures:

- (1) Monitoring of temperature/humidity control equipment.
- (2) Safe storage of records which requires that records are not to be stored less than six inches from ceilings or suspended lights or eighteen inches from sprinkler heads. Records should not be stored on the floor or in contact with electrical or fire alarm systems or where they will obstruct any exit, access panel, air conditioning duct, or fire extinguisher. Regular inspection of storage areas should be undertaken to look for signs of roof leaks or infestation of rodents or insects.
- (3) Fire prevention which requires that flammable solvents must be kept out of records storage areas; trash must not be allowed to accumulate; electrical outlets must not be overloaded; extension cords should not be used on a permanent basis, and when in use they should be industrial-weight cords. An adequate alarm or sprinkler system should be utilized.

- (4) When an emergency or disaster may be imminent, that protection measures for paper records includes securely wrapping storage areas with plastic, moving records near the floor to higher shelving to reduce loss from flooding, and making provision to move vital records to less threatened locations offsite.
- (5) Reasonable steps should be taken to secure physical access to records to prevent risk of unauthorized removal of documents or malicious acts that would damage paper records.

Maintaining duplicate electronic records is both feasible and critical to ensure protection of critical electronic information. Electronic information can be stored on a variety of medium each with specific benefits and life expectancy. The chief judges of the districts and circuits should devise methods of having not only data, but also a duplicate copy of software stored off site for recovery purposes.

Vital records are those that support the most critical activities of the judicial branch, and are necessary in the event of an emergency or disaster for the resumption of normal operations. Federal agency guidelines customarily conclude that only one to seven percent of records are vital, but a greater portion of judicial paper records may qualify as vital due to the nature of business undertaken by the judicial branch and, principally from the perspective of the clerks of court, heavy reliance on paper files. Records of the judicial branch have been divided between court records maintained by the clerks of court, and administrative records maintained by the marshals of the districts and the court administrators of the circuits, the Office of the State Court Administrator, and judges' offices.

The clerks of the circuit court, the clerks and marshals of the appellate courts, and circuit court administrators, must assess which records are deemed to be vital. These may be best analyzed by dividing them into two categories, those necessary to maintain the operation of the office and to have available a work force to keep the court in operation, and those essential for the administration of justice.

- (1) Office Functions (a partial list):
 - (i) Accounts-receivable records
 - (ii) Social security records
 - (iii) Payroll records
 - (iv) Retirement records
 - (v) Insurance records
 - (vi) Records relating to purchase and other contractual obligations, especially as relates to supplies needed for mitigation and recovery in the face of loss, and with vendors supplying recovery assistance.

Current practices suggest that most of these records are stored electronically.

Due to the configuration of Florida's appellate courts, records maintained by marshals involve a mixture of administrative matters that would fall under the aegis of clerks at the trial level (payroll records for clerk personnel and purchase orders pertinent to case file maintenance, for example) and those that would be maintained typically by court administrators at the trial level (payroll records of judicial assistants, for example). As such the appellate courts' marshals do not fit comfortably in the division proposed above between clerks on the one hand and administrators on the other. As such the records of the marshals of appellate courts are considered in both subdivisions, depending upon the function the marshal's duties.

While the preservation of closed files is required based upon retention schedules, the identification of vital records must begin by evaluating the relative importance of active, ongoing case files. As such each court in assessing which of these active groups of files is vital might, as a general proposition, elevate the protection of human safety as the highest priority, in which case, for example, juvenile dependency and felony criminal files may be regarded as more vital than other open files, such as those involving non-criminal traffic infractions. The chief judges of the districts and circuits should determine the importance of records at a local level and even on a case-by-case basis depending on the type and duration of the emergency. Partial lists of factors that may be considered are:

- (1) Does the type of case typically involve issues of human safety?
- (2) In the context of criminal or delinquent behavior, is it reasonable to assume that as a class that adult felony case files are "more vital" than are those involving misdemeanors and delinquent acts?

- (3) To what extent, if any, do guardianship matters typically involve human safety issues?
- (4) With property matters, are circuit civil cases any more vital as a class than are those in county civil?
- (5) Do criminal and delinquency matters more commonly involve property and contraband issues than they relate to matters of human safety, and thus should, juvenile dependency cases enjoy a higher priority than criminal and delinquency cases?
- (6) How critical to the maintenance of court operation are other records that relate to the operation of the courts but do not involve actual paper case files, including, by example, records associated with jury service?

Florida's appellate court clerks do not typically compartmentalize case files by case types, as do circuit court clerks. Most commonly, all active files physically within the possession of the appellate clerk, and not within the possession of judges when the matter is under active consideration, are filed by case number without regard for the class of case. As such, unless substantial changes were undertaken by the appellate clerks in the means they store active cases; it is impractical to suggest criteria by which they would identify which of these active cases is vital, or more vital, and thus deserving of heightened attention in the event of an emergency or disaster. Exceptions to this general rule exist. The Supreme Court of Florida, for example, physically separates Bar discipline cases, death penalty cases and other case categories as a matter of administrative convenience.

Separate consideration needs to be directed to records of clerks pertinent to the administration of justice, apart from case files. Records associated with jury service on the trial level and calendaring of trial dockets, for example, require evaluation. Appellate clerks' records not associated with case files that may be considered vital if not stored electronically include, by way of example, minutes from court conferences and administrative orders. Few of these kinds of records are stored only in paper form by the clerks.

Practices of the various court administrators and the Office of the State Court Administrator (OSCA) vary substantially, and attempting to define vital paper records becomes an awkward exercise, as without a comprehensive review of those practices state-wide it is impossible to determine which records maintained by administrators are exclusively paper, and the subject of this task. Among records, if maintained in paper form only, that administrators and OSCA personnel should evaluate in terms of their vital nature, would be:

- (1) Personnel files of current employees
- (2) Property inventory records
- (3) Policies and procedures manuals
- (4) Administrative orders and rules
- (5) Annual reports
- (6) Time and attendance reports
- (7) Procurement/purchase orders/requisitions
- (8) Finance and accounting records
- (9) Budget amendments and allotment balances
- (10) Payroll records

Judges of all Florida courts maintain some of their own records, and among those that should be evaluated in terms of whether they constitute vital records include:

- (1) Calendars of future hearings and trial dockets that are not kept concurrently by the clerk or retained electronically.
- (2) Notes taken by judges on pending cases.
- (3) Memoranda prepared by court staff on active cases, if not stored elsewhere electronically.
- (4) Research files.
- (5) Files maintained by the chief judge.

GUIDELINES

These recommended policies and guidelines are for the purpose of protecting the technology infrastructure of the judicial branch and judicial branch records, and to ensure access to court records in the event of natural disasters, terrorism, biological concerns and extended information system outages.

Administrative Order AOSC01-54 specifically calls for statewide policy and guidance to be developed for the purpose of protecting the courts technology infrastructure and ensuring the backup of critical information both in electronic and paper formats. The spirit of the order also calls for local autonomy in both planning and execution. The policy section offers specific areas that the chief judges of the districts and circuits should address in a formal policy to be developed and executed at the local level. Specific areas to be addressed are given to ensure some level of consistency is given to the protection of court technology and records.

While these guidelines should be achievable with resources and support that exist or likely to be available, additional resources may be necessary to implement the guidelines due to the variety and complexity of technology in the judicial branch. Existing technology is varied throughout the state and may require specific proprietary solutions. Wherever possible, enterprise solutions should be put into practice for greater manageability and consistent application of security measures. In addition, information security is unlike many other critical business functions that the courts are accustomed to fulfilling. 100% security can never be achieved. This is due to the fundamental nature of the task at hand, which is directing limited resources in a manner that minimizes overall risk. What makes information security unique is that a relatively significant risk may or may not require a significant amount of resources to minimize it. Further, not all risks can be altogether eliminated.

(a) Risk Assessment and Security

- (1) 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.
- (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.

(b) Backup Critical Information Electronic and Paper

- (1) 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. These methods shall be documented and tested on a regular basis to ensure availability of court applications and information during an emergency.
- (2) The chief judges of the districts and circuits and each judicial branch entity should implement methods to physically secure paper, monitor and control environmental factors at paper storage sites, develop emergency procedures to protect paper when disaster is imminent, and develop mitigating measures if paper is lost or destroyed.

(c) Information Technology Security Manager

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. All designated ITSMs should be registered with Office of the State Court Administrator, and establish a statewide communication network to share threat information to provide advance warning to the various courts and justice entities in an effort to reduce risk, and manage incidence response. Any issues related to security breaches such as viruses and unauthorized access should be reported to the users' local systems administrator for immediate response. Then the local systems administrator shall report security-related incidents to the designated Information Technology Security Manager who will then coordinate the next steps if required.

(d) Threat Assessment and Response

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. These guidelines should also include measures to protect evidence without further jeopardizing court technology infrastructure. The ITSM's shall be the coordinating entity with law enforcement regarding investigations that involve computer crimes, cyber terrorism, and other technology security related incidents in the courts. The statewide ITSM Group should develop a secure Intranet page where information can quickly be posted, and security patches quickly made available for download. ITSM's should establish a list of local contacts in order to communicate threat information and coordinate efforts with other justice related entities. Security officers should have regular training on laws regarding computer crimes, and investigative techniques in order to properly gather evidence if criminal prosecution is pursued.

(e) Security Management Practices

(1) Systems Development Methodology. New systems development and up grades of existing systems should follow a formal systems methodology, which should include risk analysis and security architecture planning as part of the process.

- (2) Cryptography and Access Controls. Security management practices such as cryptography should be implemented when necessary to ensure confidentiality and integrity of information. Industry standard cryptography methods should be used when confidentiality and integrity of information is vital and required by law, such as sealed electronic records. Access controls should be put into place to control access to specific resources once a user is allowed to enter a system.
- (3) Telecommunications and Network Security. The majority of information system communications occur over distributed network systems. 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.
- (4) Event Logging. 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. Audit and monitoring mechanisms allow for the collection of information to ensure compliance with policy and procedures regarding network security as the greatest security threats are usually within the local organization.
- (5) Vulnerability Analysis. Regular and frequent system vulnerability analysis should be conducted. Part of the analysis should include research of available system patches, research of new or emerging threats that exist, and new filters and virus patches that should be applied.

(f) Backup of Records, Paper and Electronic

The chief judges of the districts and circuits and judicial branch entities should conduct a study regarding which records are stored in electronic format, paper format or both. This will identify where duplication already exists.

(g) Mitigation Measures (Recovery) and Alternate Site Planning

(1) Alternate Site Planning

Alternate technology and facility planning should be a part of the overall disaster recovery plan. There are different levels of alternate site readiness such as:

- (A) HOT Site, which is a fully configured facility, with operational mirror of all technology.
- (B) Warm Site, which is a facility with minimal equipment, software and data must be restored.
- (C) Cold Site, which is an empty facility requiring delivery and installation of technology equipment and restoration of applications and software.
- (D) Multiple Sites, which are distributed production and technology facilities.
- (E) Reciprocal agreement, which is another organization with similar facilities and technology will provide backup operations.

(2) Manual System And Forms

- (A) 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. The need for paper forms to sustain court operations in the event of power failure depends on the severity of the outage. Most court operations experience minor power outages from time to time, which commonly result in a brief interruption of service. This section addresses those circumstances in which the outage is not restored within a few hours, in some cases, or a few days, in others.
- (B) Restoration of a light source is presumed to be a prerequisite before utilization of any of paper forms would be feasible. Restoration of temperature control devices is unlikely to occur before the restoration of power, and to the extent that a specific building does not have operable windows in certain weather conditions it is unlikely that any semblance of normal court activity would resume before power is restored.

(C) By example, the delivery of judicial services by an appellate court might not be substantially undermined if power outages endured for several days. The deliberate pace of appellate proceedings, and the minimal presence of parties and attorneys, contributes to this conclusion. Oral arguments could be rescheduled, and several days' delay in resolving most cases would not significantly prejudice the rights of litigants. Disposition of the emergency matters handled by appellate courts, with rare exception, can be deferred a few days without profound impact on the courts' constituency.

- (D) Operations of many functions of circuit courts cannot be as easily accommodated by loss of power or automated systems. Substantive and procedural due process concerns militate that courts be available regularly for, again by example, first appearance hearings of arrestees and consideration of domestic violence injunctions.
- (E) No effort has been undertaken to make assessments of which of the forms listed below would be essential for an entity of the judicial system to have on hand in the event of power outages. Instead, they are listed, in varying degrees of completeness, so that the responsible officials can make informed judgments about what forms might be deemed essential to have available to ensure continued operations.
- (F) Circuit Court Administrators, OSCA and Appellate Court Marshals
 - (i) Circuit Court Administrators operate somewhat independently, and, as such, the assessment of what paper forms they should consider having on hand might be considered in terms of their functions as would suit the arrangement of the respective offices. A supply of printed forms might be advised for ordering supplies, processing payroll, keeping track of work schedules, submitting mileage reimbursement requests, and the like.
 - (ii) Appellate marshals should consider the need for forms for signing up new employees, for leave and attendance, for requisition forms for purchasing, for accounts payable, for year end financial statements, for legislative packages and for budgeting.

