JUDICIAL COUNCIL
OF CALIFORNIA
INFORMATION TECHNOLOGY
ADVISORY COMMITTEE

www.courts.ca.gov/itac.htm
itac@jud.ca.gov

INFORMATION TECHNOLOGY ADVISORY COMMITTEE

MINUTES OF OPEN MEETING

May 5, 2017
12:00 PM to 1:00 PM
Teleconference

Advisory Body Members Present:	Hon. Sheila F. Hanson, Chair; Hon. Louis R. Mauro, Vice Chair; Mr. Brian Cotta; Hon. Julie R. Culver; Hon. Michael S. Groch; Hon. Samantha P. Jessner; Hon. Jackson Lucky; Mr. Terry McNally; Hon. Kimberly Menninger; Hon. James Mize; Mr. Snorri Ogata; Hon. Alan G. Perkins; Hon. Peter J. Siggins; Hon. Joseph Wiseman; Ms. Jeannette Vannoy; Mr. David H. Yamasaki
Advisory Body Members Absent:	Ms. Alexandra Grimwade; Mr. Darrel Parker; Ms. Allison Merrilees in for Hon. Mark Stone; Mr. Don Willenburg; Chief Judge Wiseman
Others Present:	Hon. Daniel Buckley; Mr. Robert Oyung; Mr. Jake Chatters; Mr. Mark Dusman; Ms. Virginia Sanders-Hinds; Ms. Kathy Fink; Ms. Jamel Jones: Mr. Patrick O'Donnell; Ms. Fati Farmanfarmaian; Ms. Andrea Jaramillo; Ms. Jackie Woods; Ms. Marcela Eggleton; JCC Staff

OPEN MEETING X–X)

Call to Order and Roll Call
The chair called the meeting to order at 12:01 PM, and took roll call.

Approval of Minutes
The advisory body reviewed and approved the minutes of the March 17, 2017, Information Technology Advisory Committee meeting.

There were no written comments received.

DISCUSSION AND ACTION ITEMS (ITEMS 1 - 5)X–X)

Item 11
Opening Remarks and Chair Report
Provide general update on activities relevant to the committee.
Presenter: Hon. Sheila F. Hanson, Chair

Update: Judge Sheila F. Hanson welcomed members to the May 5 ITAC meeting and called for roll. She formally announced the departure of Justice Terence L. Bruiniers from ITAC and thanked him for his leadership as a former ITAC chair and vice-chair as well as his commitment to membership since 1999. Justice Bruiniers led ITAC through the

transition from CTAC, adopting the successful workstreams model, and served as the executive sponsor for the Tactical Plan Update and Video Remote Interpreting workstreams. He has also been a champion and leader of the appellate courts implementation of e-filing statewide. He will be missed on ITAC, but will remain connected in his ongoing role and leadership of the Video Remote Interpreting pilot program and the Technological Subcommittee of the Language Access Plan Implementation Task Force, which he chairs.

Judge Hanson has included with your materials an update of subcommittee members, liaison assignments, and workstream sponsors. Pease reach out to her or Justice Louis R. Mauro if you have questions or concerns.

Lastly, ITAC is currently seeking membership nominations. There are currently appellate and trial court judicial officer positions, as well as two new court information officer positions available for appointment. All members are encouraged to reapply, as well as nominate colleagues in the branch. Nominations are due May 12.

Chair report concluded.

Item 2

Judicial Council Information Technology (JCIT) Update

Present for discussion the activities and news coming from the Judicial Council's Information Technology (JCIT) office, including an organizational update.

Presenter: Mr. Robert Oyung, Chief Information Officer/Director

Update: Mr. Robert Oyung provided an update on the direction of JCIT. The focus of JCIT is to align with the four-year branch strategic plan goals. Which is broken into individual technology initiatives and then broken down into the two-year tactical plan. Aligning will help JCIT to support these goals by 1. Promote the digital court, 2. Optimize the infrastructure, 3. Optimize branch resources, and 4. Promote rule and legislative changes. The strategic plan generates individual initiatives over the next four years to support those goals in the tactical plan. More detail can be found in the slide deck included with your materials.

Feedback from customers has been good. Courts would like JCIT to provide more leadership for enterprise services and initiatives, master service agreements (MSAs), leveraged purchases are of value, and more should be negotiated. Small courts desire more assistance and consulting from JCIT due to limited court IT staff. Additionally, JCIT needs transparency regarding processes, costs, and services; low resources result in slow responses to their requests; and that the costs for some services were too expensive. Finally, courts felt that sometimes JCIT was hesitant to make recommendations or explain rationale clearly.

Mr. Oyung wants to make sure his staff can do their best work. JCIT will be providing enterprise IT leadership. The transformation will focus on five major activities: baseline services, new services, innovation, acting as trusted IT advisor, and establishing a program management office. Expected results are better business alignment with

branch; improved partnerships; IT services sized and funded to match business demand; and improved employee engagement.

JCIT is in the process of gathering a complete list of MSAs to share with courts.

Item 3

Branch Technology Summit Planning

Brainstorming session on potential topics for the branch Technology Summit being held in August 2017.

Facilitator: Mr. Robert Oyung, Chief Information Officer/Director

Update:

Mr. Oyung gave an update on the upcoming technology summit. It will be held August 23 (afternoon) – 24 (morning) in Sacramento. Attendees will include CEOs, Appellate courts, technology advisory committees, as well as others. This summit is a chance to identify next steps for the branch. Share any topics you think might be important for this meeting with Mr. Oyung. This effort will help with the next strategic and branch plans. ITAC members had the following suggestions for potential topics: E-services expansion or services that do not require a court visit, demo at summit of self-represented litigants (SRL) kiosks, look into uniform fee applications, there seems to be various workflows at different courts and it seems that it should be statewide, consensus on data capture for family law and civil case processing systems, unique opportunity to do a session on local technology governance models, and trial courts transcripts in relation to transcript assembly platform (TAP).

Mr. Oyung will share these brainstorm ideas he has received as well as topics discussed at the 2012 summit post meeting.

Item 44

Annual Agenda Amendment Consideration: Digital Evidence (Action Required)

Revisit the "digital evidence" placeholder initiative included on ITAC's current annual agenda. Discuss potential scope of work and consider whether to initiate a workstream in the current year. Facilitators: Hon. Sheila F. Hanson, Chair

Mr. Snorri Ogata, Member and Chief Information Officer, Superior Court of Los Angeles County

Action:

Judge Hanson noted this item became a placeholder during the annual agenda discussion at December 2016 meeting. The decision to wait until after the adoption of the Tactical Plan and ITAC was able to scope out their role. She wants ITAC to review and gauge if there is enough interest and an executive sponsor to lead a workstream this year. If so, there will be a motion to amend the annual agenda and authorize the workstream.

Mr. Snorri Ogata supports this item. Law enforcement agencies are using a lot of digital evidence. The current challenge is around rules and guidelines being updated to

include this type of evidence. Justice Louis R. Mauro understood from the e-Courts conference that there are no standards for this medium and this could be an opportunity to develop a single branch solution. Judge Kimberly Menninger would like to sponsor this workstream and Mr. Oyung is able to offer a JCIT co-lead with a trial or appellate court person. Mr. Patrick O'Donnell believes Court Executives Advisory Committee (CEAC) is working on this issue as well so it might be helpful to work with them. Mr. David Yamasaki is a CEAC liaison and assigned to a working group with this focus, he will share updates with ITAC going forward.

Request a Motion to Amend the Annual Agenda authorizing ITAC to form a Digital Evidence (Phase I, exploratory) Workstream that would investigate and define aspects of digital evidence to be addressed by the committee for the first three tasks.

Approved

Item 55
Innovation Grants Update

Review the grants awarded for technological innovations by the Judicial Council, and provide an update on the coordination with related initiatives and branch IT governance.
Presenters: Mr. Robert Oyung, Chief Information Officer/Director
Ms. Marcela Eggleton, Senior Analyst, Special Projects

Update: Due to time constraints, Mr. Oyung asked members to review the materials and consider ideas that will help. Differed to June 9 in-person meeting.

ADJOURNMENT

There being no further business, the meeting was adjourned at 12:00 p.m.

Approved by the advisory body on [enter date].

JUDICIAL COUNCIL
OF CALIFORNIA
INFORMATION TECHNOLOGY
ADVISORY COMMITTEE

www.courts.ca.gov/itac.htm
itac@jud.ca.gov

INFORMATION TECHNOLOGY ADVISORY COMMITTEE

MINUTES OF ACTION BY EMAIL BETWEEN MEETINGS

MAY 19, 2017

Email Proposal

The Information Technology Advisory Committee was asked to consider by email action whether to approve or disapprove the recommendation that two initial funding requests (IFRs)/Concepts move forward and develop into full budget concept proposals (BCPs). 1. The first IFR/Concept proposed to request funds for a Self-Represented Litigants Statewide E-Services Solution. 2. The second IFR/Concept proposed to request funds for a statewide Single Sign-On Solution (i.e., Identity Management solution). A BCP is a proposal to change the level of service or funding sources for activities authorized by the Legislature, or to propose new program activities not currently authorized. IFRs/Concepts are the first step in the BCP development process and provide an overview and vision for potential BCPs. The IFR/Concept documents for the two requests was available on the advisory body web page on the California Courts website listed above; and also to members via email. Due to timing constraints, the committee's voting on the IFRs/Concepts needed to take place via action by email.

Notice

On May 12, 2017 a notice was posted advising that the ITAC was proposing to act by email between meetings under California Rules of Court, rule 10.75(o)(2).

Public Comment

Because the action by email concerned a subject that otherwise must be discussed in an open meeting, the ITAC invited public comment on the proposal under rule 10.75(o)(2). The public comment period began on Friday, May 12, 2017 at 4:45 p.m. and ended at 4:00 p.m. on Tuesday, May 16, 2017. No comments were received.

Action Taken

After the public comment period ended, ITAC members were asked to submit their votes by 4:00 p.m. on Friday, May 19. Eighteen (18) members voted to approve the request; zero (0) members opposed; one (1) members did not vote. The request was approved.