(G) Appellate Court Clerks

A partial list of forms that appellate clerks might consider having on hand in the event of power outage and loss of automation would include:

- (i) Docketing logs, to ensure that incoming motions, notices, briefs and records can be promptly filed, with data input into case management to follow with the restoration of power from the information registered on docketing logs.
- (ii) Disposition forms; to ensure that case dispositions can continue to the extent possible during an outage, with data entry to follow upon restoration of power.
- (iii) Perfection forms; for those courts that no longer maintain paper records of case progress, forms should be devised so that personnel can identify perfected appeals ready for consideration by the court.
- (iv) To the extent that the court is dependent upon automation for case and panel assignments, paper forms for scheduling of cases should be maintained.
- (v) Order copy sets; preferably pre-printed copy sets for the issuance of court orders should be considered, which if necessary could be issued in handwriting or typed manually, in the event the equipment for that was available.

(H) Clerks of the Circuit Court

There is no arm of the judiciary that would face a greater challenge in sustaining operations in the event of power or automation loss for more than a few hours.

Appendix H is a list of forms, some of which would be indispensable to the continued operations of circuit court clerks in the event of power and automation loss. Some of the duties of circuit court clerks embrace functions arguably not contemplated within the term of the judiciary for purposes of this exercise (marriage licensing, for example). This extensive list includes paper forms for some of these clerk functions that might be useful in the event of an extended power outage.

(I) Judges' Offices

The protocols of judges' offices among the different levels of courts, among the circuits and counties, and among those offices within a single county vary substantially, and make an assessment of forms that would be useful to them in the event of a prolonged power/automation outage difficult.

Among the issues that should be considered by the courts is a provision for each judge's office to be equipped to calendar hearings without resort to automated systems, and to issue orders without resort to word processing or electric typewriters. As such, paper calendars and preprinted copy sets for orders should be considered. Some judges in some circuits currently hand-write simple orders on forms, and these forms could enjoy wide use in the event of power outage. Copy sets, or a supply of carbon paper, would be essential with the unavailability of electric duplicating equipment.

(h) Recovery - Paper Records

- (1) Each 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. A recovery plan should include:
 - (A) Instructions on whom to notify in case of emergency to relate details about the nature of the emergency and the level of vulnerability of the records.
 - (B) Assessing the damage to records as soon as possible and taking steps to stabilize the condition of the records so further damage will not occur.
 - (C) Assembling a records recovery team in the event of major records damage to help in stabilizing the condition of the records.
 - (D) Consulting with contractors that provide records disaster recovery services if the damage assessment indicates the need for their expertise.
 - (E) Recovering the records and the information that they contain, or providing replacement of any lost recorded information when recovery is not feasible; and resuming normal business using the recovered records and information.

- (2) The composition of paper makes it vulnerable to water, fire, chemical and biological damage. A very brief overview of recovery techniques is provided. Custodians of judicial records cannot be expected to become experts in sophisticated recovery measures available with current technology; as such, each custodian should develop a professional relationship with a qualified vendor who can assist on short notice to assist in the recovery of damaged paper records.
- (3) Fire damage is either complete, in which recovery is impossible, or edges of paper are damaged, in which event recopying the affected areas is indicated if the paper is unsightly or malodorous.
- (4) Water damage: Mold and adherence occur within 48 hours, and damaged paper must be stabilized promptly. Methods of recovery depend on the type of paper, whether loose or bound, and the size of the affected paper, and include.
- (5) Air Dry create a dry condition and separate pages. Clip papers to monofilament line or interleave pages with paper towels or plain newsprint. Vacuum Dry involves using a special tanker supplied by a recovery company to extract water from large amounts of records.
- (6) Freeze Dry a measure to control the spread of mold spores.
- (7) More detailed explanations of recovery methods are widely available on the Internet. See, for example, http://www.nedcc.org/plam3/tleaf37.htm.

(i) Re-creating Destroyed Paper Records

- (1) The re-creation of destroyed paper case files requires the cooperation of attorneys and parties involved in those cases to provide copies of documents that they have themselves generated or have been created by the court in question. In some types of case files this may not be feasible (for example, criminal traffic files typically are comprised of a uniform traffic citation and perhaps accompanying reports from law enforcement, in which case backup copies should be available from the law enforcement agency.) The orders issued by the state's appellate courts are retained electronically in case management systems, which are backed up offsite.
- (2) Most vital administrative records are maintained electronically (exceptions to this may include personnel files, as distinct from payroll records) and their re-creation in the event of loss is beyond the scope of this section that addresses recreating of destroyed paper records. Successful recreation of paper personnel files would depend upon, in part, the cooperation of employees and the availability of duplicate documentation that might be maintained by other sources.

(j) Recovery - Electronic Records

- (1) Each entity of the judicial branch responsible for court records and administrative records should prepare an electronic records and critical applications recovery plan to establish specific procedures for personnel to follow in the event that an emergency or disaster occurs. A recovery plan should include:
 - (A) Instructions on whom to notify in case of emergency to relate details about the nature of the emergency and the level of vulnerability of the electronic records and information systems.
 - (B) Assessing the damage to data and information systems as soon as possible, and taking steps to stabilize the condition of the equipment or electronic media to avoid further damage.
 - (C) In the event of major records damage or application failure there shall be two teams assembled: A recovery team is needed to focus to salvaging data at the primary site, and a response team is needed to focus on getting technology back up and running perhaps at an alternate site.
 - (D) Consulting with contractors that provide records disaster recovery services if the damage assessment indicates the need for their expertise.
 - (E) Recovering the records and the information that they contain, or providing replacement of any lost recorded information when recovery is not feasible; and resuming normal business using the recovered records and information.

(k) Statewide Security Assessment

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. This effort will assist the Court in evaluating mitigation planning that presently exists, and how best to protect judicial branch records through corrective actions that may be included in future budget processes at the local and state levels. A sample survey is shown in Appendix I. Following this assessment, the council should consider recommendations to the Court for mandatory standards to be followed by all entities of the judicial branch.

(1) Electronic Filing of Court Pleadings

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 A

INSTRUCTIONS FOR PREPARATION OF ADMINISTRATIVE AND EMERGENCY PROCEDURES

(a) Introduction

- (1) The Supreme Court, districts and circuits should develop a set of Administrative and Emergency Procedures. These procedures will provide judges, security, law enforcement, staff, and the public with specific steps necessary to adequately respond to emergencies not requiring the relocation of court operations to alternate facilities.
- (2) These instructions serve as a guide to assist in the development of each court's Administrative and Emergency Procedures. The final layout and the actual content of the procedures should represent what works best for each court.

(b) Instructions for Developing Each Court's Procedures

- (1) Administrative and Emergency Procedures should include specific procedures to follow, information necessary to respond (such as phone numbers, law enforcement / fire / hazard / security / county emergency operations contacts, escape routes, location of supplies, etc.), and the responsibilities of key personnel for the variety of emergency situations that may face each court facility.
- (2) These procedures do not necessarily need to include the procedures for relocating operations to alternate facilities. The issues related to relocating court facilities will be incorporated into a separate Continuity of Operations Plan (COOP).

(3) The procedures should be organized by type of emergency situation. While all possible emergency situations should be considered in procedures, emphasis should be placed on the emergency situations most likely to impact court operations. Such emergencies include, but are not limited to:

- (A) Suspicious Packages
- (B) Natural Disasters / Severe Weather
- (C) Fire
- (D) Gas Leaks
- (E) Bomb Threats
- (F) Chemical Hazards
- (G) Civil Disturbances
- (H) High Profile Cases
- (I) Excessive Number of Cases
- (J) Disruptive Individual: Employee
- (K) Disruptive Individual: Public Citizen
- (L) Loss of Basic Utilities

APPENDIX B

OUTLINE AND SAMPLE OF CONTINUITY OF OPERATIONS PLAN (COOP)

WARNING: This Appendix contains information pertaining to the deployment, mobilization, and tactical operations of the judicial branch in response to emergencies and is exempt from public disclosure under the provisions of section 281.301, Florida Statutes, and Florida Rule of Judicial Administration 2.051

- (a) Table of Contents
- (b) Foreword
 - (1) Provide a foreword from the chief justice or chief judge.
- (c) Section I: Introduction
 - (1) Provide a brief introduction.
- (d) Section II: Concept of Operations (CONOP)
 - (1) In this section consider including the following:
 - (A) An outline of purpose and intentions of the plan.
 - (B) A list assumptions used to develop the plan.
 - (C) Scenarios under which the plan may be activated.
 - (D) Organizational structure of the court.
 - (E) Notification procedures for key staff in all scenarios to include duty and non-duty hours and with or without warning.
 - (F) Documented authorized successors at least three-levels below chief justice or chief judge.
 - (G) Operational hours for emergency and non-emergency functions.
 - (H) Procedures for contacting both essential and non-essential personnel during any warning conditions, this should include checklists, notification lists, and phone trees.

(e) Section III: Responsibilities and Procedures

- (1) In this section consider including the following:
 - (A) Specialized lists of responsibilities based on unique organizational structure to the unit-level.
 - (B) Identification of key staff to support operations and communications procedures to contact and provide information to non-essential staff.
 - (C) Identification of alternate facility.
 - (D) Pre-positioning of emergency operating records and legal and financial documents, regardless of media in which they are contained, essential to the continued functioning of an organization during and after an emergency.
 - (E) Resources necessary to perform essential functions.
 - (F) Pre-packaged supplies, equipment, and other logistical support that will ensure the performance of essential functions.
 - (G) Establishment of provision for continued telecommunications and computer staff support.
 - (H) Policies for the security of primary and alternate facilities during emergency and non-emergency situations that includes provisions for identifying access restrictions. The security procedures should be able to accommodate all-hazards.
 - (I) Initial requirements for receiving, supporting, and relocating the key staff.

(f) Section IV: Phase I – Activation

- (1) This section of the plan should incorporate details to accomplish the general steps associated with the activation phase as presented in the flowchart in Attachment C. The goal should be to have alternate operations as described in phase II below, fully functional within 24 hours of COOP activation.
 - (A) In this section consider including the following:
 - (i) Specific actions to alert and notify key staff, non-essential personnel, and critical customers that COOP activation is imminent
 - (ii) Specific actions to terminate primary operations and activate key staff, communications links, and the alternate facility
 - (iii) Specific actions for an efficient and complete transition of direction and control from primary facility to the alternate facility that includes measures for security at both sites. The procedures should be complementary to the court's Building Evacuation Plans (if these plans are not developed they need to be)
 - (iv) Details regarding notification of key staff when they are not at the primary facility
 - (v) Administrative procedures for travel, transportation, and relocation to the alternate facility
 - (vi) Minimum standards for communication, direction, and control to be maintained until the alternate facility is operational
 - (vii) Procedures for determining whether or not full operations in the primary facility can be reconstituted within 30 days of activation

(g) Section V: Phase II – Alternate Operations

- (1) This section of the plan should incorporate details to accomplish the general steps associated with the alternate operations phase as presented in the flowchart in Appendix C. The goal is to be able to perform the mission essential functions for a period of up to 30 days.
 - (A) In this section consider including the following:
 - (i) Specifics regarding the performance of mission essential functions.
 - (ii) Reestablishment of normal lines of communication to all critical customers and stakeholders.
 - (iii) Assignment of responsibilities to key staff to perform mission essential functions
 - (iv) Determination if current staffing meets the workload to perform mission essential functions, and activation of additional staff as necessary.
 - (v) Additional guidance to all personnel in regards to duration of alternate operations and include pertinent information on payroll, time and attendance, duty assignments, etc.
 - (vi) Preparations for transfer of communications and vital records and databases back to the primary facility. Circumstances may dictate that a long-term (more than 30 days) alternate facility is designated and subsequently occupied.

(h) Section VI: Phase III – Reconstitution and Termination

- (1) This section of the plan should incorporate details to accomplish the general steps associated with the reconstitution and termination phase as presented in the flowchart in Appendix C. The goal is to be able to either transfer back to the primary facility and resume full operations or transfer to a long-term alternate facility and resume full operations.
 - (A) In this section consider including the following:
 - (i) Provide general guidance and policy on ending alternate operations and returning to a non-emergency status at the primary facility or a long-term alternate facility.
 - (ii) Establish specific actions to ensure a timely and efficient transition of communications, direction and control, and transfer of vital records and databases to primary facility.
 - (iii) Develop taskforce to assess all phases and elements of the alternate operations and provide specific solutions to correct any areas of concern.

CONTINUITY OF OPERATIONS PLAN (COOP)

FLORIDA STATE COURTS SYSTEM (NAME OF THE CIRCUIT/DISTRICT)

(<u>Optional:</u> <u>Insert a Seal or Graphic here</u>.)

(Month Year)

WARNING: This Appendix contains information pertaining to the deployment, mobilization, and tactical operations of the judicial branch in response to emergencies and is exempt from public disclosure under the provisions of section 281.301, Florida Statutes, and Florida Rule of Judicial Administration 2.051

TABLE OF CONTENTS

TABLE OF CONTENTS i				
FOREWORD				
SECTION I: INTRODUCTION				
I-1	Purpose		X	
I-2	Applicability	X		
I-3	Superscession	X		
I-4	Authorities	X		
I-5	References		X	
I-6	Policy		X	
SECTION II: CONCEPT OF OPERATIONS (CONOP)				
II-1	Objectives		X	
II-2	Planning Con	X		
II-3	COOP Execut	X		
II-4	Time-Phased	X		
II-5	(Name of the	X		
II-6	Alternate Rela	X		
II-7 II-8	Mission Esser Delineation of	X		
II-8 II-9	Warning Cond	X X		
II-10	Direction and	X		
II-11				
II-12	<u>=</u>			
SECT	ION III: RESP	ONSIBILITIES AND PROCEDURES		
III-1	Key Personne	l and Group Responsibilities and Procedures	X	
111 1	•	ge of the (Name of the Circuit/District)	X	
		Circuit Court Administrator	X	
	c. Emergenc	y Coordinating Officer	X	
	d. Public Inf	ormation Officer	X	
		ergency Management Group	X	
		Judges and Staff	X	
	` '	gency Management Team	X	
шэ		gency Operational Team	X	
III-2 III-3	Personnel Coo	and Databases	X X	
III-4			X X	
III-5				
III-6	7 11			
	J			

SECT	ION IV: PHASE I – ACTIVATION		
IV-1	Alert and Notification Procedures	X	
IV-2	Initial Actions		
IV-3	Activation Procedures Duty Hours		
IV-4	Activation Procedures Non-Duty Hours		
IV-5	Deployment and Departure Procedures – Time-Phased Operations x		
IV-6	Transition to Alternate Operations x		
IV-7	Site-Support Responsibilities	X	
SECT	TON V: PHASE II – ALTERNATE OPERATIONS		
V-1	Execution of Mission Essential Functions	X	
V-2	Establishment of Communications x		
V-3	Relocation Group Responsibilities		
V-4	Augmentation of Staff x		
V-5	AMPLIFICATION OF GUIDANCE TO ESSENTIAL AND NON-ESSEN	TIAL	
	ONNEL X		
V-6	Development of Plans and Schedules for Reconstitution		
	and Termination	X	
SECT	TION VI: PHASE III – RECONSTITUTION AND TERMINA	ATION	
VI-1	Overview	X	
VI-2	Procedures	X	
VI-3	After-Action Review and Remedial Action Plan	X	
	APPENDICES	X	

FORWARD

(Introduction to this COOP by the Chief Judge of the Circuit/District)
(Name of Chief Judge), Chief Judge
(Name of the Circuit/District

SECTION I: INTRODUCTION

I-1 Purpose

This Continuity of Operations Plan (COOP) establishes policy and guidance to ensure the execution of the mission essential functions for the (<u>Name of the Circuit/District</u>) in the event that an emergency in (<u>Name of City</u>), Florida threatens or incapacitates operations, and the relocation of selected personnel and functions of any court facilities in (<u>Name of the Circuit/District</u>) is required. Specifically, this plan is designed to:

- a. Ensure that the (<u>Name of the Circuit/District</u>) is prepared to respond to emergencies, recover from them, and mitigate against their impacts.
- b. Ensure that the (<u>Name of the Circuit/District</u>) is prepared to provide critical services in an environment that is threatened, diminished, or incapacitated.
 - c. (Others as necessary)
- I-2 Applicability and Scope
 - a. This document is applicable to the (Name of the Circuit/District).
- b. Support from other state agencies and local governments as described herein will be coordinated with the responsible office as applicable.
- c. A separate Continuity of Operations Plan (COOP) will be developed for the Florida Supreme Court, each district court, and each circuit court within the State of Florida.
- d. A Continuity of Government (COG), and Concept of Operations (CONOP) Plan will need to be developed for the Florida Supreme Court.

I-3 Superscession

This document supersedes any other documents for the (<u>Name of the Circuit/District</u>) related to emergency operations requiring relocation to alternate facilities.

- I-4 Authorities
 - a. Administrative Order AOSC02-XX, (Title), dated (Month, Day, Year)
 - b. (Others as necessary)
- I-5 References
 - a. (To be determined)

- I-6 Policy
 - a. (<u>To be determined</u>)

SECTION II: CONCEPT OF OPERATIONS (CONOP)

II-1 Objectives

The objective of this COOP is to ensure that a viable capability exists to continue essential court functions across a wide range of potential emergencies, specifically when the primary facility is either threatened or inaccessible. The objectives of this plan include:

- a. Ensure the continuous performance of a court's essential functions/operations during an emergency;
- b. Protect essential facilities, equipment, records, and other assets;
- c. Reduce or mitigate disruptions to operations;
- d. Reduce loss of life, minimize damage and losses;
- e. Identify and designate principals and support staff to be relocated;
- f. Facilitate decision-making for execution of the Plan and the subsequent conduct of operations; and
- g. Achieve a timely and orderly recovery from the emergency and resumption of full service to all customers.

II-2 Planning Considerations and Assumptions

- a. In accordance with State guidance and emergency management principles, a viable COOP capability:
 - Must be maintained at a high-level of readiness;
 - Must be capable of implementation both with and without warning;
 - Must be operational no later than three hours after activation;
 - Must maintain sustained operations for up to 30 days; and
 - Should take maximum advantage of existing State or Federal and local government infrastructures.

The following assumptions were used as a basis of design for the Plan's concept of operations and implementation procedures:

a. (<u>List All Assumptions</u>)

II-3 COOP Execution

- a. Emergencies, or potential emergencies, may affect the ability of the (Name of the Circuit/District) to perform its mission essential functions from any or all primary court facilities in counties included in the (Name of the Circuit/District). The following are scenarios that could mandate the activation of the (Name of the Circuit/District) COOP.
 - Any primary court facility in the (<u>Name of the Circuit/District</u>) is closed to normal business activities as a result of an event or credible threats of an event that would preclude access or use of the court facility and the surrounding area.
 - Any city in the (<u>Name of the Circuit/District</u>) is closed to normal business
 activities as a result of a widespread utility failure, natural disaster,
 significant hazardous material incident, civil disturbance, or terrorist or
 military attacks. Under this scenario there could be uncertainty regarding
 whether additional events such as secondary explosions, or cascading
 utility failures could occur. If multiple court facilities are located in any of
 the cities or metropolitan areas in the (<u>Name of the Circuit/District</u>),
 activation of COOP contingencies to address such scenarios may be
 necessary.
- b. In an event so severe that normal operations are interrupted, or if such an incident appears imminent and it would be prudent to evacuate any primary court facility or city in the (Name of the Circuit/District) as a precaution, the (Chief Judge or Other Designated Person or Persons), may activate the (Name of the Circuit/District) COOP. The relevant alternate facility (Alternate facilities should be predetermined and listed in an appendix) will be activated, if necessary and at the discretion of the (Chief Judge or Other Designated Person or Persons).
- c. (The Court Emergency Management Group (CEMG) or other predetermined group) for the (Name of the Circuit/District) will gather at the (Name of Alternate Facility or Name of Predetermined Secure Location). The (CEMG or other predetermined group) will ensure the mission essential functions of the closed primary facility are maintained and capable of being preformed using the relevant alternate facility until the assumption of full operations is re-established at the primary facility.

d. The (Name of the Circuit/District) (CEMG or other predetermined group) may be supplemented by selected staff from appropriate State, County, or other agencies. The (Name of the Circuit/District) (CEMG or other predetermined group) will serve as an initial relocation team for COOP activation or potential activation. The (CEMG or other predetermined group) will either relocate temporarily to the relevant alternate facility, if necessary, or operate remotely from a (Predetermined Secure Location) serving as an assembly site. The (CEMG or other predetermined group) will be responsible to continue mission essential functions of the (Name of the Circuit/District) within six hours and for a period up to seven days pending regaining access to the (Name of the Courthouse) or the occupation of the relevant alternate.

- e. All judges and staff necessary to perform the mission essential functions of the (Name of the Circuit/District) will need to be contacted and advised to report to either the relevant alternate facility, predetermined secure location, or other location as determined by the (CEMG or other predetermined group). Clear instructions as to the actions necessary to be preformed by each of these judges and staff should be predetermined by the (CEMG or other predetermined group) provided to them by the CEMG.
- f. Incidents could occur with or without warning and during duty or non-duty hours. Whatever the incident or threat, the (Name of the Circuit/District) COOP will be executed in response to a full-range of disasters and emergencies, to include natural disasters, terrorist threats and incidents, and technological disruptions and failures.
- g. It is expected that, in most cases, the (Name of the Circuit/District) will receive a warning of at least a few hours prior to an incident. Under these circumstances, the process of activation would normally enable the partial, limited, or full activation of the (Name of the Circuit/District) COOP with a complete and orderly alert, notification of all personnel, and activation of the (CEMG or other predetermined group).
- h. Without warning, the process becomes less routine, and potentially more serious and difficult. The ability to execute the (Name of the Circuit/District) COOP following an incident that occurs with little or no warning will depend on the severity of the incident's impact on the physical facilities, and whether the (Name of the Circuit/District) personnel are present in the effected facility or in the surrounding area.
- Positive personnel accountability throughout all phases of emergencies, including COOP activation, is of utmost concern, especially if the emergency occurs without warning, during duty hours. Court facility Safety and Evacuation Plans, Administrative and Emergency Procedures, and Section/Office COOP Implementation Plans should provide for such accountability.

II-4 Time-Phased Implementation

The purpose of a Time-Phased Implementation is to maximize the preservation of life and property in the event of any natural or man-made disaster or threat thereof, by making the best use of available personnel, equipment, facilities, and other resources. This Plan is designed to provide a flexible response in all-hazards environment. The degree to which this Plan is implemented depends on the type and magnitude of the event or threat. The extent to which this will be possible will depend on the emergency, the amount of warning received, whether personnel are on duty or off-duty at home or elsewhere, and possibly, the extent of damage to primary court facilities and their occupants. The Disaster Magnitude Classification definitions will be used to determine the execution level of the (Name of the Circuit/District) COOP. These levels of disaster are defined as:

- Minor Disaster. Any disaster that is likely to be within the response capabilities of local government and results in only minimal need for State or federal assistance.
- Major Disaster. Any disaster that will likely exceed local capabilities and require a
 broad range of State and federal assistance. The Federal Emergency Management
 Agency (FEMA) will be notified and potential federal assistance will be
 predominantly recovery-oriented.
- Catastrophic Disaster. Any disaster that will require massive State and federal assistance, including immediate military involvement. Federal assistance will involve response as well as recovery needs.

(Details regarding the timed-phase implementation will need to be developed)

II-5 (Name of the Circuit/District) Essential Judges and Staff

- a. (Name of the Circuit/District) judges and staff who are relocated under this plan to the selected alternate facility are known collectively as the Essential Judges and Staff (EJS). The EJS must be able to continue operations and the performance of mission essential functions for up to 30 days with resource support (List of the Essential judges and staff (EJS) for in each county/primary court facility should be predetermined and listed in an appendix).
- b. Each EJS member will be assigned to one or both of the following two categories; however, not all (Name of the Circuit/District) judges and staff will necessarily be on the EJS:

- (1) Emergency Management Team. These are EJS members who will deploy and relocate to either the selected alternate facility or the relevant assembly site to provide direction and control, prepare the selected alternate facility, and establish the operational capability of the alternate facility within six hour of activation, and earlier in a warning scenario.
- (2) <u>Emergency Operational Team</u>. These are judges and staff who comprise the balance of the EJS, consisting of key judges and staff that will relocate to the selected alternate facility. These judges and staff are anticipated to be fully operational within 12 hours of activation or earlier in a warning scenario.
- c. Since alternate facility space and support capabilities may be limited, the membership of the EJS may need to be restricted to only those personnel who possess the skills and experience needed for the execution of mission essential functions.
- d. (Name of the Circuit/District) judges and staff who are not designated EJS members may be directed to move to other facilities or duty stations, or may be advised to remain at or return home pending further instructions. COOP activation will not, in most circumstances, affect the pay and benefits of either EJS members or other (Name of the Circuit/District) judges and staff.

II-6 Alternate Relocation Point

- a. The determination of the alternate relocation point (ARP) will be made at the time of activation by the (Chief Judge or Other Designated Person or Persons) in consultation with the (Chief Judge or Other Designated Person or Persons) and will be based on the incident, threat, risk assessments, and execution timeframe. If only the court facility is inaccessible and there is no threat in the surrounding area, the primary alternate facility (Alternate facilities should be predetermined and listed in an appendix). If the surrounding area is threatened or the primary alternate facility is not available, a secondary facility will need to be chosen.
- A list of possible secondary alternative facilities should be maintained to assist in the decision-making process if needed (<u>The list should be included as an appendix</u>).
- c. To ensure the adequacy of assigned space and other resources, the all possible alternate facilities included in the appendices will, at a minimum, be reviewed by the (Name of the Circuit/District) ECO annually. The (Chief Judge or Other Designated Person or Persons) will be advised of the results of this review and any updates to the ARP information.

II-7 Mission Essential Functions

It is important to establish priorities before an emergency to ensure that the relocated staff can complete the mission essential functions. All (<u>Designated Persons</u>) shall ensure that mission essential functions can continue or resume as rapidly and efficiently as possible during an emergency relocation. Any task not deemed mission essential must be deferred until additional personnel and resources become available (<u>A listing of detailed mission</u> essential functions must be included as an appendix).