Chair Report: *Proposed amendment to the Information Technology Advisory Committee (ITAC) 2017 Annual Agenda. The Judicial Council Technology Committee will consider approving this addition at its June 12, 2017 meeting.*

#	Project	Priority	Specifications	Completion Date/Status	Describe End Product/ Outcome of Activity
17	**Digital Evidence Phase I: Assessment** **Investigate, Assess, and Report on Statutes, Rules, Business Practice, and Technical Standards Related to Digital Evidence** *Major Tasks:* (a) Review existing statutes and rules of court to identify impediments to use of digital evidence and opportunities for improved processes. (b) Survey courts for existing business practices and policies regarding acceptance and retention of digital evidence. (c) Survey courts and justice system groups regarding possible technical standards and business practices for acceptance and storage of digital evidence. (d) Report findings to ITAC and provide recommendations on next steps. (h) Coordinate and plan with JCIT regarding operational support, if appropriate.		***Judicial Council Direction:*** Tactical Plan for Technology Goal 1: Promote the Digital Court: Digital Evidence: Acceptance, Storage, and Retention ***Origin of Project:*** Tactical Plan for Technology 2017-2018 and ITAC members discussed need to pursue during their December 2016 annual agenda planning session and their May 5, 2017 meeting. ***Resources:*** *ITAC:* Workstream *Judicial Council Staffing:* Information Technology, Legal Services *Collaborations:* Workstream members; CEAC, TCPJAC ***Key Objective Supported:*** Goal 1	July 2018	Assessment Findings and Recommendations

CALIFORNIA JUDICIAL BRANCH

Disaster Recovery Framework

A Guide for the California Judicial Branch

VERSION 1.9

MAY 31, 2017

JUDICIAL COUNCIL
OF CALIFORNIA
INFORMATION TECHNOLOGY
ADVISORY COMMITTEE

Table of Contents

1.0 INTRODUCTION 3
2.0 DEFINITION 3
3.0 DISASTER RECOVERY FRAMEWORK 3
3.1 Scope 3
3.2 Organizational Characteristics 4
3.3 Organizational History and Importance of Disaster Recovery 4
3.4 Supporting References and Content 5
3.5 Documentation Structure 5
4.0 PURPOSE OF DISASTER RECOVERY 6
5.0 SUPPORTED AND RECOMMENDED BACKUP TECHNOLOGIES 7
5.1 Disk 7
5.2 Cloud 8
6.0 CONTINGENCY STRATEGIES 8
6.1 Backup Methods 9
6.2 Alternate Sites 10
6.3 Recovery Options 10
6.3.1 Cold site 10
6.3.2 Warm site 11
6.3.3 Hot site 11
6.3.4 Mirrored site 11
6.3.5 Cloud 11
6.4 Selecting an Option 11
6.5 Equipment Replacement 14
6.5.1 Vendor agreements 14
6.5.2 Equipment inventory 14
6.5.3 Existing compatible equipment 15
7.0 PROVEN AND AVAILABLE TECHNOLOGIES AND PRODUCTS 15
7.1 Technologies Currently Deployed in the Branch 15
7.2 Potentially Useful Technologies Not Known to be Implemented in the Branch 15
8.0 EXAMPLE SCENARIOS AND DEPLOYMENT SOLUTIONS 16
8.1 Single-Site Small or Medium JBE 19
8.1.1 Scenario 1: Cloud-based DR 19
8.1.2 Scenario 2: Court-to-court colocation 20
8.2 Medium or Large JBE With Two or More Sites in Close Proximity 22
8.2.1 Scenario 1: Cloud-based DR 22

8.2.2 Scenario 2: Colocation data center 22
8.3 Medium or Large JBE with Two or More Sites NOT in Close Proximity 23
8.3.1 Scenario 1: Cloud-based DR 23
8.3.1 Scenario 2: Secondary-site data center 24
9.0 PLANNING 25
10.0 IMPLEMENTATION 26
11.0 KEY POINTS, CONCERNS, AND COMPLIANCE 27
11.1 Backup of Microsoft Office 365 & Cloud Data 27
11.2 Abandonment of Tapes 27
11.3 Use of Primary SAN or Array 27
11.4 Use of Virtualization Cluster 27
11.5 Retention of Data (Backups) 27
11.6 Data Classifications 28
11.7 Purpose-Built Backup Appliance vs. Backup Server 28
11.8 Cloud Service Subscriptions and Payments 28
11.9 Uncompromised Access to Credentials for Recovery Systems and Cloud Platforms 29
12.0 MONITORING, TESTING, VALIDATION, AND REVIEW 29
12.1 Regular Review of Backup and Disaster Recovery Systems 29
12.1.1 E-mail notifications 29
12.1.2 Backup job monitoring and auditing 29
12.1.3 Site recovery/cutover systems monitoring and auditing 30
12.2 Routine Testing Exercises 30
12.3 Testing Simulations 30
12.3.1 Loss of building access 30
12.3.2 Loss of access to all systems (onsite or offsite) based on catastrophic outage or disaster 30
12.3.3 Backup system failure 30
12.3.4 High-availability (site recovery) system failure 31

1.0 INTRODUCTION

The Judicial Branch Disaster Recovery Framework serves as a model and aid for implementing and maintaining a lean and robust information technology (IT) disaster recovery (DR) solution. The framework and related reference materials will assist judicial branch entities (JBEs) with establishing a disaster recovery strategy and will offer recommendations and examples of products and services that can accommodate the varying needs of small to large Supreme, appellate, and superior courts. The Supreme Court, the Courts of Appeal, and the superior courts (hereafter collectively referred to as JBEs) are not required to implement the framework in its entirety; rather, the intent is to highly encourage JBEs to use the framework as a template to develop a disaster recovery strategy and solution most appropriate to their unique local business requirements. Additionally, each court's disaster recovery implementation will differ significantly based on factors such as geographic location, natural disaster risk ratings, types of hosting solutions in use, and varying business drivers. The framework is for use as a guide and versatile benchmark of what should be in place in each JBE.

This guide is intended to provide a roadmap for JBE's and does not include all the details or steps required for implementing a trusted, fail-safe disaster recovery plan or solution. It does, however, provide tools and examples for JBEs to design disaster recovery solutions appropriate to their needs and recommend ways to ensure the integrity and usefulness of the those solutions.

2.0 DEFINITION

A disaster recovery plan includes a set of branch policies, procedures, diagrams, documentation, systems, and tools "to enable the recovery or continuation of vital technology infrastructure and systems following a *natural* or *human-induced disaster*."[1] It also includes a robust redundant and/or alternate infrastructure to facilitate quick recovery of critical systems, with regular defined intervals of testing that occur to ensure the integrity of the approach.

3.0 DISASTER RECOVERY FRAMEWORK

3.1 Scope

The disaster recovery framework has been developed for the establishment of a baseline reference model for disaster recovery within the judicial branch of California. It is known that existing and future DR plans put into place by JBEs will differ from one another primarily because of varying logistics and challenges with facilities, geographic locations, funding, and/or internal requirements. To produce the framework, input was solicited from

[1] Wikipedia contributors, "Disaster recovery," *Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Disaster_recovery&oldid=772607446* (as of May 9, 2017), referencing Georgetown University, Business Continuity and Disaster Recovery, *Disaster Recovery, https://continuity.georgetown.edu/dr* (as of May 9, 2017).

multiple courts ranging in size from small to large so that a comprehensive framework could be developed that suits all entities within the judicial branch. The framework is designed to set a direction, identify and address the growing importance of DR within the branch, and ensure that the rapid evolution and adoption of technology within the branch are complemented with a plan to ensure the integrity of electronic data and systems.

The goals of the framework are to:

- Suggest and define model disaster recovery guidelines for the branch;
- Suggest and define standard recovery times and priorities for each of the major technology components of the branch;
- Be usable by all judicial branch entities as a court's disaster recovery plan;
- Provide baseline guidance for backups and high-availability options and scenarios for JBEs to incorporate into their disaster recovery strategies;
- Provide visual reference of various disaster recovery scenarios;
- Provide guidance to all members of the judicial branch on establishing methods of applying disaster recovery and therefore ensuring the integrity, survivability, and recoverability of various systems and data; and
- For each platform, operating system, application, and security device, provide the basis for the development of implementation standards, procedures, and guidelines that can then be monitored and enforced against the recommendations defined in the framework.

3.2 Organizational Characteristics

The framework establishes how various systems and data are to be backed up and protected from data loss and will be made highly available to mitigate the chances that the disaster recovery plan would need to be relied on. Some judicial branch entities interface and share data with one another, increasing the complexities and risk factors of data ownership and protection. Additionally, because of the complex inner workings of the judicial branch and each individual JBE, each court's Continuity of Operations Plan (COOP) overlaps. The IT DR plan and all related material should be placed into and support the COOP. It is not, however, a replacement for the COOP, and neither is the COOP a holistic solution for IT disaster recovery.

3.3 Organizational History and Importance of Disaster Recovery

Over the past decade, JBEs have increasingly deployed more and more technology to increase operational efficiencies, improve public access to justice, and to streamline

interaction with various justice partners. Specifically, over the last four years, as a result of budget reductions and other hardships, some JBEs have elected and others were forced to deploy and host their own case management systems: systems that were once managed by a central entity or provider (e.g., the judicial branch, with its California Courts Technology Center [CCTC] or a respective county). Additionally, some JBEs have begun using cloud-provided services, systems, and software, drastically changing the traditional approach to disaster recovery and how data is backed up and preserved.

3.4 Supporting References and Content

Following are some sources and publications that the Judicial Council's Information Technology Advisory Committee (ITAC) referenced in the development of this framework:

- Next Generation Hosting Strategy Workstream output(s) (ITAC deliverable pending)
- Information Systems Controls Framework (Judicial Council and ITAC deliverable)
- California Courts Technology Center
- NASCIO—*Cyber Disruption Response Planning Guide* (*www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf*)
- National Institute of Standards and Technology—Special Publication 800-34 Rev. 1 (Contingency Planning Guide for Federal Information Systems) (*http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*)

3.5 Documentation Structure

An IT disaster recovery plan is supported by documentation that captures differing levels of detail while ensuring that the plan is flexible enough to adapt as organizational and IT priorities and dependencies change. The IT disaster recovery framework should consist of the following categories of documents:

- Organizational policy (for JBEs)—expresses management's expectations regarding disaster recovery and importance of data, including expectations for time to recover based on categorized tiers of data types and importance.
- IT department policy—further refines management's expectations, specifically of data protection from a technical perspective and for safeguarding electronic data from loss or destruction within specified parameters, as defined by the local entity. The department policy informs IT staff of the department's comprehensive approach toward disaster recovery, ensuring that all subdivisions in the department are working cohesively to comply.