II-8 Delineation of Mission Essential Functions

If the (Name of Circuit/District) COOP cannot be implemented for any reason, the (Name of the Circuit/District) function will revert to the Florida Supreme Court. The Florida Supreme Court will then determine which Florida State Court or other organization will perform this critical mission for Florida. The following delineation structure is provided for guidance to The Florida Supreme Court to support the Justices' decision making process in the event that this catastrophic scenario arises.

- a. If the (Name of Circuit/District) COOP cannot be implemented for any reason, the Florida Supreme Court will assume responsibility for the ensuring the continuous performance of the (Name of the Circuit/District) mission essential functions.
- b. If for any reason the Florida Supreme Court cannot assume or maintain responsibility for the execution of the (Name of the Circuit/District) COOP and continuous performance of mission essential functions, the (Name of a Neighboring Circuit/District) will be prepared to assume responsibility for the (Name of the Circuit/District) mission essential functions.
- c. If for any reason (Name of a Neighboring Circuit/District) cannot assume or maintain responsibility for the execution of the (Name of the Circuit/District) COOP and continuous performance of mission essential functions, the (Name of a Secondary Neighboring Circuit/District) will be prepared to assume responsibility for the (Name of the Circuit/District) mission essential functions.

II-9 Warning Conditions

a. With Warning. It is expected that, in most cases, the (Name of the Circuit/District) will receive a warning of at least a few hours prior to an event. This will normally enable the full execution of the COOP with a complete and orderly alert, notification, and deployment of the Emergency Management Team to an assembly site or a pre-identified ARP.

- b. Without Warning. The ability to execute the COOP following an event that occurs with little or no warning will depend on the severity of the emergency and the number of personnel that survive. If the deployment of the EJS is not feasible because of the loss of personnel, temporary leadership of the (Name of the Circuit/District) will be passed to the Florida Supreme Court as explained in subparagraph II-8 above.
 - (1) <u>Non-Duty Hours</u>. (<u>Name of the Circuit/District</u>) judges and staff should be able to be alerted and activated to support operations for the duration of the emergency (<u>The necessary information and means of communicating with judges and staff should be developed and outlined in an appendix).</u>
 - (2) <u>Duty Hours</u>. If possible, the COOP will be activated and available members of the EJS will be deployed as directed to support operations for the duration of the emergency.

II-10 Direction and Control

- a. Authorized (Name of the Circuit/District) successors to the Chief Judge are listed in Appendix (X) (This appendix X should be developed and included). Lines of succession shall be maintained by all (Name of the Circuit/District) organizational elements, reporting to the Chief Judge to ensure continuity of mission essential functions. Successions should be provided to a minimum depth of three at any point where policy and directional functions are carried out.
- b. Each (<u>Name of the Circuit/District</u>) organizational element shall pre-delegate authorities for making policy determinations and decisions. All such pre-delegations will specify what the authority covers, what limits may be placed upon exercising it, who (by title) will have the authority, and under what circumstances (This appendix should be developed and included).
- c. The (<u>Chief Judge or Other Designated Person or Persons</u>) for the (<u>Name of the Circuit/District</u>) may order activation of the (<u>Name of the Circuit/District</u>) COOP Plan.
- d. The CEMG and the Emergency Management Team, if pre-deployed, may be requested by the (<u>Chief Judge or Other Designated Person or Persons</u>) to disseminate (<u>Name of the Circuit/District</u>) COOP guidance and direction during the activation and relocation phases. Pending the activation of the COOP, the CEMG and the Emergency Management Team will monitor the situation and assist in the notification process as necessary.

e. When executed, the appropriate County Emergency Operations Center should be notified and requested to provide any previously agreed upon assistance to (Name of the Circuit/District). (An appendix outlining the assistance to be provided by the County Emergency Operations Center should be developed with the

II-11 Operational Hours

developed and included).

- a. During COOP contingencies, the (<u>Chief Judge or Other Designated Person or</u> Persons) will determine the hours of work for the EJS.
- b. Certain members of the EJS must be prepared to support a 24-hour-per-day, 7-day-per-week operation.

II-12 Alert and Notification

- a. <u>Alert Procedures</u>. If the situation allows for warning, judges and staff may be alerted prior to activation of the COOP. In all situations allowing for an alert the procedures must include notification to the Emergency Coordinating Officer of the Florida judicial branch.
 - (1) Information and guidance for (<u>Name of the Circuit/District</u>) judges and staff will normally be passed telephonically using an emergency notification telephone tree/cascade (<u>The necessary information and means of communicating with judges and staff should be developed and outlined in an <u>appendix</u>). Depending on the situation, current information may also be available via:</u>
 - (A Florida Supreme Court hotline if approved and developed).
 - (The (Name of the Circuit/District) hotline if approved and developed).
 - (Announcements to local radio and TV stations if approved and developed).
 - (Other means if approved and developed).
 - (2) Judges and staff should listen for specific instructions. All judges and staff should remain at their office or home until specific guidance is received.
 - (3) The (<u>Chief Judge or Other Designated Person or Persons</u>) will direct the activation of the (<u>Name of the Circuit/District</u>) COOP.

- b. <u>Notification Procedures</u>. Upon notification to activate the (<u>Name of the Circuit/District</u>) COOP:
 - (1) The (<u>Chief Judge or Other Designated Person or Persons</u>) will notify the (<u>Circuit Court Administrator for the (Name of the Circuit)</u>, the <u>Marshal of the (Name of the District or Other Designated Person or Persons</u>)) of the current situation and that the COOP is being activated.
 - (2) The (<u>Circuit Court Administrator for the (Name of the Circuit) or Marshal of the (Name of the District or Other Designated Person or Persons</u>)) will notify the Emergency Coordinating Officer, if other than himself/herself, and the primary staff (i.e. staff serving in the EJS) using the telephone tree or other available means of communication.
 - (a) The primary staff then initiate their respective COOP notification cascade and contact each person in their chain relaying the information and guidance provided by the (Circuit Court Administrator for the (Name of the Circuit) or Marshal of the (Name of the District or Other Designated Person or Persons)).
 - (b) The primary staff will make a second attempt to contact those individuals who were not initially available. If this attempt is unsuccessful, the primary staff will leave a message or send a page.
 - (c) Once initial contact is made (message left/page sent), primary staff call the (<u>Circuit Court Administrator for the (Name of the Circuit) or Marshal of the (Name of the District or Other Designated Person or Persons)</u>) and report status of cascade, including personnel not contacted.
 - (d) The (<u>Circuit Court Administrator for the (Name of the Circuit) or Marshal of the (Name of the District or Other Designated Person or Persons</u>)) will in turn report status to the (<u>Chief Judge or Other Designated Person or Persons</u>) via telephone or other means of available communication.
 - (e) For personnel not initially contacted, once the message or page is received, they should immediately contact the primary staff who contacted them.
 - (f) Notification may be via personal contact, telephone, cell phone, pager, radio and TV broadcasts, or a combination thereof.
 - (g) When a call or other notification is received by anyone in a calling cascade, the information given by the primary staff should be carefully

recorded to ensure that it is passed accurately to the next person in the cascade.

- (h) The primary staff will notify the (<u>Circuit Court Administrator for the (Name of the Circuit) or Marshal of the (Name of the District or Other Designated Person or Persons)</u>) upon completion of their notification process.
- (i) The primary staff will report all unsuccessful contact attempts to the (<u>Circuit Court Administrator for the (Name of the Circuit) or Marshal of the (Name of the District) or Other Designated Person or Persons)</u> after relocation has been affected.
- (3) The Emergency Coordinating Officer of the Florida judicial branch will notify the Chief Justice of the Florida Supreme Court; the State Courts Administrator; and the State of Florida Emergency Operations Center that an emergency relocation has been affected in the (Name of the Circuit/District) as specified in the (Name of the Circuit/District) COOP.

SECTION III: RESPONSIBILITIES AND PROCEDURES

III-1 Key Personnel and Group Responsibilities and Procedures

Note: In this section you will need to outline the responsibilities and procedures necessary for key personnel and groups to perform for successful activation of the COOP and for successful performance of the mission essential functions under COOP operations. List provided below should be contracted or expanded as necessary.

- a. Chief Judge of the (Name of the Circuit/District).
- b. Marshal/Circuit Court Administrator.
- c. Emergency Coordinating Officer.
- d. Public Information Officer.
- e. Court Emergency Management Group.
- f. Essential Judges and Staff.
 - (1) Emergency Management Team.
 - (2) Emergency Operational Team.

III-2 Personnel Coordination

Note: This section should provide guidance in personnel issues for successful activation of the COOP and for successful performance of the mission essential functions under COOP operations. The verbiage provided below should be contracted or expanded as necessary.

- a. Only judges and personnel who are needed for the continuous execution of mission essential functions will be included on the list of Essential Judges and Staff (EJS).
- b. Following activation and deployment of the EJS, additional personnel may be contacted to augment operations at the alternate relocation point (ARP).
- c. All requests for augmentation of the EJS must be coordinated through the Chief Judge of the (Name of the Circuit/District).

d. During COOP operations, personnel not activated as members of the EJS, will be provided information on their status by (develop means to accomplish this task). The Emergency Coordinating Officer will be responsible for providing and disseminating the most current information via (developed means).

III-3 VITAL RECORDS AND DATABASES

- a. One (<u>Name of the Circuit/District</u>) COOP objective is to ensure the protection of vital records, regardless of media type, that are needed to support mission essential functions under all emergency conditions.
- b. Types of vital records and databases may include:
 - (1) List the types of vital records and databases that are applicable.

III-4 DRIVE-AWAY KITS AND BLACK-BAGS

- a. The (<u>Designated Person or Persons</u>) is responsible for providing guidance to staff on the requirement for and the contents of these kits, which may contain such items as software, databases, publications, laptop computers, etc. Checklists may need to be used to help ensure the inclusion of all necessary contents.
- b. It is strongly encouraged that essential items and data be pre-positioned at the intown ARP or other off-site location instead of being carried in a drive-away kits, because EJS may be at home when the order to deploy is received and access to the drive-away kits may be difficult or impossible.
- c. Items to consider including in these kits might include:
 - (1) Rules of Court should be in Black-Bag.
 - (2) Tape Recorder and Tapes should be in Black-Bag.
 - (3) Batteries.
 - (4) List of what positions have to be filled to hold a court hearing need to be predetermined and included in the in the Black-Bag.
 - (5) Laptop with all necessary forms on a CD should be considered to include in the Black-Bag.
 - (6) Normal office supplies can be purchased at a local office supply store after an emergency. May only include enough supplies for a 24 hour period in the Black-Bag.

(7) Have a laundry list of all necessary office supplies in the Black-Bag.

III-5 TELECOMMUNICATIONS AND INFORMATION SYSTEMS SUPPORT

- a. Telecommunications capabilities at the potential alternate facilities are sufficient for the performance of mission essential functions under the COOP. Information systems support at the potential alternate facilities will be provided by (<u>Designated Person or Persons</u>) who is a member of the EJS. Mobile communications support will be provided by (<u>Designated Person or Persons</u>).
- b. It is imperative that each Section and Office ensure that unique or critical information system requirements are considered in planning and, if appropriate, are identified as capabilities to be provided by support organizations at the potential alternate facilities.
- c. Items to consider during the planning process might include:
 - (1) Plans should address all three types of communication (Internal, External, Media).
 - (2) Plans should include the development of a telephone trees.
 - (3) Plans should consider use of a Hotline housed in a secondary location.
 - (4) Plans should consider radio communications using available staff with radios (SA investigators, bailiffs, facility security, HAMM radio operators, etc.).
 - (5) Plans should recognize different needs for a one hour emergency to an extended emergency.
 - (6) Plans should consider the use of a communication center to serve as a hub for communication needs of all local users.
 - (7) Plans should develop a plan when all communications systems are unavailable (i.e. a Comms-Out Plan).
 - (8) At a minimum, all members of the EJS are suggested to have pagers.

III-6 SECURITY AND ACCESS CONTROLS

- a. The (CEMG or other predetermined group) will ensure that the (Name of the Circuit/District) COOP and the evacuation plans for each court facility are complementary and coordinated if a COOP activation is required.
- b. The (<u>Designated Person or Persons</u>) will ensure all necessary security and access controls are provided at the alternate court facility. Also, the (<u>Designated Person or Persons</u>) will ensure the primary court facility is secured during COOP operations.
- c. Items to consider during the planning process might include:
 - Plans should address security issues regarding the transporting of inmates.
 - Plans may want to consider the utilizing video technology if available.
 - Plans should establish a goal of duplicating security established at the primary facility.
 - Video technology and the establishment of MOA/MOU's with a vender could prove valuable in addressing security issues.
 - Plans could address security issues by developing procedures in which hearings are held in the local jails.

SECTION IV: PHASE I - ACTIVATION

In general, the following procedures are to be followed in the execution of the (Name of the Circuit/District) COOP. The extent to which this will be possible will depend on the emergency, the amount of warning received, whether personnel are on duty or off-duty, and the extent of damage to the effected court facilities and its occupants. This Plan is designed to provide a flexible response to multiple events occurring within a broad spectrum of prevailing conditions. The degree to which this Plan is implemented depends on the type and magnitude of the events or threats thereof.

IV-1 Alert and Notification Procedures

- a. The (Name of the Circuit/District) notification process as related to COOP activation should, if necessary, allow for a smooth transition of the Essential Judges and Staff to an alternate facility to continue the execution of mission essential functions across a wide range of potential emergencies. Notification may be in the form of:
 - (1) A COOP alert to the Essential Judges and Staff and all non-essential (Name of the Circuit/District) employees that relocation is imminent.
 - (2) An announcement of a (Name of the Circuit/District) COOP activation that directs the Emergency Management Team to report to an assembly site or a designated alternate relocation point (ARP), and provides instructions regarding movement, reporting, and transportation details to an assembly site or a designated ARP.
 - (3) Instructions to the Emergency Operational Team to report for departure and relocation to a designated ARP, when selected and prepared, and instructions to non-essential employees.
- b. Upon receipt of a COOP alert from the (<u>Designated Person or Persons</u>), or a designated successor, the (<u>Circuit Court Administrator for the (Name of the Circuit)</u> or Marshal of the (<u>Name of the District</u>) or Other Designated Person or <u>Persons</u>), notifies the the (<u>Circuit Court Administrator for the (Name of the Circuit)</u> or Marshal of the (<u>Name of the District</u>) or Other Designated Person or <u>Persons</u>) who, in turn, notify staff using their internal telephone notification cascades. Notification may be via personal contact, telephone, cell phone, pager, radio and TV broadcasts, or a combination thereof.
- c. The (<u>Designated Person or Persons</u>) notifies the appropriate County Emergency Operations Center, and Judicial Branch Emergency Coordinating Officer that an emergency relocation of the (<u>Name of the Circuit/District</u>) is anticipated or is in progress.

IV-2 Initial Actions

a. Based on the situation and circumstance of the event, the (<u>Designated Person or Persons</u>) will evaluate the capability and capacity levels required to support the current mission essential functions of the effected court facilities and select an appropriate ARP.

- b. The (<u>Designated Person or Persons</u>) directs the immediately deploy of the Emergency Management Team to an assembly site or the designated ARP.
- c. The (<u>Designated Person or Persons</u>) coordinates the immediately deploy of the Emergency Management Team to an assembly site or the designated ARP.
- d. The (<u>Designated Person or Persons</u>) notifies the (<u>Designated Person or Persons</u>) designated ARP Facility Manager to expect the relocation of the (<u>Name of the Circuit/District</u>) court facility.
- e. The (<u>Designated Person or Persons</u>) prepares the ARP for (<u>Name of the Circuit/District</u>) court operations.
- f. The (<u>Designated Person or Persons</u>) provides instructions and guidance on operations and the location of the ARP.
- g. The (<u>Designated Person or Persons</u>) provides regular updates to the (<u>Chief Judge</u> or Other Designated Person or Persons) regarding ARP activation.
- h. The (<u>Designated Person or Persons</u>) notifies the appropriate County Emergency Operations Center, and Judicial Branch Emergency Coordinating Officer that an emergency relocation of the (<u>Name of the Circuit/District</u>) is anticipated or is in progress.
- i. All (<u>Designated Person or Persons</u>) initiate their respective COOP notification cascade. After the cascades are complete, the results, including individuals not contacted are reported to the (<u>Designated Person or Persons</u>).
- j. The Essential Judges and Staff members report to an assembly site or deploy to the designated ARP to assume (<u>Name of the Circuit/District</u>) court facility mission essential functions.
- k. All (<u>Designated Person or Persons</u>) who have established drive-away kits ensure that they are complete, with current documents and equipment, and commence movement of the resources.
- l. All (<u>Designated Person or Persons</u>) assemble the remaining documents and other assets as required for the performance of mission essential functions and begin preparations for the movement of these resources.

- m. All personnel and sections of the effected court facility or facilities should implement normal security procedures for areas being vacated.
- n. The security personnel as the effected court facility should take appropriate measures to ensure security of the effected court facilities and equipment or records remaining in the building.

IV-3 Activation Procedures Duty Hours

- a. The (<u>Designated Person or Persons</u>) notifies the (<u>Designated Person or Persons</u>) of the emergency requiring activation of the (Name of the Circuit/District) COOP.
- b. The (<u>Designated Person or Persons</u>) activates the (<u>Name of the Circuit/District</u>) COOP and notifies the appropriate ARP Facility Manager.
- c. The (<u>Designated Person or Persons</u>) directs (<u>Designated Person or Persons</u>) to begin movement of the Emergency Management Team to an assembly site or to the designated ARP facility immediately.
- d. The Emergency Operational Team immediately deploys to an assembly site or a designated ARP to assume mission essential functions.
- e. The tasks in Section IV-2 Initial Actions are completed in their entirety.

IV-4 Activation Procedures Non-Duty Hours

- a. The (<u>Designated Person or Persons</u>) notifies the (<u>Designated Person or Persons</u>) of the emergency requiring activation of the DEM COOP Plan.
- b. The (<u>Designated Person or Persons</u>) activates the (<u>Name of the Circuit/District</u>) COOP and notifies the appropriate ARP Facility Manager.
- c. The (<u>Designated Person or Persons</u>) directs (<u>Designated Person or Persons</u>) to begin movement of the Emergency Management Team to an assembly site or to the designated ARP facility immediately.
- d. The Emergency Management Team immediately deploys to an assembly site or a designated ARP to assume mission essential functions.
- e. The Emergency Operational Team and other employees are directed to remain at home pending further guidance.
- f. The tasks in Section IV-2 Initial Actions are completed in their entirety.

IV-5 Deployment and Departure Procedures – Time-Phased Operations

Allowances for partial pre-deployment of any mission essential functions which are critical to operations will be determined by the (<u>Designated Person or Persons</u>) at the time the (<u>Name of the Circuit/District</u>) COOP activation is directed. This determination will be based on the event or the level of threat. The following actions establish general administrative procedures to allow for travel and transportation to the ARP. Specific instructions will be provided at the time a deployment is ordered.

- a. The (<u>Designated Person or Persons</u>) directs the (<u>Designated Person or Persons</u>) to begin deployment of the Emergency Management Team and the select Emergency Operational Team members to the ARP.
- b. Emergency Management Team. The Emergency Management Team is directed by the (<u>Designated Person or Persons</u>) to either relocate to a designated assembly site or an ARP. Team members should ensure that they have their official driveaway kits and the personal preparedness bags. This team will most likely use privately owned vehicles for transportation to the designated facility after marshalling at a pre-determined assembly site. Specific instructions will be provided at the time of activation.
- c. <u>Emergency Operational Team</u>. The Emergency Operational Team members immediately begin movement taking with them all office drive-away kits, if applicable, not already transported by the members of the Emergency Management Team and their personal preparedness bags. This team will most likely use privately owned vehicles for transportation to the designated facility. Specific instructions will be provided at the time of activation.
- d. Non-Essential Personnel. Non-essential personnel present at the effected court facility at the time of an emergency notification will be directed to proceed to their homes to await further instructions. At the time of notification, any available information regarding routes that should be used to depart the court facility or other appropriate safety precautions. During non-duty hours, non-essential personnel will remain at their homes pending further guidance.

IV-6 Transition to Alternate Operations

a. Following the activation of the (Name of the Circuit/District) COOP and establishment of communications links with the (Designated Person or Persons) and the Emergency Management Team at an assembly site, the (Designated Person or Persons) or his designated successor orders the cessation of operations at the primary court facility.

- b. The (<u>Designated Person or Persons</u>) notifies the appropriate County Emergency Operations Center, and Judicial Branch Emergency Coordinating Officer that an emergency relocation of (<u>Name of the Circuit/District</u>) court facility is complete and provides contact numbers.
- c. As appropriate, press, news media, outside customers, vendors and other service providers are notified by the Public Information Officer that the (Name of the Circuit/District) has been temporarily relocated.

IV-7 SITE-SUPPORT RESPONSIBILITIES

Following notification that a relocation of the (Name of the Circuit/District) court facility has been ordered or is in progress, the appropriate ARP Facility Manager will implement (Name of the Circuit/District) COOP Site-Support Procedures and prepare for the activation of the (Name of the Circuit/District) COOP and to receive the Emergency Management Team within six hours and the Emergency Operational Team within 12 hours.

SECTION V: PHASE II - ALTERNATE OPERATIONS

V-1 EXECUTION OF MISSION ESSENTIAL FUNCTIONS

Upon activation, the Emergency Management Team will begin providing support for the following functions:

- a. Monitor and assess the situation that required the relocation;
- b. Monitor the status of personnel and resources;
- c. Establish and maintain contact with the appropriate County Emergency Operations Center and the Judicial Branch Emergency Coordinating Officer, or other designated person;
- d. Plan and prepare for the restoration of operations at the (Name of the Circuit/District) court facility of other long-term facility.

V-2 Establishment of Communications

- a. The (<u>Designated Person or Persons</u>) will ensure all necessary and preplanned communications systems are established, adequate, and functioning properly; and
- b. The (<u>Designated Person or Persons</u>) will service and correct any faulty or inadequate communications systems.

V-3 Relocation Group Responsibilities

- a. <u>Emergency Management Team Responsibilities</u>. As soon as possible following their arrival at the designated ARP or pre-identified assembly site in the Tallahassee vicinity, the A-Team members will begin providing support for the following functions:
 - (1) Coordinate transition of the (<u>Name of the Circuit/District</u>) mission essential functions from the Emergency Operational Team to the reconstituted (<u>Name of the Circuit/District</u>) court facility of other long-term facility.
- b. <u>Essential Judges and Staff Responsibilities</u>. As soon as possible following their arrival at the designated alternate facility, the Emergency Operational Team members will begin providing support for the following functions:
 - (1) The (<u>Designated Person or Persons</u>) will disseminate administrative and logistics information to the Essential Judges and Staff upon arrival. This information should generally cover the operational procedures for the next 30 days.

The Essential Judges and Staff will be directed to the assigned temporary courtrooms and work locations.

- (2) The Essential Judges and Staff will receive continual briefings and updates from the (Designated Person or Persons).
- (3) The Essential Judges and Staff will perform the mission essential functions of the effected (Name of the Circuit/District) court facility as predetermined and prearranged through the efforts of the Court Emergency Management Group.

V-4 AUGMENTATION OF STAFF

- a. If it becomes evident that the Essential Judges and Staff cannot ensure the continuous performance of mission essential functions, the (<u>Designated Person or Persons</u>) will determine the positions necessary to ensure the continuous performance of mission essential functions.
- b. The (<u>Designated Person or Persons</u>) will then ensure that the identified positions are staffed with individuals who have the requisite skills to perform the tasks.
- V-5 Amplification of Guidance to Essential and Non-Essential Personnel
 - a. The (<u>Designated Person or Persons</u>) will develop informative Memorandum for dissemination to all (<u>Name of the Circuit/District</u>) employees regarding the duration of alternate operations, pertinent information on payroll, time and attendance, duty assignments, and travel authorizations and reimbursements.
 - b. The (<u>Designated Person or Persons</u>) will approve this Memorandum and the (<u>Designated Person or Persons</u>) will then distribute the document to the relocated personnel and the non-essential staff through appropriate media and other available sources.
- V-6 Development of Plans and Schedules for Reconstitution and Termination
 - a. The (<u>Designated Person or Persons</u>) will develop Reconstitution and Termination Plans and Schedules to ensure an orderly transition of all (<u>Name of the Circuit/District</u>) functions, personnel, equipment, and records from the temporary alternate location to a new or restored court facility.
 - b. The (<u>Designated Person or Persons</u>) will approve the plans and schedules prior to the cessation of operations.
 - c. The (<u>Designated Person or Persons</u>) will oversee the Reconstitution and Termination process.

SECTION VI: PHASE III - RECONSTITUTION AND TERMINATION

VI-1 Overview

Within 24 hours of an emergency relocation, the (<u>Designated Person or Persons</u>), will initiate operations to salvage, restore, and recover the effected court facilities after the approval of the local and Federal law enforcement and emergency services involved. Reconstitution procedures will commence when the (<u>Designated Person or Persons</u>) ascertain that the emergency situation has ended and is unlikely to recur. Once this determination has been made, one or a combination of the following options may be implemented, depending on the situation.

- a. Continue to perform mission essential functions at the ARP for up to 30 days.
- b. Begin an orderly return to the effected court facility and reconstitute full operations.
- c. Begin to establish a reconstituted court facility in some other facility in the (Name of the City), Florida vicinity.

VI-2 Procedures

Upon a decision by the (<u>Designated Person or Persons</u>) that the court facility can be reoccupied, or that a different facility will be established as a new court facility:

- a. The (<u>Designated Person or Persons</u>), will oversee the orderly transition of all court functions, personnel, equipment, and records from the ARP to a new or restored court facility.
- b. Prior to relocating back to the primary court facility or another building, the (<u>Designated Person or Persons</u>) will conduct appropriate security, safety, and health assessments for suitability.
- c. When necessary equipment and documents are in place at the new or restored court facility, the staff remaining at ARP will transfer mission essential functions and resume normal operations.