- List of systems/data categorized by recovery time—a complete categorized list of data assets broken into tiers of criticality, including specific hardware, systems, software, and data that support the mission of the JBE. This document includes the ITAC-recommended criticality ranking of many systems; however, local organizational policy within each JBE may necessitate changes to the list.

- List of appendixes
  - Appendix A: List of high-level technical requirements and systems and data categorized by recovery time
  - Appendix B: Recommended minimum requirements for a backup solution

- List of types of events that would trigger the declaration of a disaster or operational crisis to the JBE/region
  - Loss of data center (natural, by fire, by water, etc.)
  - Infrastructure or major equipment failure
  - Power outage or significant voltage surge
  - Cloud-hosted–circuit outage (single point of failure) or cloud data center outage (single point of failure)
  - Severing of communication cables (cut fiber, etc.)
  - Security breach
  - Data hostage situation (e.g., ransomware)
  - Malicious behavior—internal sabotage
  - Malicious behavior—vendor sabotage

- Checklists
  - Planning
  - Implementation and milestones
  - Verification and testing

- Guidelines—recommendations that can be used when other guidance has not been established. Guidelines are usually created at lower operational levels, such as by departments, to address immediate needs until consensus is reached on broader direction.

4.0 PURPOSE OF DISASTER RECOVERY

Data and electronic information are paramount to the operation and success of each judicial branch entity. The broad term *information system* is used to identify a human and electronic process for the collection, organization, storage, and presentation of information. Consistent with that of other industries, JBEs' use of systems and technology has increased over time. Any JBE would be challenged to continue normal operations without systems that have become integral to business process.

The purpose of IT disaster recovery is to restore or maintain operations of technology systems supporting critical business functions following a natural or human-induced disaster. Although this

document focuses primarily on IT disaster recovery, it is important that the disaster recovery plan support and align with the business continuity plan and/or other established plans and protocols that JBEs have in place (e.g., Continuity of Operations Plan, *https://coop.courts.ca.gov*).

Consideration should also be given to aligning the JBE disaster recovery plan to those of applicable justice partner agencies. The goal is to facilitate restoration of related or dependent services across agencies where possible.

Technologies such as backup, off-site storage, replication, and private/hybrid cloud, and metrics such as recovery point objective (RPO) and recovery time objective (RTO) are all valid discussion points and planning considerations when reviewing disaster recovery options.

A disaster recovery plan should be tailored to the individual JBE, with the goal that vital systems are preserved and made operational at performance, availability, and cost levels that meet JBE business continuity objectives.

5.0 SUPPORTED AND RECOMMENDED BACKUP TECHNOLOGIES

5.1 Disk

A disk is a data storage device used for storing and retrieving digital information. It is a type of nonvolatile memory, retaining stored data even when powered off.[2]

- Pros
  - **Local**. Data is on the premises and therefore within your control.
  - **Speed**. Because data is local, it is typically accessed from internal networks that are capable of providing faster access times. There is also no overhead from latent internet bandwidth.
  - **Security**. Disks are not managed by a third party, which can protect your data from hacking and loss of privacy.

- Cons
  - **Management**. Controlling access to data—including virus protection and vulnerability protection—becomes the responsibility of the local agency.
  - **Cost**. Disks require upfront capital expense in addition to ongoing maintenance contracts when used in mission-critical applications.
  - **Physical security**. Protection from physical threats including fire, water damage, and natural disaster are paramount and become the responsibility of the local agency.

[2] Wikipedia contributors, "Cloud computing," *Wikipedia, The Free Encyclopedia,* *https://en.wikipedia.org/wiki/Hard_disk_drive* (as of May 30, 2017).

5.2 Cloud

"Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand."[3]

- Pros
  - **Cost**. Onsite hardware and capital expenses are unnecessary and storage costs relatively low because you pay only for the storage you require.
  - **Expansion**. Scalable architecture allows for convenient provisioning of additional storage space as needed.
  - **Offsite location**. Data can be stored in geographically distant locations, possibly preventing loss from disaster.
  - **Physical security**. Leading cloud providers typically assume the responsibility of keeping your data highly secure and mirrored across multiple centers within the United States. *Note: When using a cloud vendor, care should be taken to ensure all of a JBE's data—including all replicas—are housed and maintained within the United States. Additionally, it is important to clearly analyze and understand what level(s) of data protection and recovery options the cloud provider includes or offers.*

- Cons
  - **Outages**. If the Internet goes down on your side or on your cloud provider's side, you won't have access to your information.
  - **Bandwidth**. Large amounts of bandwidth are required to conduct storage transfers.
  - **Exclusivity**. Once data has been transferred and procedures have been implemented, moving storage to another provider may be challenging.
  - **Privacy and security**. With private data exposure and data hostage situations becoming more commonplace, the cloud poses newer and varying security risks, some of which are still unknown. Careful analysis and IT controls should be framed around managing permissions (both internal and external); confidentiality of intellectual property; accidental and intentional deletion on individual, shared and cloud drives; and clear-cut audit trails.

NOTE: Tape technology is not a current or acceptable backup medium for production and/or critical data.

6.0 CONTINGENCY STRATEGIES

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the business impact analysis. Several alternatives should be considered when

[3] Wikipedia contributors, "Cloud computing," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/wiki/Cloud_computing (as of May 30, 2017).

developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the business impact analysis and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice will depend on the incident, type of system and operational requirements. Specific recovery methods should be considered and may include commercial contracts with cold, warm, or hot backup-site vendors (see section 6.3); cloud providers; mirrored sites (see section 6.3.4); reciprocal agreements with internal or external organizations; and service-level agreements (SLAs) with the equipment vendors. In addition, technologies such as RAID (redundant array of independent disks), automatic failover, uninterruptible power supplies, and mirrored systems should be considered when developing a system recovery strategy.

6.1 Backup Methods

System data should be backed up regularly. Policies should specify the frequency of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Data may be backed up on magnetic disks, cloud storage or other common-day and reliable mediums. The specific method for conducting backups should be chosen based on system and data availability and integrity requirements. Methods include electronic vaulting, storing to mirrored disks (using direct-access storage devices [DASDs] or RAID), and storing to cloud provided storage platforms.

Storing backed-up data offsite is *essential* business practice. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. With offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data were required—for recovery or testing, for example—the organization would contact the storage facility and request specific data/disks to be transported to the organization or to an alternate facility. Commercial storage facilities often offer media transportation and response and recovery services.

When selecting an offsite storage facility and vendor, the following criteria should be considered:

- Geographic area—distance from the organization and the probability of the storage site's being affected by the same disaster that might strike the organization

- Accessibility—length of time necessary to retrieve the data from storage, and the storage facility's operating hours
- Security—security capabilities of the storage facility and employee confidentiality, which must meet the data's sensitivity and security requirements
- Environment—structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls)
- Cost—cost of shipping, operational fees, and disaster response and/or recovery services

6.2 Alternate Sites

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, the plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

- Dedicated site owned or operated by the organization
- Reciprocal agreement or memorandum of agreement with an internal or external entity
- Commercially leased facility

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three types of alternate sites may be categorized in terms of their operational readiness. Based on this factor, sites may be identified as cold, warm, hot, mobile, or mirrored sites. Progressing from basic to advanced, the sites are described below.

6.3 Recovery Options

6.3.1 Cold site

A cold site typically consists of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities.

6.3.2 Warm site

Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. A warm site is maintained in an operational status ready to receive the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as a normal operational facility for another system or function, and in the event of contingency plan activation, the normal activities are displaced temporarily to accommodate the disrupted system.

6.3.3 Hot site

Hot sites are office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, seven days a week. Hot-site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated.

6.3.4 Mirrored site

Mirrored sites are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data are processed and stored at the primary and alternate sites simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

6.3.5 Cloud

A cloud "location" can serve as warm, hot, or mirrored site and have a number of other benefits and purposes. Cloud offerings can provide remote and virtual infrastructure and are typically rated at a high-tiered classification for uptime, reliability, and scalability. Contracted services are often available through cloud providers to help with a JBE's disaster recovery strategy and goals that require technical assistance by the cloud provider. For additional offerings and recommendations relative to the cloud, please reference the judicial branch Next Generation Hosting Strategy Workstream deliverables.

6.4 Selecting an Option

The cost and ready-time differences among the four options are obvious. The mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain; however, they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. The selection of fixed-site locations should account for the time and mode

of transportation necessary to move personnel there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) that affected the organization's primary site. The table below summarizes the criteria that can be employed to determine which type of alternate site meets the organization's requirements. Sites should be analyzed to ensure that the security, management, and operational and technical controls of the systems to be recovered are compatible with the prospective site. Such controls may include firewalls and physical access controls, data remanence controls, and security clearance levels of the site and staff supporting the site.

Alternate-Site Selection Criteria

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold	Low	None	None	Long	Fixed
Warm	Medium	Partial	Partial/Full	Medium	Fixed
Hot	Medium/High	Full	Full	Short	Fixed
Mirrored	High	Full	Full	None	Fixed

These alternate sites may be owned and operated by the organization (internal recovery), or commercial sites may be available under contract. Additionally, cloud providers can provide IaaS (Infrastructure as a Service) computing that mimics a colocation site and offers near-unlimited services and opportunities. If contracting for the site with a commercial vendor, adequate testing time, workspace, security requirements, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during the recovery period) must be negotiated and clearly stated in the contract. Customers should be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation will be addressed and how priority status is determined should be negotiated.

Two or more organizations with similar or identical IT configurations and backup technologies may enter into a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. With sites that serve as alternate sites for each other, a reciprocal agreement or memorandum of understanding (MOU) should be established. A reciprocal agreement should be entered into carefully because each site must be able to support not only its own workload but the other organization's as well, in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and sensitivity of data that

might be accessible by other privileged users, in addition to functionality of the recovery strategy.

An MOU, memorandum of agreement (MOA), or a service level agreement (SLA) for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities. The legal department of each party must review and approve the agreement. In general, the agreement should address at a minimum, each of the following elements:

- Disaster declaration (i.e., circumstances constituting a disaster and notification procedures)
- Site and/or facility priority access and/or use
- Site availability
- Site guarantee
- Other clients subscribing to the same resources and site, and the total number of site subscribers, as applicable
- The contract or agreement change or modification process
- Contract or agreement termination conditions
- The process to negotiate extension of service
- Guarantee of compatibility
- IT system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software)
- Change management and notification requirements, including hardware, software, and infrastructure
- Security requirements, including special security needs
- Whether staff support is provided
- Whether facility services are provided (use of onsite office equipment, cafeteria, etc.)
- Testing, including scheduling, availability, test time duration, and additional testing, if required
- Records management (onsite and offsite), including electronic media and hard copies

- Service-level management (performance measures and management of quality of IT services provided)
- Workspace requirements (e.g., chairs, desks, telephone, PCs)
- Supplies provided or required (e.g., office supplies)
- Additional costs not covered elsewhere
- Other contractual issues, as applicable
- Other technical requirements, as applicable

6.5 Equipment Replacement[4]

If the IT system is damaged or destroyed or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster.

6.5.1 Vendor agreements

As the contingency plan is being developed, SLAs with hardware, software, and support vendors may be made for emergency maintenance service. An SLA should specify how quickly the vendor must respond after being notified. The agreement should also give the organization priority status for the shipment of replacement equipment over equipment being purchased for normal operations. SLAs should further discuss what priority status the organization will receive in the event of a catastrophic disaster involving multiple vendor clients. In such cases, organizations with health- and safety-dependent processes will often receive the highest priority for shipment. The details of these negotiations should be documented in the SLA, which should be maintained with the contingency plan.

6.5.2 Equipment inventory

Required equipment may be purchased in advance and stored at a secure off-site location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the alternate site. This solution has certain drawbacks, however. An organization must commit financial resources to purchase this equipment in advance, and the

[4] Section 6.5 is taken from NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010), § 3.4.4, pp. 24–25, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf (as of May 10, 2017).

equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.

6.5.3 Existing compatible equipment

Equipment currently housed and used by the contracted hot site or by another organization within the agency may be used by the organization. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

When evaluating the choices, the contingency planning coordinator should consider that purchasing equipment when needed is cost-effective, but can add significant overhead time to recovery while waiting for shipment and setup; conversely, storing unused equipment is costly, but allows recovery operations to begin more quickly. Based on impacts discovered through the business impact analysis, consideration should be given to the possibility of a widespread disaster requiring mass equipment replacement and transportation delays that would extend the recovery period. Regardless of the strategy selected, detailed lists of equipment needs and specifications should be maintained within the contingency plan.

7.0 PROVEN AND AVAILABLE TECHNOLOGIES AND PRODUCTS

7.1 Technologies Currently Deployed in the Branch

The following currently deployed technologies and in use throughout the branch help JBEs meet their disaster recovery plan objectives:

- Barracuda Backup with secondary Barracuda Backup appliance and/or cloud replica(s)
- Barracuda Cloud-to-Cloud Backup
- Barracuda Essentials for Office 365
- VMware Site Recovery Manager
- Various cloud providers
- Various storage area network (SAN) solutions with “snapshot” and “lagged mirror” technology

7.2 Potentially Useful Technologies Not Known to be Implemented in the Branch

Following are examples of technologies that are believed not yet to have been implemented in the branch, but that exhibit strengths in disaster recovery objectives:

- Veeam Backup & Replication with cloud replica
- Rubrik Cloud Data Management with cloud replica
- Amazon Web Services (AWS) Storage Gateway
- Microsoft Azure Site Recovery
- Veeam DRaaS (Veeam Cloud Connect)

NOTE: The products and/or technologies listed above are for baseline reference purposes only. JBEs do not have to choose one of these solutions, but rather can use the technologies on the list or reference the list to determine what solutions best fit within their technology environments and meet their recovery objectives.

8.0 EXAMPLE SCENARIOS AND DEPLOYMENT SOLUTIONS

Disaster recovery scenarios can be very complex and impossible to work out without specific details. Sections 8.1–8.3 offer guidelines for some general scenarios. Note that a number of caveats to implementation must be taken into account when creating a disaster recovery scenario, including the following:

- **Identify business-critical servers and data**. Identifying the business-critical servers and data will provide the information required to size the disaster recovery scenario. This information is critical to scenarios pertaining to cloud services and physical hardware.
- **Determine data circuit requirements**. Using the information from the identifying server and data needs will allow the JBE to determine the bandwidth requirements to support the replication and synchronization of the DR scenario.
- **Identify technology to facilitate DR**. Identifying the technologies in use is important. DR scenarios are intended to assist in implementing a DR plan for IT and so focus on electronic data. However, JBEs may have critical data that are not in electronic format. Therefore, the JBE needs to identify technologies that can be used to assist in the DR plan. As an example, if a court has gone paperless, it can store the documentation for cases on the cloud, leaving the documentation accessible during an outage or disaster. However, if the court still stores paper case files, in the event of a disaster the court may lose those paper files and be unable to recover them. Another component that can support a JBE's DR strategy is through the use of virtualization technology, which allows for easy transfer of servers between data center and cloud.
- **Identify physical requirements**. Many of the scenarios in section 8.0 require physical hardware and, therefore, the related space, racks, servers, network equipment, and appliances. It

is important to identify what equipment will be necessary and to ensure that power and cooling are sufficient to meet the needs of that equipment following a disaster. However unlikely it is, these scenarios may one day be running the critical court operations for a JBE, and they should be provided similar resources to the primary data center.

To discuss DR scenarios effectively, a common starting point for the differing terminology is also essential. In many cases, different definitions for the same terminology are floating in the ether. Below are several relevant terms and their definitions:

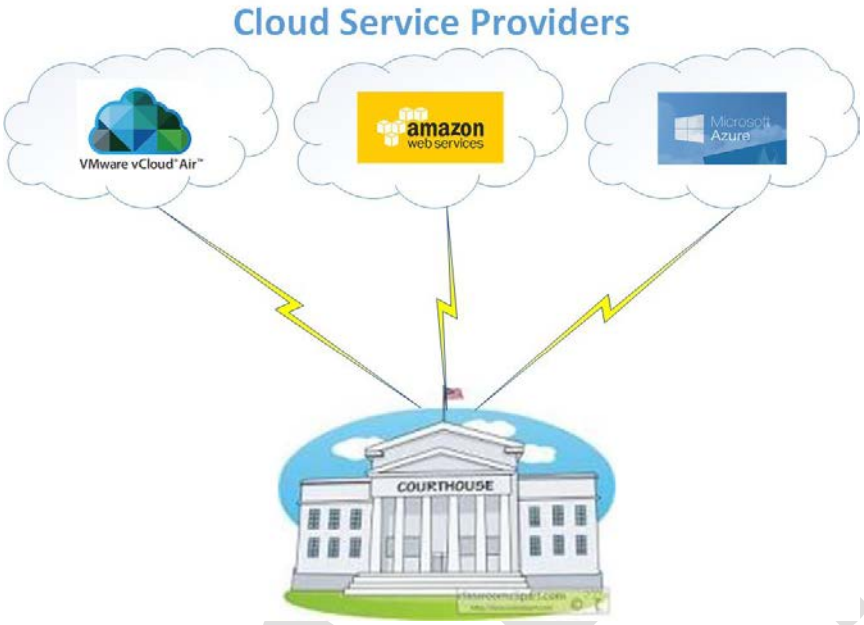
- Public cloud—a network of remote servers and storage hosted by a vendor and accessible on the Internet. It allows for the storage, management, and processing of data offsite, rather than using local resources. Cloud advantages include scalability, instant provisioning, and virtualization of resources. The public cloud typically shares resources among many tenants or customers.

- Private cloud—similar to a public cloud, but resources are dedicated to a single tenant or customer. A private cloud can also reside on the premises, providing the benefits of local use and control while leveraging the benefits of a cloud computing platform. Examples of on-premises private cloud solutions are VMware, Nutanix, and Microsoft Hyper-V hypervisor. On-premises private cloud offers the same advantages as any other cloud, including scalability, instant provisioning, and virtualization.

- Hybrid cloud—a cloud computing environment using a mix of cloud services (public and private) and on-premises hardware (standard data center) to facilitate communication between a data center and cloud services.

- Cloud service providers—vendors who sell public and private cloud services and hybrid solutions. Top-tier cloud service providers include Amazon Web Services, Google, Microsoft, VMware and Oracle. The top-tier providers offer comprehensive solutions for virtually any cloud computing needs with multiple cloud service locations to ensure maximum survivability.

Figure 1. Cloud Service Providers



- Disaster recovery (DR)—a set of policies and procedures to enable recovery of critical technology infrastructure and systems following a major outage or disaster. DR's main goal is to protect data and ensure that business can resume as quickly as possible following an event.

- Business continuity (BC)—the ability to continue to deliver services at a predefined level following an outage or disaster. Whereas DR allows you to protect data and rebuild, BC allows you to continue running through the outage or as soon as possible thereafter depending on the specific events.

- Colocation data center—a third-party data center where rack space can be rented to host physical hardware such as servers and appliances. Colocation data centers have a rating supplied by the Uptime Institute to let you know how much uptime you can expect. The ratings range from Tier I to Tier IV, with the highest tier providing the highest uptime and fault tolerance.
  - Tier I: Minimum of 99.671 percent availability, with no redundancy in power, cooling, or network
  - Tier II: Minimum of 99.741 percent availability; N+1 redundancy in power and cooling
  - Tier III: Minimum of 99.982 percent availability; N+1 redundancy in power, cooling, and network, with multiple uplinks for data
  - Tier IV: Minimum of 99.995 percent availability; 2N+1 redundancy in power, cooling, and network, with multiple uplinks for data

  Examples of Tier III and Tier IV data centers are Recovery Point's Gaithersburg Data Center and Switch's SUPERNAP, respectively.