VI-3 After-Action Review and Remedial Action Plan

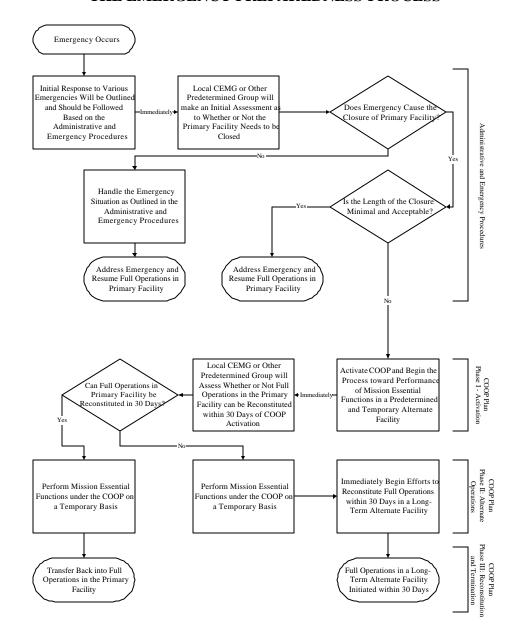
a. An After-Action Review information collection process will be initiated prior to the cessation of operations at the ARP. The information to be collected will, at a minimum, include information from any employee working during the (Name of the Circuit/District) COOP activation and a review of the strengths and weaknesses at the conclusion of the operations.

b. The information should be incorporated into a COOP Remedial Action Plan. Recommendations for changes to the (Name of the Circuit/District) COOP and any accompanying documents will be developed and incorporated into the COOP Annual Review Process.

Note: Include Appendices to the COOP as necessary.

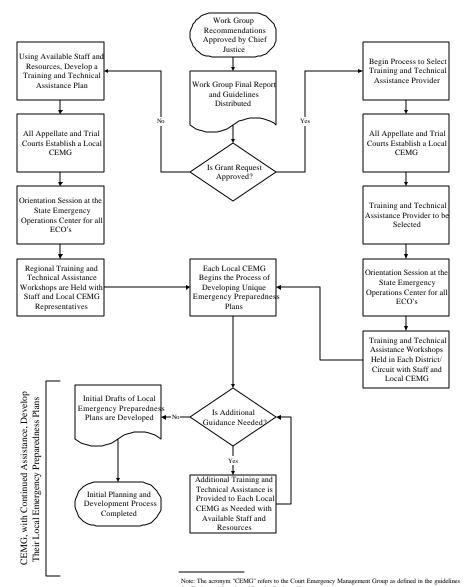
APPENDIX C

THE EMERGENCY PREPAREDNESS PROCESS



APPENDIX D

IMPLEMENTATION PROCESS



for Closing or Alteration of Regular Business Hours.

APPENDIX E

EMPLOYEE PROFILE

The information contained on this form is intended for use by the ____ Judicial Circuit of Florida in the event of an emergency for the purpose of contacting the designated Emergency Contact Persons and aiding the employee should the need arise. This information will be maintained by the circuit's Personnel Officer and it is each court employee's responsibility to communicate changes as they occur.

EMPLOYEE INFOR	RMATION				
LAST NAME:	FIRST NAME:	INITIAL:	DATE OF B	SIRTH:	_
TITLE:	DEPARTMENT/DIVISION:	IMM	EDIATE SUPERVIS	SOR AND PHONE:	-
HOME ADDRESS:					-
OFFICE ADDRESS:					-
HOME PHONE:	OFFICE PHONE:	ALTERNATE PHO	ONES (cell/pager):		_
MEDICAL INFORM	MATION (OPTIONAL)				
MEDICAL CONDITIONS/	ALLERGIC TO:	BLOO	OD TYPE:		
MEDICATION REQUIRED	D/INTERVALS:				_
DOCTORS:					_
		SPECIALIZATION	N:		_NAME
ESS:		PHONE:			_ADDR
		SPECIALIZATION	N:		_NAME
ESS:		PHONES:			_ADDR
PERSONS TO NOT	TFY IN AN EMERGENCY				
LAST NAME:	FIRST NAME:	INITI	AL:	RELATIONSHIP:	_
ADDRESS:					_
HOME PHONE:	OFFIC	EPHONE:		ALTERNATE PHONES (cell/pager):	-
LAST NAME:	FIRST NAME:	INITI	AL:	RELATIONSHIP:	-
ADDRESS:					_
HOME PHONE:	OFFIC	EPHONE:		ALTERNATE PHONES (cell/pager):	_
EMPLOYEE SIGNATURE	:			DATE:	

APPENDIX F

EMERGENCY CONTACT LOG

	LAST NAME	EMERGENCY CONTACTIS	TANKS JEWN	# EMPLOYEE	CONFIDENTIAL		Control of the Control	EMERGENCY CONTACT(S)	LAST NAME	EMPLOYEE	CONFIDENTIAL	LAST NAME	EMERGENCY CONTACT(5)	LASTNAME	BENDLIAME #	CONFIDENTIAL	100000000000000000000000000000000000000	LAST NAME	EMERGENCY CONTACTIS	LAST NAME	COMPLOYEE INC.	Investment of the second
	THEST NAME		PROF NAME						ARMI ISH			THOS NAME		THIST WAME				FIRST NAME		FIRST NAME		
	RELATIONSHIP		1000	-			THE REAL PROPERTY.	BELLA TORONO	III.			NELA HORSHIP		muz				RELATIONSHIP		TITLE		
			000	200					600					800						008		
	ADDRESS		AUURESS	Apparation				Annases	AUDRESS			AUUMESS		ADDRESS			Seatter Control	ADDRESS		ADDRESS		
	CETY		1110	- Carro				CITY	GII.			1100		OTY				ADD		OTTY		
	BIATE		TO OUT	John St.			-	arara	OF COM			91018		ZIP 000E			7	STATE		ZIP CODE		The second second
	3000 4II		A TANCAL	TANAMA A			-	an cons	a Bacha			All COUR		# 3MOH				ZIP CODE		# 3MOH		
	# 3MOH		04.1.0				100000000000000000000000000000000000000	HOME #	2			TOTAL S		ALT. 8				HOME #		ALTS		
	WT. 8		Constant	A Ground or				17.4	Charles	-		10.170		OFFICE#	-			ALT.#		OFFICE #		
			WITH STATES	MEDICAL CONDITIONS	OPTIONAL				ALLENDES	MEDICAL COMPTIONS	CHANGLACE			ALLERGIES	MEDICAL CONDITIONS/	OPTIONALI				ALLERGIES	MEDICAL CONDITIONS:	TANKSTRAN
			2411	arcon					179	90000				TYPE	BL000					TYPE	81,000	

APPENDIX G

FAMILY DISASTER PLAN

Name: Date:

It is recommended that every employee of the judicial branch have a
personalized Family Disaster Plan. Families can - and do - cope with disaster

by preparing in advance and working together as a team. Follow the steps listed in this document to create your family's disaster plan. Knowing what to do is your best protection and your responsibility.

4 STEPS OF SAFETY

1. Find Out What Can Happen To You

Contact your local emergency management or civil defense office and American Red Cross chapter – be prepared to take notes:

LOCAL OFFICE:	ENTER
	TELEPHONE
	NUMBER HERE:
Emergency	
Management Office	
American Red Cross	
Chapter	
FEMA Region IV	(770) 220-5224
Office (serving FL)	

Ask what types of disasters are most likely to happen. Request information on how to prepare for each.

Learn about your community's warning signals: what they sound like and what you should do when you hear them.

Ask about animal care after disaster. Animals may not be allowed inside emergency shelters due to health regulations.

Find out how to help elderly or disabled persons, if needed.

Next, find out about the disaster plans at your workplace, your children's school or daycare center and other places where your family spends time.

2. Create a Disaster Plan

Meet with your family and discuss why you need to prepare for disaster. Explain the dangers of fire, severe weather and other disasters to children. Plan to share responsibilities and work together as a team.

Discuss the types of disasters that are most likely to happen. Explain what to do in each case.

Pick two places to meet: Right outside your home in case of a sudden emergency, like a fire. Outside your neighborhood in case you can't return home. Everyone must know the address and phone number.

Ask an out-of-state friend to be your "family contact." After a disaster, it is often easier to call long distance. Other family members should call this person and tell them where they are. Everyone must know your contact's phone number.

Discuss what to do in an evacuation.

Plan how to take care of your pets.

3. Complete This Checklist

Post emergency telephone numbers by phones (fire, police, ambulance, etc.).

Teach children how and when to call 911 or your local Emergency Medical Services number for emergency help.

Show each family member how and when to turn off the water, gas and electricity at the main switches.

Check if you have adequate insurance coverage.

Teach each family member how to use the fire extinguisher (ABC type), and show them where it's kept.

Install smoke detectors on each level of your home, especially near bedrooms.

Conduct a home hazard hunt.

Stock emergency supplies and assemble a Disaster Supplies Kit.

Take a Red Cross first aid and CPR class.

Determine the best escape routes from your home. Find two ways out of each room.

Find the safe spots in your home for each type of disaster.

4. Practice and Maintain Your Plan

Quiz your kids every six months so they remember what to do.

Conduct fire and emergency evacuation drills.

Replace stored water every three months and stored food every six months.

Test and recharge your fire extinguisher according to manufacturer's instructions.

Test your smoke detectors monthly and change the batteries at least once a year.

EMERGENCY PREPAREDNESS

Learn how to protect yourself and cope with disaster by planning ahead. Take these things into consideration when preparing your Family Disaster Plan.

Emergency Supplies

Keep enough supplies in your home to meet your needs for at least three days. Assemble a Disaster Supplies Kit with items you may need in an evacuation. Store these supplies in sturdy, easy-to-carry containers such as backpacks, duffle bags or covered trash containers.

Include:

A three-day supply of water (one gallon per person per day) and food that won't spoil.

One change of clothing and footwear per person, and one blanket or sleeping bag per person.

A first aid kit that includes your family's prescription medications.

Emergency tools including a battery-powered radio, flashlight and plenty of extra batteries.

An extra set of car keys and a credit card, cash or traveler's checks.

Sanitation supplies.

Special items for infant, elderly or disabled family members.

An extra pair of glasses.

Keep important family documents in a waterproof container. Keep a smaller kit in the trunk of your car.

Vehicles with full gas tanks.

Pet care items.

Duct tape and plastic sheeting.

Evacuation Plan

Evacuate immediately if told to do so.

Listen to your battery-powered radio and follow the instructions of local emergency officials.

Wear protective clothing and sturdy shoes.

Take your family disaster supplies kit.

Lock your home.

Use travel routes specified by local authorities--don't use shortcuts because certain areas may be impassable or dangerous.

If you're sure you have time:

Shut off water, gas and electricity before leaving, if instructed to do so.

Post a note telling others when you left and where you are going.

Make arrangements for your pets.

Home Hazard Hunt

During a disaster, ordinary objects in you home can cause injury or damage. Anything that can move, fall, break or cause a fire is a home hazard. For example, a hot water heater or a bookshelf can fall. Inspect your home at least once a year and fix potential hazards. Contact your local fire department to learn about home fire hazards.

Utilities

Locate the main electric fuse box, water service main, and natural gas main. Learn how and when to turn these utilities off. Teach all responsible family members. Keep necessary tools near gas and water shut-off valves.

Remember, turn off the utilities only if you suspect the lines are damaged or if you are instructed to do so. *If you turn the gas off, you will need a professional to turn it back on.*

Neighbors Helping Neighbors

Working with neighbors can save lives and property. Meet with your neighbors to plan how the neighborhood could work together after a disaster until help arrives. If you're a member of a neighborhood organization, such as a home association or crime watch group, introduce disaster preparedness as a new activity. Know your neighbors' special skills (e.g., medical, technical) and consider how you could help neighbors who have special needs, such as disabled and elderly persons. Make plans for childcare in case parents can't get home.

Have a Pet Plan

Make arrangements for your pets as part of your household disaster planning. If you must evacuate your home, it's always best to take your pets with you. For health and space reasons, pets will not be allowed in public emergency shelters. If, as a last resort, you have to leave your pets behind, make sure you have a plan to ensure their care. Contact your local animal shelter, humane society, veterinarian, or emergency management office for information on caring for pets in an emergency.

Find out if there will be any shelters set-up to take pets in an emergency. Also, see if your veterinarian will accept your pet in an emergency.

IF DISASTER STRIKES

Remain calm and patient. Put your plan into action.

CHECK FOR INJURIES

Give first aid and get help for seriously injured people.

LISTEN TO YOUR BATTERY POWERED RADIO FOR NEWS INSTRUCTIONS

Evacuate, if advised to do so. Wear protective clothing and sturdy shoes.

CHECK FOR DAMAGE IN YOUR HOME

Use flashlights. Do not light matches or turn on electrical switches, if you suspect damage.

Sniff for gas leaks, starting at the water heater. If you smell gas or suspect a leak, turn off the main gas valve, open windows, and get everyone outside quickly.

Shut off any other damaged utilities. (You will need a professional to turn gas back on.)

Clean up spilled medicines, bleaches, gasoline, and other flammable liquids immediately.

REMEMBER TO...

Confine or secure your pets.

Call your family contact--do not use the telephone again unless it is a life-threatening emergency.

Check on your neighbors, especially elderly or disabled persons.

Make sure you have an adequate water supply in case service is cut off.

Stay away from downed power lines.