- Data egress and ingress—data traffic in and out of the cloud. Egress data traffic comes from an external source into the cloud. Think of this as uploading data to the cloud, such as when

backing up data to the cloud or synchronizing on-premises servers with servers in the cloud. Ingress data traffic comes from the cloud to on-premises servers. Think of this as the download of data from the cloud, such as in a data recovery from cloud storage or when accessing running servers in the cloud. The terminology is important because vendors charge different amounts per gigabyte depending on whether the data constitutes egress or ingress traffic.

- Load balancers—appliances that manage redundant systems, allowing users to be directed to different servers for the same data. For example, load balancing can be used for a SharePoint intranet site to point the user to one of two redundant SharePoint servers (e.g., Sharepoint1 or Sharepoint2) to balance the number of connections and bandwidth. A load balancer can also be used to point to one application or server primarily and point to a secondary one in the event of an outage.

- Tapeless backup appliance—an appliance designed to replace a tape backup system. Typically, these appliances consist of a large amount of storage to hold backups. The appliance also often has data management tools built in. Various backup appliances also have native support for many top-tier cloud service providers to ensure seamless data replication.

- Warm or hot sites—physical locations for DR and their availability. Warm sites consist of hardware and network connectivity to support production but are not 100 percent up to date, require manual intervention, and can take hours or days to bring online. Hot sites are duplicates of production environments with real-time synchronization; they run concurrently with the main production site. Switching to a hot site can take minutes to bring online.

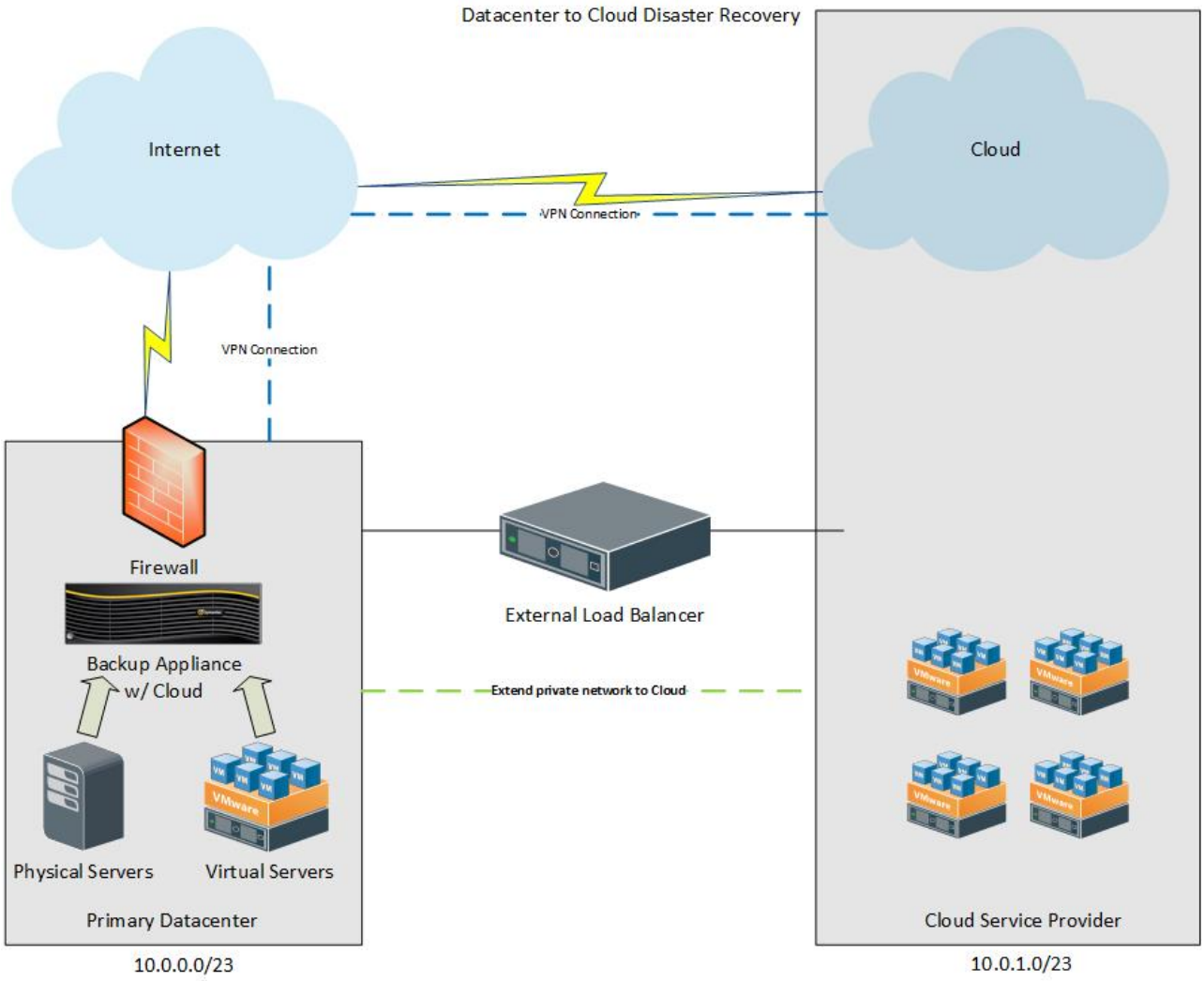
8.1 Single-Site Small or Medium JBE

8.1.1 Scenario 1: Cloud-based DR

Cloud-based **DR** is the preferred **DR/BC** scenario. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters. Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be

implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

Figure 2. Cloud-Based DR Diagram

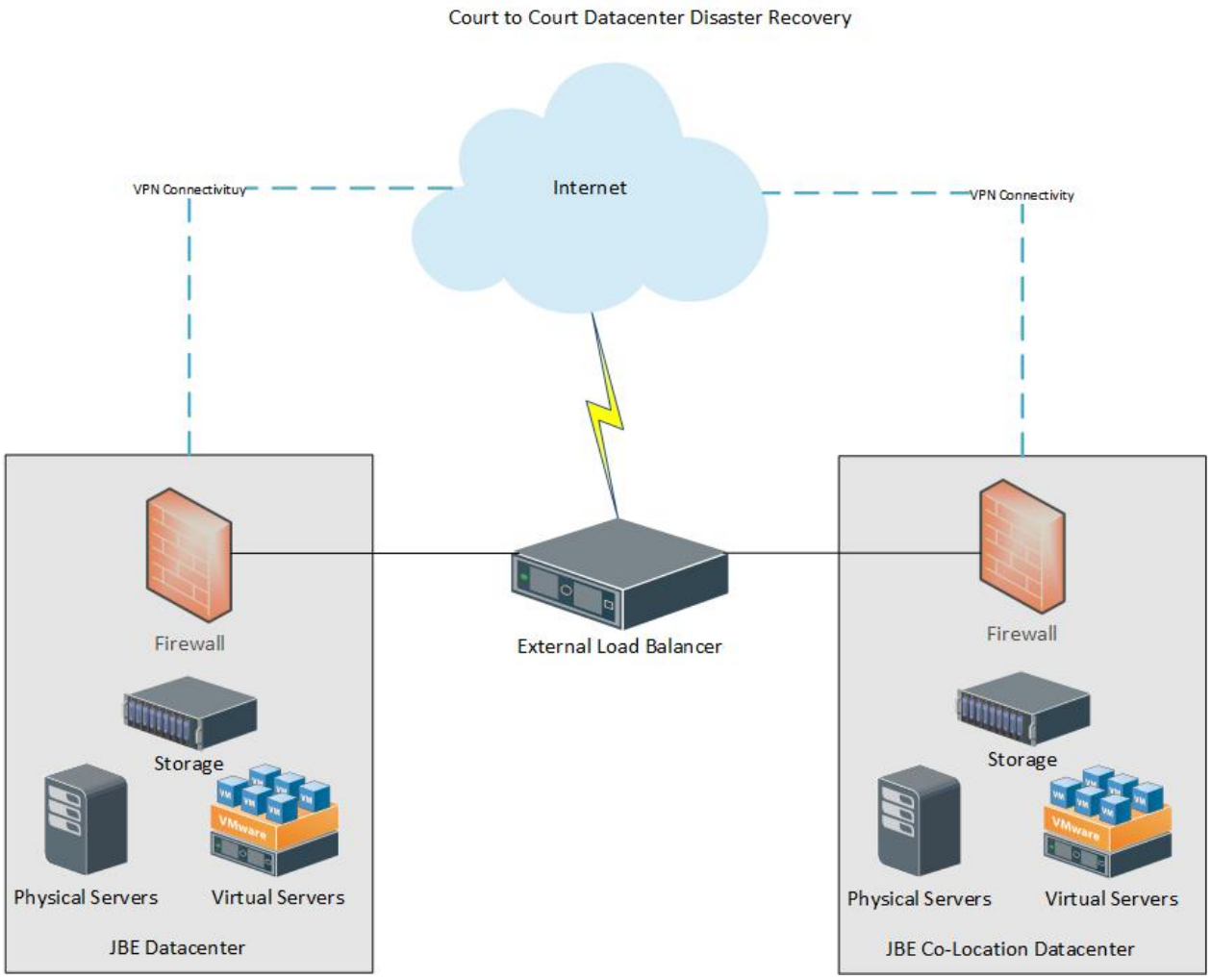


8.1.2 Scenario 2: Court-to-court colocation

Court-to-court colocation involves two similar courts in geographically diverse locations. A memorandum of understanding needs to be put into place to accommodate the complexities of this option. Implementation of this type of agreement requires a JBE to lend or borrow space in a JBE data center for racks of equipment. The JBE has to put a dedicated data circuit in the borrowed data center of an appropriate size based on requirements. In this scenario, each critical server or appliance requires a similar hardware setup, whether physical or virtual. In addition,

replication has to be implemented and managed for SQL, data, and other servers. Network components also need to be in place to allow the JBE to route to the **warm or hot** redundant **sites**. Several appliances and tools can assist with running a **warm or hot site**. **Load balancers** are crucial for routing to allow the JBE to point its server addresses to different IPs. These appliances can be set up so that if one of them is down, the external IP addresses can route to the standby **load balancer**. Other options such as hosted websites and tools that may be unavailable in the event of a disaster or outage can help in moving production.

Figure 3. Court-to-Court Colocation Diagram



8.2 Medium or Large JBE with Two or More Sites in Close Proximity

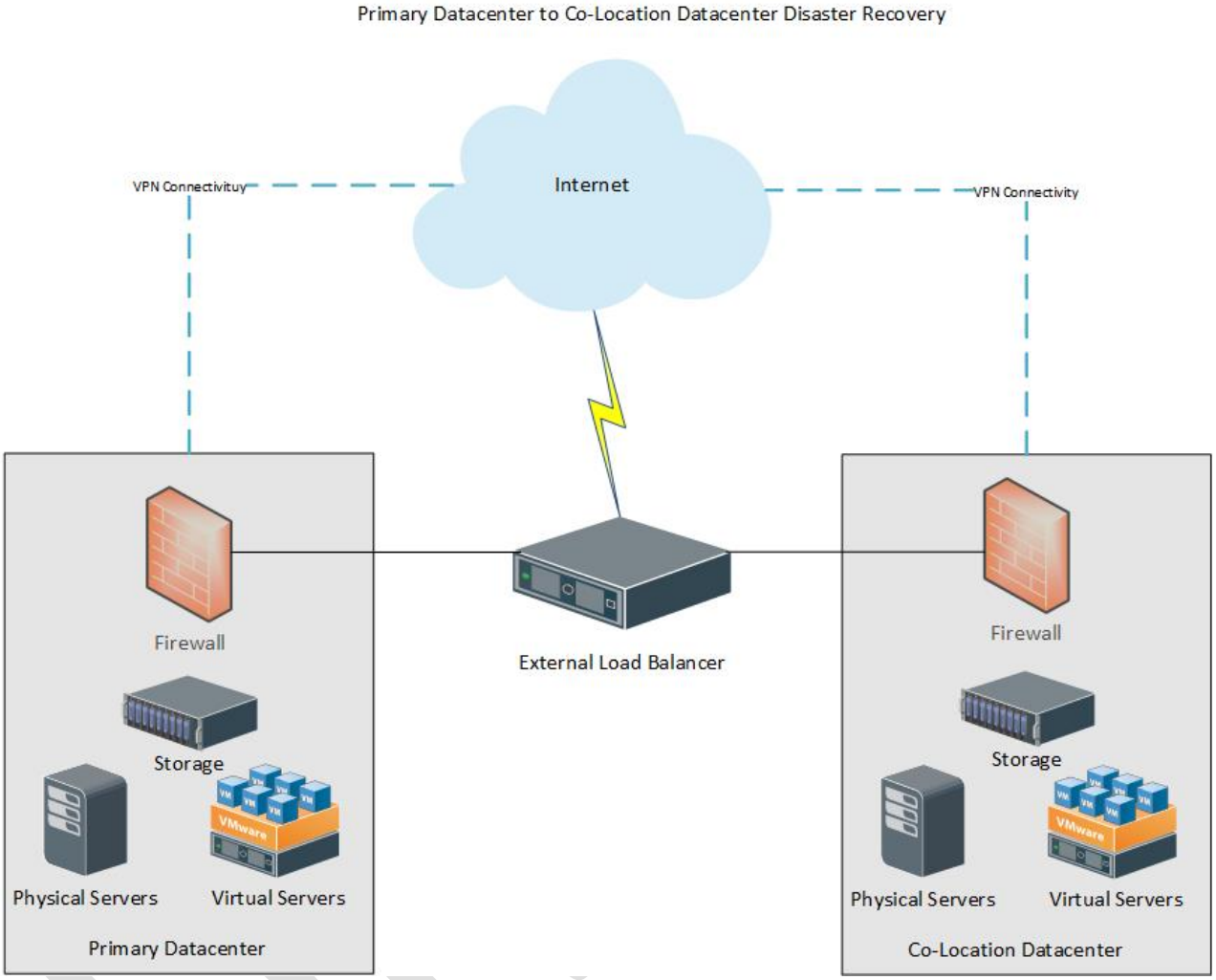
8.2.1 Scenario 1: Cloud-based DR

As stated in section 8.1.1, cloud-based **DR** (see figure 2, above) is the preferred **DR/BC** scenario. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters. Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

8.2.2 Scenario 2: Colocation data center

In this scenario, a JBE uses a third-party data center to host the physical and virtual servers and appliances. Using a **colocation data center** to host data requires the JBE to install a dedicated circuit (sized appropriately per requirements) at both locations to ensure full data replication and synchronization. Each critical server requires a similar hardware setup, either physical or virtual. In addition, replication and synchronization has to be implemented and managed for SQL, data, and other services. Network components also need to be in place to allow the JBE to route to the **warm or hot sites**. **Load balancers** are crucial for routing to allow the JBE to point its server addresses to different IPs. These appliances can be set up so that if one of them is down, the external IP addresses can route to a standby **load balancer** hosted at the **colocation data center**. Other considerations include hosted websites and tools that may be unavailable in the event of a disaster or outage.

Figure 4. Colocation Data Center Diagram



8.3 Medium or Large JBE with Two or More Sites NOT in Close Proximity

8.3.1 Scenario 1: Cloud-based DR

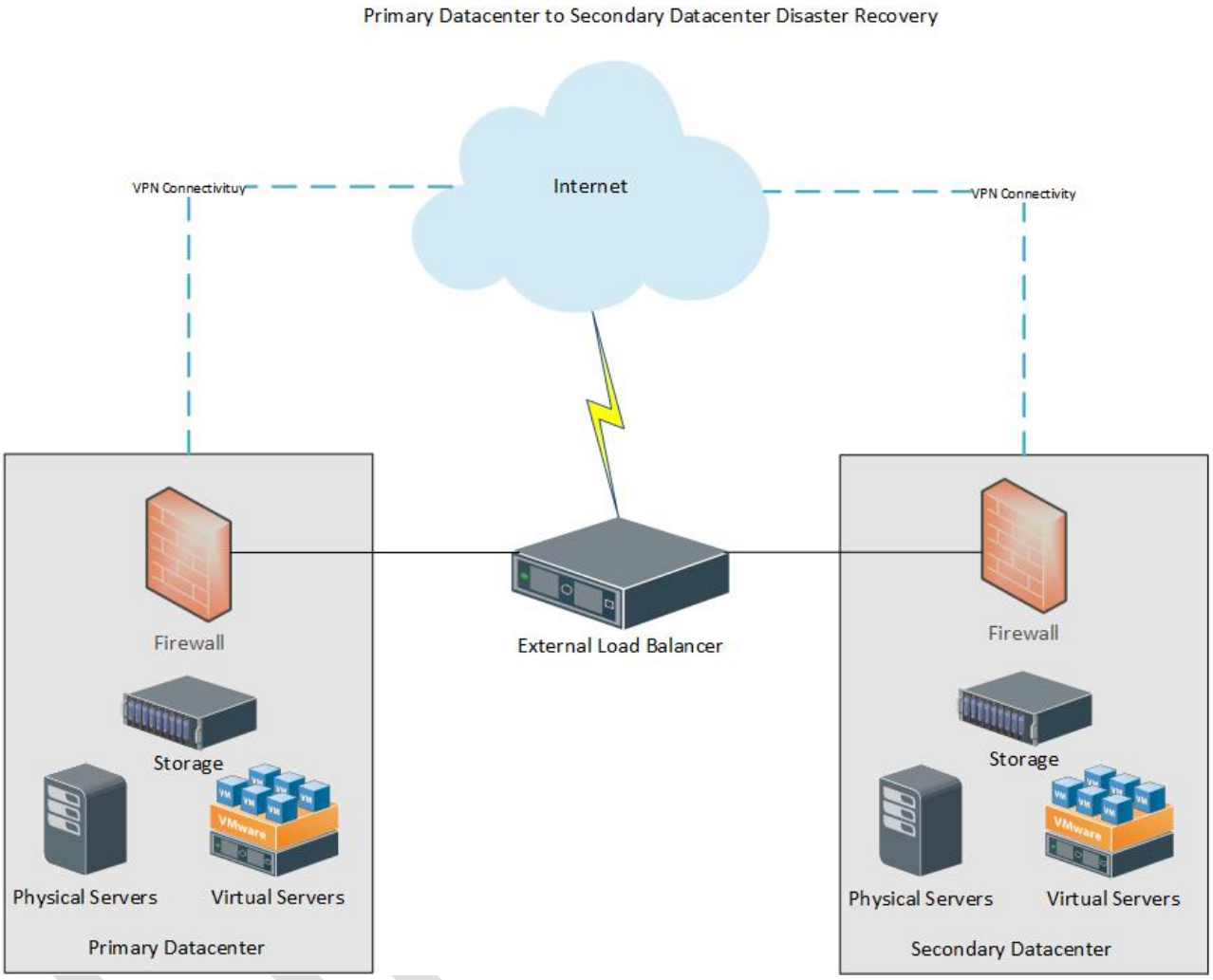
As with single-site JBEs and those with two or more sites in close proximity, cloud-based **DR** (see figure 2, above) is the preferred **DR/BC** scenario for JBEs with two or more sites *not* in close proximity. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers

and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters. Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

8.3.1 Scenario 2: Secondary-site data center

A secondary-site data center is similar to a **colocation data center.** It uses a secondary court site as a redundant data center, which typically requires an increase in bandwidth at the secondary site as well as a dedicated data circuit (sized appropriately per requirements) between the two data centers to ensure data replication and synchronization. Each critical server requires a similar hardware setup, either physical or virtual. In addition, replication has to be implemented and managed for SQL, data, and other services. Network components also need to be in place to allow the JBE to route to the **warm or hot sites. Load balancers** are crucial in this scenario to allow the JBE to point its server addresses to different IPs. These addresses can be set up so that if one of them is down, the external IP addresses can route to the standby **load balancer** located at the secondary site as needed. Other considerations include hosted websites and tools that may be unavailable in the event of a disaster or outage.