The contents of this document were taken from the Federal Emergency Management Agency's (FEMA) Community and Family Preparedness Program and the American Red Cross Community Disaster Education Program. For more information call you local American Red Cross Chapter and by calling FEMA 1-800-480-2520, or writing: FEMA, P.O. Box 2012, Jessup, MD 20794-2012. Publications are also available on the World Wide Web at: FEMA's Web site: http://www.fema.gov and American Red Cross Web site: http://www.fema.gov and American Red Cross Web site: http://www.fema.gov

EMPLOYEE EMERGENCY RECOVERY GUIDE

All employees should complete this form. This Recovery Guide is designed to provide information that will assist an assist the employee to stabilize their basic needs following an emergency.

Insurance Information						
Health Insurance	Policy Number	Telephone Number				
Primary Care	Address:	Telephone				
Physician:		Number:				
Disability	Policy Number:	Telephone				
Insurance		Number:				
Life Insurance	Doliov Numbon	Tolombono				
Life filsurance	Policy Number:	Telephone Number:				
		Number.				
Other Insurance:	Policy Number:	Telephone				
outer insurance.	Toney Trainioer.	Number:				
Home Owners	Policy Number:	TelephoneNumber:				
Insurance:						
Vehicle Insurance:	Policy Number:	Telephone				
		Number:				
	Employer Information					
Employee	Address:	Telephone				
Assistance		Number:				
Program:						
Emergency	Telephone					
Coordinating	Number:					
Officer:	1,021001.					
Emergency	Telephone					
Hotline	Number:					

Community Services	s and Emergency Manage	ement Agencies
American Red	Telephone	
Cross	Number:	
County	Telephone	
Emergency	Number:	
Management		
Office		
Florida	Telephone	
Emergency	Number:	
Management		
Office		
Federal	Telephone	
Emergency	Number:	
Management		
Agency:		
Other Agencies:	Telephone	
	Number:	

Credit Car	Credit Card and Financial Information					
Financial	Account	Telephone				
Institution:	Number:	Number:				
Financial	Account	Telephone				
Institution:	Number:	Number:				
Credit Union	Account Number	Telephone				
		Number:				
Mortgage	Account Number	Telephone				
Company:		Number:				
Credit Card	Account	Telephone				
Companies:	Numbers:	Numbers:				

	Emergency Plan Form	
	Out-of-State Contacts	
Name:	Address:	Telephone
		Number:
	Local Contacts	
Name:	Address:	Telephone
		Number:
	Nearest Relative	
Name:	Address:	Telephone
		Number:
	Family Work Numbers	
Spouse	Parent	Other
E		
	mergency Telephone Number	S
Police:	Telephone	
	Number:	
T.	T 1 1	
Fire:	Telephone	
	Number	
II.amikal	Talaghana	
Hospital	Telephone	
	Number	
	Eamily Dlane	
Name:	Family Physicians	
Name:	Telephone	
ranic.	Niverala	
Name.	Number	
Name:	Telephone	

APPENDIX H

CRITICAL FORMS

Circuit Civil

Civil Cover Sheet	Notice of hearing (Demand for Hearing)
	<i>e</i> ,
Summons for Corporations	Demand for Hearing – Per
	F.S. 713.585(3)
Summons for Individuals	Division Audit Sheet
Affidavit of Exemption	Balance Sheet
from Garnishment	
Affidavit of Indigency	Cash Confirmation Sheet

Domestic Relations

Summons	Modification Forms
Defaults	Purchase Orders
Subpoenas	Blank Motions
Writs of Attachment	Outgoing Transfer Form
Court Minutes	Financial Affidavit
Evidence Control Report	Registration Forms
Injunction Petitions	Indigency Affidavit
Injunction Orders	Indigency Order
Divorce Forms	Clerk's Certificate
Custody Forms	Notices of Action
Paternity Forms	

Child Support

Forms for minutes	Evidence Form
-------------------	---------------

Disaster Recovery Forms

Blank Purchase Orders	Time Sheets
Itemized Cost Sheet for	
Emergency Fund	
Reimbursement	

Mental Health

Petition for Involuntary Examination (Baker Act)	Summons to Appear
Affidavit	Application for Attorney
Ex Parte Order for	Order for Involuntary
Involuntary Examination	Assessment and
·	Stabilization
Notice of Hearing on	Order for Involuntary
Petition for Involuntary	Treatment
Placement	
Report of General Master	Notice of Hearing on
	Petition for Involuntary
	Treatment
Order for Involuntary	Notice of Hearing on
Placement	Petition for Involuntary
	Assessment and
	Stabilization
Petition for Involuntary	Notice of Right to be
Assessment and	Examined by Professional
Stabilization (Marchman Act)	Appointed by the Court

County Civil

Marriage licenses	Voluntary dismissal
Marriage license application	Garnishment
Statement of claim	Waiver-garnishment
Affidavit of Indigency	Affidavit of non-payment
Certificate of Indigency	Affidavit of non-military
	service
Summons	Clerk's certificates
Summons/notice to appear	Clerk's certificate-lien bond
Civil cover sheet	Clerk's certificate-improper
	towing
Certificate of mailing	Stipulation
Notice of mailing foreign	Affidavits
judgment	
Notice of compliance-	Clerk's worksheet
garnishment	
Motion for writ of	Clerk's certificate
garnishment	
Writ of garnishment	Foreclosures
Affidavit of exemption	Certificate of disbursements
Affidavit of prisoner	Certificate of sale
Order regarding Indigency	Certificate of title
Appeals	Certificate of no
	disbursements
Case finalization	Division audit sheet
Final judgment	Cashier balance sheet
Writ of possession	Cash confirmation sheet
Writ of execution	Letter for nsf check
Order of dismissal	Deposit slips from bank

Circuit and County Criminal

Subpoena for deposition	Clerk's Certificate of
	Forfeiture
Certificate of mailing	Judgment of Acquittal
Letter to Civil ref TOT	Sentencing
Subpoena SAI	Uniform Commitment
Subpoena duces tecum	Drug Offender Probation
	Order
Witness subpoena	Certificate of Mailing
Court minutes form and	Capias
there are SEVERAL	
Order declaring defendant	Order of probation and
indigent and appointment of	Community Control and
counsel	Community Control II
Notice for arraignment and	Summons
trial, etc	
Charges/Cost/Fee	Final Judgment
Judgment	

Circuit Juvenile

Release Order	Summons (Delinquency)
Detention Order	Summons (Truancy)
Home Detention/Non-Secure	Custody Orders (law
Detention/Electronic	enforcement authorized to
Monitoring Order	take child into custody)
Affidavit of Insolvency	Summons (Child in need of
(Delinquency)	services)
Affidavit of Insolvency	Summons (Dependency)
(Dependency)	
Shelter/Placement Orders	Summons (Termination of
	Parental Rights)
Order Appointing Counsel	Subpoenas (several types:
for Child (Delinquency)	trial, deposition, duces
	tecum)
Order Appointing Counsel	Receipt book (in lieu of
for Parents (Dependency)	cash control system
	receipts)
Order Canceling Custody	Deposit book
Order	
Blank Order (to cover all	
other contingencies)	

APPENDIX I

EMERGENCY PREPAREDNESS SURVEY

PART A - PAPER RECORDS

Name: Title:
DCA (if applicable):
Circuit (if applicable): County: Agency:
Address: City: Zip Code:
Phone: E-mail:
1. Where are paper records warehoused? Check all that apply and the name of the location:
 ÿ Designated space within courthouse ÿ County Storage Facility ÿ State of Florida storage facility ÿ Outsourced facility
2. Is the storage facility environmentally controlled? ÿ Yes ÿ No Go to question 5 if you answered "no.".
3. Environmentally controlled variables that are being controlled. Check all that apply:
ÿ Temperature ÿ Humidity ÿ Sunlight ÿ Dust/Contamination ÿ None

4. Environmentally controlled variables that are being controlled and are also	О
being monitored in case the variables should fail. Check all that apply:	

- ÿ Temperature
- ÿ Humidity
- ÿ Sunlight
- ÿ Dust/Contamination
- ÿ None
- 5. Fire extinguishing system used at the storage facility:
- ÿ Water-based sprinkler system
- ÿ Halon or other chemical based fire-extinguishing system
- ÿ Powder based fired extinguishing system
- ÿ None
- 6. Do preventive measures exist to protect paper in the event the room is flooded by water? ÿ Yes ÿ No

If yes, please briefly describe (please limit your response to 1,000 characters):

- 7. How is the paper secured from threat of theft or vandalism? Check all that apply:
- ÿ Security video monitoring
- ÿ Security guards
- ÿ Secure entry
- ÿ Other:
- ÿ No security

8. Is there a method of tracking paper files that are not in storage? Yes y No
If yes, please briefly describe (please limit your response to 1,000 characters):
9. Do you presently have recovery procedures if paper files are lost or damaged? ÿ Yes ÿ No
If yes, please briefly describe or sub mit copy of plan (please limit your response to 1,000 characters):
10. In the event of courthouse closure due to catastrophic event, do you have a procedure to get paper files to an alternate courthouse location? ÿ Yes ÿ No
If yes, please briefly describe or submit copy of plan (please limit your response to 1,000 characters):
11. Do you have a method of identifying vital and non-vital records in the event of a disaster? ÿ Yes ÿ No
If yes, please briefly describe or submit copy of plan (please limit your response to 1,000 characters):

12. Do you have a method of providing vital records to alternate court operations in the event of a disaster? ÿ Yes ÿ No

If yes, please briefly describe or submit copy of plan (please limit your response to 1,000 characters):

- 13. In some instances, especially during a hurricane threat, executing a preparedness plan can save paper records from damage (covering shelving with plastic sheeting, etc.). Do you have a plan to protect records before a disaster strikes? ÿ Yes ÿ No
- 14. Do you have any plans to convert you files to electronic in the future? ÿ Yes ÿ No

If yes, please briefly describe or submit copy of plan (please limit your response to 1,000 characters):

PART B- ELECTRONIC RECORDS

Name: Title:
DCA (if applicable):
Circuit (if applicable): County: Agency:
Address: City: Zip Code:
Phone: E- mail:
GENERAL INFORMATION SECURITY PRACTICES
1. What type of systems do you presently have for electronic records? Check all that apply.
ÿ Mainframe/Midrange/Mini ÿ PC Server ÿ Document Imaging System ÿ Analog Audio ÿ Digital Audio ÿ Analog Video Recordings ÿ Digital Video Recordings ÿ Other:
2. Are your technology operations centralized or distributed?
ÿ Centralized ÿ Distributed ÿ Combination
3. How many full-time equivalent staff do you have in direct support of information technology?
4. Do you have a formally designated information systems security manager? ÿ Yes ÿ No

- ÿ Never
- ÿ More than 6 years ago
- ÿ 3-6 years ago
- ÿ 1-3 years ago
- ÿ Within the past year
- ÿ In-house
- ÿ Third party
- 6. Do you have in place a written policy that addresses the acceptable use of technology resources? \ddot{y} Yes \ddot{y} No

7. Do you have in place an active information security awareness program:

ÿ Yes ÿ No If yes:

ÿ Client Workstations

ÿ None

 \ddot{y} Hand-held devices and laptops

ÿ For users of the systems ÿ For technology staff
8. Do your systems development projects and activities follow a formal methodology (i.e. Systems Development Life Cycle) that includes a risk assessment? ÿ Yes ÿ No
9. How often, if ever, do you comprehensively review and update all documentation related to your systems configuration (i.e. network maps, database designs, etc.)?
ÿ Never ÿ As needed ÿ Annually ÿ Quarterly
10. Do you have in place formal written procedures that address response to computer crimes? ÿ Yes ÿ No
11. What methods of access control do you currently have in place to safeguard electronic court records?
 ÿ Passwords ÿ Smart Card Authorization ÿ Biometric Authentication ÿ Key Fob Secure ID ÿ Other:
12. To what extent do you have antivirus software deployed?
ÿ Database Servers ÿ File Servers ÿ E-mail Servers/Gateways

13. How often and through what means are virus definitions updated?
ÿ Never ÿ Less than once per month ÿ Monthly ÿ Weekly ÿ Daily ÿ Real-time
ÿ Automatic ÿ Manual
14. How often and through what means are systems scanned for viruses?
ÿ Never ÿ Less than once per month ÿ Monthly ÿ Weekly ÿ Daily ÿ Real-time
ÿ Automatic ÿ Manual
15. What forms of cryptography, if any, are in use to safeguard court information?
ÿ Public Key Infrastructure (PKI) ÿ Kerberos ÿ Symmetric Key ÿ Secure Socket Layering (SSL) ÿ Wired Equivalent Privacy (WEP) ÿ IPSec ÿ Other:
16. What processes, if any, do you have in place for gathering intelligence and providing early warning regarding new and changing threats that may jeopardize the confidentiality, integrity or availability of electronic court records (i.e. viruses, hacks, etc)? (Please limit your response to 1,000 characters.)

- 17. What mechanisms, if any, do you have in place to identify security-related events that may jeopardize the confidentiality, integrity or availability of electronic court records?
- ÿ System Event Logging
- ÿ Network Intrusion Detection
- ÿ Other:
- 18. What forms of network security do you currently have in place to safeguard electronic court records?
- ÿ Proxy Server
- ÿ Network Address Translation
- ÿ Stateful Inspection Firewall
- ÿ Packet Filtering Firewall
- ÿ Managed Switch(es)
- ÿ Private Frame Relay WAN Circuits
- ÿ Private Fiber Optic WAN Circuits
- ÿ Virtual Private Networking
- ÿ Other:
- 19. When and by whom was a comprehensive vulnerability scan last performed on your systems?
- ÿ Never
- ÿ More than three years ago
- ÿ 1-3 years ago
- ÿ 6-12 months ago
- ÿ Within the past 6 months
- ÿ In-house
- ÿ Third-party
- 20. What methods do you use to physically secure equipment and media that contain electronic court records? Check all that apply.
- ÿ Secure entry
- ÿ Security Monitoring
- ÿ Security Guard
- ÿ Logging
- ÿ Other:
- ÿ No security

21. What environmental controls are present to monitor are	eas that hous	se
equipment and media containing electronic court records?	Check all the	nat
apply:		

- ÿ Temperature
- ÿ Humidity
- ÿ Dust
- ÿ Flood/Water
- ÿ Power surge
- ÿ Power outage
- 22. Are there any new security measures planned and budgeted? \ddot{y} Yes \ddot{y} No

If yes, please list (please limit your response to 1,000 characters):

EMERGENCY PREPAREDNESS (DISASTER RECOVERY AND CONTINUITY OF OPERATIONS)

- 1. Does your organization have a disaster recovery plan that covers information technology? ÿ Yes ÿ No If no, skip to question 8.
- 2. When was your disaster recovery plan last reviewed and updated?
- ÿ Never
- ÿ More than 5 years ago
- ÿ 3-5 years ago
- ÿ 1-3 years ago
- ÿ Within the past year
- 3. Is your disaster recovery plan documented? ÿ Yes ÿ No
- 4. What areas of your information technology infrastructure does your disaster recovery plan address? Check all that apply.
- ÿ Workspaces
- ÿ Workstations
- ÿ Local Area Networks
- ÿ Servers
- ÿ Wide Area Data Communications Links
- ÿ Power
- ÿ Software
- ÿ Data
- ÿ Media and Records Storage
- ÿ Staff Duties
- ÿ Other:
- 5. What events does your information technology disaster recovery plan address? Check all that apply.
- ÿ Short-term power outage (less than one week)
- ÿ Extended power outage (more than one week)
- ÿ Short-term loss of wide area data communications (less than one week)
- ÿ Extended loss of wide area data communications (more than one week)
- ÿ Short-term building evacuation (less than one week)
- ÿ Extended building evacuation (more than one week)
- ÿ Catastrophic loss of critical servers
- ÿ Catastrophic loss of entire facility
- ÿ Catastrophic loss of technology staff
- ÿ Other:

- 6. When was the last time your was plan tested?
- ÿ Never
- ÿ More than 5 years ago
- ÿ 3-5 years ago
- ÿ 1-3 years ago
- ÿ Within the past year
- 7. What methods have been utilized within the past three years to test your disaster recovery plan? Check all that apply:
- ÿ Checklist (plan circulated for review to ensure all critical areas have been addressed)
- ÿ Walkthrough (plan walked through at a meeting of management representatives)
- ÿ Simulation (plan practiced up to the point of recovery through simulating emergency)
- ÿ Parallel (full test using all personnel to ensure alternate facilities/equipment function)
- ÿ Full interruption (disaster is replicated by ceasing primary site operations)
- 8. What types of alternate technology and facilities do you have in place for disaster? Check all that apply:
- ÿ Hot site (fully configured facility, with operational mirror of all technology)
- ÿ Warm site (facility with minimal equipment, software and data must be restored)
- ÿ Cold site (empty facility requiring delivery and installation of computer equipment)
- ÿ Multiple sites (distributed production and technology facilities)
- ÿ Reciprocal agreement (another organization with similar facilities and technology)
- 9. What methods do you use to back-up electronic court records? Check all that apply:
- ÿ Back-up data on removable storage media such as DVD, Tape or CD
- ÿ Replication on remote equipment or storage appliance
- ÿ On-line replication to outsourced vendor site
- ÿ None
- ÿ Other:

10. Do you have a documented back-up methodology for electronic records? ÿ Yes ÿ No
11. How often do you back-up electronic court records?
ÿ Real-time ÿ Daily ÿ Weekly ÿ Monthly ÿ Never ÿ Other:
12. How often do you back-up system files?
ÿ Real-time ÿ Daily ÿ Weekly ÿ Monthly ÿ Never ÿ Other:
13. Where do you store your back-up data?
 ÿ Onsite ÿ Offsite facility outsourced with vendor: ÿ Offsite storage at County facility: ÿ Offsite storage at State facility: ÿ Other:
14. How often are your backups delivered to storage?
ÿ Not applicable ÿ Daily ÿ Weekly ÿ Biweekly ÿ Monthly
15. Do you store current copies of required software and technical documentation offsite? ÿ Yes ÿ No

16. When was the last time data was successfully restored from your backup method?
ÿ Never ÿ More than one year ago ÿ 6-12 months ago ÿ 3-6 months ago ÿ 1-3 months ago ÿ Within the past month
17. What alternate equipment would be immediately available for your use in the event of a loss?
ÿ Workstations ÿ Servers ÿ Mainframe/midrange/mini ÿ Printers ÿ Network components (routers, switches, hubs, cabling, etc.) 18. Do you presently have a manual process in place that would enable your organization to function in the event you had no computer system? ÿ Yes ÿ No
If yes, please briefly describe this plan (please limit your response to 1,000 characters):
19. Do you believe that there are important and relevant questions not asked in this survey? ÿ Yes ÿ No
If yes, please elaborate (please limit your response to 1,000 characters):

GLOSSARY OF TERMS

"Access Controls" means mechanisms aimed at specifying what resources can be accessed and by whom. (e.g., passwords)

"Administrative and Emergency Procedures" means procedures establishing a framework through which each district and circuit will prepare for, respond to, recover from, and mitigate the impacts of emergencies not requiring the relocation of selected personnel and functions.

"Applications & Systems Development" means: controls that are included within systems and applications software and the steps used in their development. (e.g., the Systems Development Life Cycle)

"Audit and Monitoring" means mechanisms and methods for collecting and providing information necessary to identify and respond to security-related events, and ensure compliance with policies and procedures. (e.g., system logging)

"Continuity of Operations Plan (COOP)" means policy and guidance to ensure the execution of the State Court System's mission essential functions in any event or threat thereof which requires the relocation of selected personnel and functions.

"Court Emergency Management Group (CEMG)" means a group established by the chief justice or chief judge that serves as a mechanism for coordination within the courts and specifically responsible for providing recommendations on administrative procedures, developing Emergency Preparedness Plans, creating procedures for information dissemination, establishing safety procedures for facility evacuation, and updating appropriate plans and procedures.

"Court Record" means the contents of the court file, including the progress docket and other similar records generated to document activity in a case, transcripts filed with the clerk, documentary exhibits in the custody of the clerk, and electronic records, videotapes, or stenographic tapes of depositions or other proceedings filed with the clerk, and electronic records, videotapes, or stenographic tapes of court proceedings.

"Criminal Justice Network (CJNET)" means a computer network maintained by the Florida Department of Law Enforcement that provides intelligence information to law enforcement agencies. "Cryptography" means methods of disguising information to ensure integrity, confidentiality, authenticity and non-repudiation. (e.g., electronic signatures)

"Custodian" means: any judicial branch entity that stores records on behalf of the courts in either paper or electronic formats.

"Distributed Network," means a computer network that spans a relatively large geographical area. A Wide Area Network (WAN) consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

"Emergency" means any event that can cause death or significant injury to judges, employees of the court or court-adjunct agencies, or members of the public; or that can affect the continuation of court proceedings, disrupt operations, cause physical or environmental damage to a court facility, or threaten the public's confidence in the use of the facility.

"Emergency Coordinating Officer (ECO)" means a person designated by the chief justice or the chief judge with the responsibility for preparing and maintaining the court's Emergency Preparedness Plan, assisting the Court Emergency Management Group in structuring planned responses to emergencies, and ensuring the court's plan and responses are coordinated with other federal, state, and county emergency management and law enforcement agencies and personnel.

"Emergency Preparedness Plan" means the overall plan approved by the chief justice or chief judge that encompasses both Administrative and Emergency Procedures and the Continuity of Operations Plan (COOP). The plan should not be distributed generally and the chief judge, marshal, circuit court administrator, or ECO should control the number of copies and to whom they are distributed.

"Florida State Courts Network" means the Private Frame Relay network provided by the Florida Supreme Court.

"Information Technology Security Manager" means a member of the court technology staff that is assigned the responsibility of insuring adequate mechanisms and controls are in place to maintain the confidentiality integrity and availability of court information assets.

"Intelligence" means mechanisms and tactics designed to provide early warning of new and changing threats and threat prevalence such that countermeasures can be identified and implemented in time to minimize vulnerability. (e.g., global threat advisories) "Internet" means a global network connecting millions of computers. The Internet is decentralized, and each Internet computer, called a host, is independent.

"Intranet" means a network based on Transmission Control Protocol/Internet Protocol (TCP/IP) belonging to an organization, which is accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet prevents unauthorized access. Intranets are typically used to share information specific to the organization.

"Judicial branch" means the judicial branch of government, which includes the state courts system, the clerk of court when acting as an arm of the court, The Florida Bar, the Florida Board of Bar Examiners, the Judicial Qualifications Commission, and all other entities established by or operating under the authority of the Supreme Court or the chief justice.

"Law, Investigation & Ethics" means knowledge of computer crime, adherence with laws relating to software and computer systems, investigative techniques used to determine if a computer crime has been committed and ethical obligations of information technology professionals. (e.g., software licensing compliance)

"Malicious Code/Virus" means computer programs that are specifically designed to disrupt operations corrupt or destroy information or breech confidentiality of information. (e.g., computer viruses)

"Operations Security" means the identification and implementation of controls over computer hardware, data storage media and personnel with access to these resources. (e.g., separation of duties and responsibilities)

"Physical Security" means environmental controls and physical protection of sensitive information and information technology resources including information systems personnel, data, equipment and supplies. (e.g., fire extinguishing systems)

"Public Information Officer" means a member of the court staff, appointed by the chief justice, the chief judge or circuit court administrator, who will serve as the single point of contact with the media during emergencies.

"Records of the judicial branch" means records, regardless of physical form, characteristics, or means of transmission, made or received in connection with the transaction of official business by any judicial branch entity.

"Safety Officer" means a person appointed by the chief justice or chief judge who has authority to order the evacuation of a court facility during an emergency.

"Response and Recovery" means planning and methods intended to control loss associated with uncertain events that jeopardize the confidentiality, integrity and availability of information resources. This includes contingencies and procedures for quickly, consistently and effectively responding to emergencies, security incidents and disasters. (e.g. off-site storage of data)

"Risk Assessment" means identifying assets, determining the value of those assets, identifying the vulnerabilities and threats to the assets, and then determining the level of risk. Based on this information, a review and recommendation will be made to provide cost effective safeguards to reduce or mitigate the risk. The initial risk assessment establishes the benchmark from which periodic updates are made. Risk Assessments are an important tool used to identify potential problem areas that allows them to be addressed in a preventative manner.

"Security Architecture" means concepts, principles, structures and standards used to design, implement, monitor and secure information systems and the controls used to enforce varying levels of security. (e.g., isolation of computing processes)

"Security Management Practices" means the development, documentation and implementation of standards, policies, procedures and guidelines that ensure the confidentiality, integrity and availability of information assets. (e.g. security awareness training)

"Telecommunications and Network Security" means structures and methods directed at providing integrity, availability, authentication and confidentiality for transmissions over networks.

"Court Technology Officer" means an employee of the court that specifically manages technology for a specified district or circuit.

"Vital Records" means records that are critical to the administration of justice during situations where standard methods for accessing court records may be impeded, and technology systems may be unavailable due to an emergency situation whereby the court may only function at a most basic level.

"Vital Personnel Records" means records information about an employee that is essential for providing compensation and benefits to an employee by its employer; such as, but not limited to, employee name, address, social security number, date of hire, date of birth, rate of pay, classification, payroll deductions and tax withholdings, health, life and disability insurance provider, beneficiaries, and leave records.

"Virus" means malicious code.

ACROYMNS USED IN THIS REPORT

ABC means a Fire Extinguisher of a certain type

AECO means Alternate Emergency Management Coordinator

AED means Automated External Defibrillator

BLS means Basic Life Safety Kit

CEMG means Court Emergency Management Group

CEMP means Comprehensive Emergency Management Plan

CJNET means Criminal Justice Network

COG means Continuity of Government

CONOP means Concept of Operations

COOP means Continuity of Operations Plan

COPES means Cooperative Personnel Employment System

CPR means Cardio Pulmonary Resuscitation

ECO means Emergency Coordinating Officer

FEMA means Federal Emergency Management Agency HOT means a facility where continued operations of automated systems during emergencies may be accomplished through the reestablishment of systems on alternative machines

IPSec means Internet Protocol Security

ITSM means Information Technology Security Manager

LAN means Local Area Network

OSCA means Office of the State Courts Administrator

PIO means Public Information Officer

PKI means Public Key Infrastructure

SCM means Survival Crisis Management Plan

SSL means Secure Socket Layering

TCP/IP means Transmission Control Protocol/Internet Protocol

WAN means Wide Area Network

WEP means Wired Equivalent Privacy