Figure 5. Secondary-Site Data Center Diagram



9.0 PLANNING

As with any organizational undertaking, planning is an essential element in developing a solid and useful disaster recovery plan. The JBEs in California operate within a vast range of geographical, urban, and rural environments; earthquake zones and wildfire areas; and adjacencies to other JBEs. The California JBEs have varying caseloads and case types and diverse physical plants. Each possesses automation and other mission-critical support systems that differ in small or large ways from those of neighboring JBEs. For these reasons, a one-size-fits-all approach cannot work and, therefore, this document cannot specify exactly how an individual court should approach the planning effort. Each court will have its own unique set of factors to consider in developing its disaster recovery plan.

Likewise, the relative size and complexity of each court's organizational and staffing components will largely dictate the formality of the planning effort. The smallest court unit may be able to

develop a viable plan with a relatively informal and simple effort, where a large urban court may need a more elaborate and formal approach.

An important element of any DR planning effort is to first identify and thereafter coordinate as appropriate with the court's stakeholders, including internal stakeholders (judicial officers, court managers and staff, and other elements of the court family) and external stakeholders (other agencies, bar groups and law firms, vendors, and utility providers, to name a few).

In this regard, each court needs to assess the extent to which its stakeholders should be represented and involved from the outset and the level and extent of their continuing involvement throughout the planning phase. As has already been noted, what is optimal for a small rural court will likely differ significantly from what is optimal for a large urban court. Hence, stakeholder involvement should be as large and diverse as resources and practicality permit. Disaster recovery planning is most definitely an area where more stakeholder involvement is better than less.

10.0 IMPLEMENTATION

The fate of most policy and procedure manuals is to be placed on a bookshelf to gather dust. Most manuals are intended primarily for reactive reference: A discrete question comes up and a manual is pulled down from the shelf, consulted, and put back to gather more dust. Mostly, however, it stays on the shelf until a question arises.

A disaster recovery plan by its very nature, however, needs to be viewed and studied as a road map containing a cohesive set of well-thought-out procedures and steps for pre-disaster planning and preparations, continued operation during a disaster, and post-disaster response. It is intended as a tool for an organization to *prepare itself before a disaster*, as much as it is a road map for the recovery therefrom.

For this reason, it is important that the contents of the Disaster Recovery manual be widely disseminated and studied throughout the court. *All court stakeholders* who may be affected by a disaster and have a role in the recovery therefrom *should be made fully aware of the disaster recovery plan and its contents.*

As with the planning phase, described in section 9.0, the nature and extent of the dissemination and study will vary from court to court based on each court's individual environment and situation. In a small court, implementation might consist primarily of an all-hands meeting to review it and respond to questions and concerns. In the largest JBEs, such an approach is unlikely to prove practical or effective, and a more formal and involved process will be required.

11.0 KEY POINTS, CONCERNS, AND COMPLIANCE

11.1 Backup of Microsoft Office 365 & Cloud Data

E-mail, hosted offsite and in Office 365, should be backed up by a trusted third-party backup service or product. Such cloud-to-cloud backups not only protect against catastrophic failure that Microsoft could experience in its data centers, but also protect the JBE against malicious or unintentional deletions of e-mail and allow for speedy recovery of e-mail. Likewise, all cloud-based OneDrive and SharePoint data including all other cloud-based critical data should be protected by a cloud-to-cloud backup solution.

11.2 Abandonment of Tapes

JBEs should be making efforts to separate from and decommission tape technologies for primary backup purposes, unless no other options are compatible with specific systems (e.g., AS/400). As budget and time permit, JBEs should also be looking to abandon tape backups *entirely*, including at secondary sites and for noncritical nonproduction data, and instead use the recommended backup media identified in this document.

11.3 Use of Primary SAN or Array

JBEs should never use their primary SAN and/or primary storage arrays for backup purposes. The backup environment, other than network, should be kept 100 percent separate from production storage and/or computing platforms. The only exception is for staging, test, or development systems, where a loss would not affect business operations.

11.4 Use of Virtualization Cluster

JBEs should never use their virtualization clusters, specifically a cluster served by the primary SAN or array, for backup purposes. The backup environment should be kept 100 percent separate from other resources or depend on them as little as possible.

11.5 Retention of Data (Backups)

Choosing what data to retain is a very JBE-specific decision and depends on local operating principles, local SLAs, budget for appropriate backup resources, infrastructure, and laws and rules. As with document destruction, an appropriate backup architecture should be implemented at a court that supports the JBE's retention and/or destruction requirements and aligns to the business drivers to which the JBE has committed.

11.6 Data Classifications

This framework covers the process and methods for data classification only in part, because that focus is typically a balancing act between compliance, discovery, and protection. However, larger JBEs will find that classifying data will help reduce any consumption or utilization constraints around SANs, disks, backups, and high-availability solutions. The rules for data and compliance are very specific, and so at each JBE, intake and classification of the data from various sources, such as those that follow, are important:

- **Payment Card Industry (PCI)**. Reference PCI resources and/or your merchant account provider for relevant information.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**. Reference HIPAA resources and/or your local county for relevant information.
- **California Law Enforcement Telecommunications System (CLETS)**. Reference CLETS documents or contact your CLETS contact for relevant information.

11.7 Purpose-Built Backup Appliance vs. Backup Server

The industry allows JBEs to select any available backup solutions that meet their needs and align to the Judicial Branch *Disaster Recovery Framework*. JBEs should assess their environments to select an appropriate backup solution that presents the fewest risks and is least disruptive to ongoing management efforts. Some backup solutions are designed as purpose-built appliances (non-Microsoft) rather than traditional Microsoft Windows servers with a backup software application installed. Purpose-built appliances are recommended over traditional Microsoft Windows backup servers because they are immune to or far less affected by common-environment outages (Microsoft's Active Directory and the like) and less susceptible to malware targeted specifically for Microsoft-based servers. In a crisis, dependencies can impede recovery activities and compromise a JBE's ability to focus on restoration of data.

11.8 Cloud Service Subscriptions and Payments

Based on how the California State Controller's Office (SCO) operates, in addition to the time it takes for invoices and approvals for payment to work their way through the process, payments to contracted vendors and organizations can often be delayed. Many vendors require payment in full within 30 days of receipt of goods (Net-30), whereas the SCO pays on terms of Net-45 at best. The delay of payment can introduce complications with JBE cloud service subscriptions. When a JBE contracts with a cloud service provider, the JBE should carefully review the contract and/or agreement terms and conditions regarding what happens with a customer's data following a delayed payment. For example, when the Legislature and Governor's Office experience delays approving the California budget,

delays of payments have historically resulted for many vendors. Whereas local infrastructure is a capital expenditure and is less affected by delayed payments, cloud infrastructure and services are operating expenses and rely 100 percent on timely payments.

11.9 Uncompromised Access to Credentials for Recovery Systems and Cloud Platforms

It is essential for JBEs to plan and be prepared for the worst of circumstances. JBEs should implement a credentials locker, credentials list, and so on, and store them in a documented and secured location away from and off of any IT system or facility that could be compromised and result in the activation of a JBE's recovery plan. Should a JBE's IT environment be compromised based on an IT failure, facility failure, or natural disaster, uncompromised access to credentials is mandatory to ensure that the JBE can access its backups and other DR-related systems. The JBE's credentials should be kept alongside the JBE's disaster recovery plan. JBEs should always lean on a multifaceted approach to where mission-critical documentation (e.g., credentials and DR plan) is stored and located in case access to anything and/or everything could potentially be impeded and/or permanently inaccessible until recovery.

12.0 MONITORING, TESTING, VALIDATION, AND REVIEW

A JBE's backup strategy and DR strategy (if applicable) should be comprehensively tested *at least* once per calendar year. The sophistication or simplicity of the DR solutions in place at each JBE is irrelevant to this recommendation. Of course, a JBE may choose to test more frequently if desired, and should implement a more frequent testing exercise if any uncertainty or lack of integrity exists with the backup and/or DR solutions in place.

12.1 Regular Review of Backup and Disaster Recovery Systems

12.1.1 E-mail notifications

E-mail notifications for alerts and other information should be set up in each system that makes up a JBE's DR solution. These e-mails should be reviewed regularly (e.g., daily) and checked for errors and completeness.

12.1.2 Backup job monitoring and auditing

A responsible person, persons, or team should be assigned the task of auditing all backup jobs on a JBE's backup system on a regular interval. Doing so will ensure that any new systems brought into the environment have a second and certain chance of being captured within the backup and DR plan.

12.1.3 Site recovery/cutover systems monitoring and auditing

A response person, persons, or team should be assigned the task of auditing all site recovery systems on a regular/repeat interval. Doing so will ensure that any new systems brought into the environment have a second and certain chance of being captured within the site recovery and DR plan.

12.2 Routine Testing Exercises

JBEs should establish a testing plan or testing effort and execute a routine testing exercise on a regular interval, but no less frequent than once per calendar year. Testing exercises help provide peace of mind, but more important, they prove that backup and site recovery systems are working as designed and will work should they be needed in a real scenario. Although most systems allow for out-of-band testing and data-redirect without affecting production performance or data, outages may be required for testing and should therefore be included in the test plan.

12.3 Testing Simulations

12.3.1 Loss of building access

In addition to routine and general types of testing, JBEs should run simulations that reflect real-life possibilities. One simulation is to react to a full loss of building access—specifically, the building that houses the JBE's data center. In this test, ideally, an IT team would consider working offsite or from another building.

12.3.2 Loss of access to all systems (onsite or offsite) based on catastrophic outage or disaster

In addition to routine and general types of testing, JBEs should run simulations that reflect real-life possibilities. One simulation is to react to a full loss of all systems either at the JBE's primary data center, the cloud, or both. In this test, ideally, an IT team would consider working offsite or from another building.

12.3.3 Backup system failure

In addition to routine and general types of testing, JBEs should run simulations on recovering data when their primary backup appliances or systems have failed but all other production systems, including secondary replicas of backups, are operational.

12.3.4 High-availability (site recovery) system failure

In addition to routing and general types of testing, JBEs should run simulations on remediating systems in the event that their primary site recovery systems have failed and cannot function as designed.

APPENDIX A

LIST OF HIGH-LEVEL TECHNICAL REQUIREMENTS AND SYSTEMS/DATA CATEGORIZED BY RECOVERY TIME

RECOVERY-TIME DISCLAIMERS

- Recovery time depends on the following:
  - The actual disaster (severity)
  - Whether the facility or physical access is affected, including safety situations (e.g., hazmat, fire, smoke)
  - Staff capacity and availability
  - Replacement equipment (if applicable)
  - Conflicting DR recovery commitments or plans (e.g., CCTC or other data centers/cloud)
  - Recovery actions, such as abrupt responses that could lead to some or significant permanent data loss based on available backups, the approach taken for data restoration, and/or disaster recovery site cutovers
- Fault tolerance is typically costly and requires additional hardware and software.
- Some functionality or components are built into other component systems (overlap of functionality).
- Time to recover (TTR) is the maximum recommended/defined outage time for purposes of implementing priorities for data recovery and outage mitigation.
- Hardware items on the end-user side of IT (e.g., printers, desktops, scanners, barcode readers, etc.) have not been included because they are considered end-user equipment and are outside the scope of the disaster recovery framework.

HIGH-LEVEL TECHNICAL REQUIREMENTS

- TTR of 12 hours maximum
- Infrastructure (network, Active Directory (AD), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP))
- Shared/combined storage (SAN, etc.)
- Virtual hypervisor/platform
- Backup solution/platform
- Wi-Fi

- Load balancers
- Reverse proxy

BUSINESS RECOVERY REQUIREMENTS (EXAMPLES OF SYSTEMS AND SERVICES)

The tiers below align with the judicial branch Next Generation Hosting Strategy Workstream's output, except in ways that clearly delineate how approaches to disaster recovery differ from hosting and uptime, given that all are interrelated and depend on one another for the reliability and protection of data.

- **TIER 1**—HIGH priority; TTR (not considering disclaimers) of 12 to 48 hours maximum; and systems and services as follows:
  - VoIP
  - Case Management Systems (CMS)
  - Document Management Systems (DMS)
  - File servers (holding judicial, executive, human resources, finance, and IT data and documentation)
  - E-mail (systems dependent on e-mail, such as alert and public communication systems), Microsoft Office 365, and others
  - Public website (hosted on-premises or offsite); important for a mechanism to broadcast information to the public and for the public to send or input data to the court; the portal at each court
  - Electronic reporting, docket, and minutes
  - Jury management system (JMS)
  - Virtual private network (VPN)
  - Electronic Probable Cause Declaration (ePCD)
  - Electronic Search Warrants (eWarrant)
  - Interfaces (interagency; some e-filing)
  - Building access control (e.g., Identiv, Schneider Electric)
  - Finance systems on-premises
  - Human resources systems on-premises, time card systems, Phoenix/SAP
  - Jury instructions
- **TIER 2—**MODERATE priority; TTR (not considering disclaimers) of 48 to 72 hours maximum; and systems and services as follows:
  - Intranets
  - File servers (holding less- or moderately important data)
  - Print servers
  - Building automation system
  - California Courts Protective Order Registry
  - CLETS
  - Department of Motor Vehicles access, controls or interface

- Other interfaces: various justice partners (e.g., Franchise Tax Board, Department of Justice, district attorney, police department, California Highway Patrol, sheriff, etc.)
- Site control (elevator controls, door controls, etc.)
- Electronic transcript assembly tools/software
- Interactive voice response (traffic, jury, etc.)
- Electronic signing product/solution
- Middleware
- Reporting systems (not built into CMS, but standalone)

- **TIER 3**—LOW priority; TTR (not considering disclaimers) of 168 hours maximum; and systems and services as follows:
  - IT tools and unique IT management systems (e.g., help desk, logging, controls, and network/system/application monitoring)
  - Video surveillance
  - Meeting systems (WebEx, Skype, etc.)
  - Digital signage
  - Queuing systems
  - Mobile device management

APPENDIX B

RECOMMENDED MINIMUM REQUIREMENTS FOR A BACKUP SOLUTION

Note: Tape should never be used as the primary backup medium.

- Disk-based
- Cloud-based
- Cloud-to-cloud backup capabilities for Microsoft Office 365 (e.g., OneDrive, SharePoint, Exchange Online) backups
- Sufficient Internet bandwidth for cloud and/or remote backups
- Scalable (can grow as court grows without large, repeated capital expenditures)
- Granular backup and restoration (e.g., exchange items in mailboxes, SQL objects, individual files)
- Ability to create multiple schedules
- Ability to notify or alert IT staff of problems
- Ability to verify backups
- Ability to restore to a different backup target
- Ability to encrypt sensitive or classified data or information
- Ability to audit all changes made to the backup system, backup jobs, schedules, etc.
- Ability to create multiple backup jobs
- Ability to create backup schedules with multiple backup targets
- Ability to replicate *offsite:*
  - To the cloud
  - To a secondary backup system
  - To a removable or portable disk
  - To tape (*as last resort*)
- Ability to initialize or mount a backed-up virtual machine in the cloud (specific for cloud backup solutions)

CALIFORNIA JUDICIAL BRANCH

Disaster Recovery Plan

Superior Court of [Insert Court Name]

VERSION 1.2

MAY 31, 2017

Table of Contents

1.0 INTRODUCTION 1
1.1 Definitions 1
1.2 Purpose 1
1.3 Applicability 2
1.4 Scope 2
1.5 Disaster Recovery Plan Phases 3
1.6 Assumptions 4
2.0 DISASTER RECOVERY APPROACH 4
3.0 COMMUNICATIONS PLAN 4
3.1 Status Reporting 5
3.1.1 Pre-Declaration 5
3.1.2 Post-Declaration and Coordination 5
3.1.3 Post-Declaration and Onsite Execution 6
3.1.4 Post-Disaster 6
4.0 DISASTER RECOVERY TEAM POSITIONS AND ASSIGNED ROLES AND RESPONSIBILITIES 6
4.1 Disaster Recovery Manager 6
4.2 Account Manager 6
4.3 Executive Management—[Court Name] 7
4.4 Executive Management—[External DR Provider Name] 7
4.5 Backup Administrator 7
4.6 Storage Administrator 7
4.7 Network Administrator 7
4.8 Network Software Support 8
4.9 Unix Administrator 8
4.10 Windows Administrator 8
4.11 Applications Software Support 8
4.12 Database Support 8
4.13 Middleware Support 9
4.14 Service Desk 9
4.15 Emergency Operations Center 9
4.16 Training, Testing, and Exercising the Disaster Recovery Team 9
5.0 DISASTER RECOVERY PLAN 10
5.1 Site Evacuation 10
5.1.1 Evacuation Procedure 10
5.2 Notification and Activation Phase 10

5.2.1 Notification Procedures 10
5.2.2 Establish Crisis Management Center 10
5.2.3 Incoming Telephone Call Procedures 10
5.2.4 Alert External Service Provider(s) 10
5.2.5 Activate Conference Bridge 10
5.2.6 Notify Help Desk 10
5.2.7 Notify Alternate Hosting Facility(s) 10
5.2.8 Alert Offsite Data Vaulting Facility 10
5.2.9 [Continue as needed] 10
5.3 Assessment and Reporting Phase 10
5.3.1 Damage Assessment Phase 10
5.3.2 DR Team Report Recommendations to the DR Manager 10
5.4 Strategy Review and Declarations Phase 11
5.4.1 Review Recovery Strategies 11
5.4.2 Information Technology Strategy 11
5.4.3 Criteria 11
5.4.4 Declaration 11
5.5 Post-Declaration Activation and Administrative Phase 11
5.5.1 Activation Decision 11
5.5.2 Personnel Activation and Notification Procedures 11
5.5.3 Administrative Procedures 11
5.5.4 Tape Shipping Methodology 11
5.5.5 Put Vendors on Notice 11
5.6 Continuity of Services and Initial Recovery Phase 11
5.6.1 Recovery Phase 11
5.7 Return Phase 11
5.7.1 Return to Production Site 11
5.7.2 Approach for Plan Deactivation 12
5.7.3 Preparedness Phase 12
6.0 DISASTER RECOVERY PLAN TESTING 12
6.1 Objectives 12
6.2 Scheduling 12
6.3 Success Criteria 12
6.4 Noncontributing Factors 12
6.5 Environmental Change Coordination 12
7.0 PERSONNEL ACTIVATION AND NOTIFICATION PROCEDURES; TELEPHONE LOG 12
8.0 CALL LISTS 12
9.0 APPLICATIONS TECHNICAL RECOVERY PLANS 12
10.0 APPENDIXES 12

10.1 Appendix B: [contact list].....12
10.2 Appendix I: [worksheet—DR Team Positions].....12

1.0 INTRODUCTION

This disaster recovery plan identifies the steps to recover the Superior Court of [court name] County technology infrastructure housed at [court location].

1.1 Definitions

This plan references the following definitions:[1]

- **Business continuity plan**: The documented arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period and to return to performing its critical functions after an interruption. The business continuity plan is not a component of the disaster recovery plan. A business continuity plan is also referred to as a continuity of operations plan (COOP).
- **Disaster**:
  - A sudden, unplanned catastrophic event causing unacceptable damage or loss.
  - An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time.
  - An event where an organization's management invokes their recovery plans.
- **Disaster recovery (DR)**: The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
- **Disaster recovery plan**: The management-approved document that defines the resources, actions, tasks, and data required to manage the technology recovery effort. The disaster recovery plan is a component of the business continuity plan.
- **Disaster recovery planning**: The technical component of business continuity planning.
- **Disaster recovery team**: The main group of personnel in charge of the recovery effort.

1.2 Purpose

This disaster recovery plan mitigates the risk of system and service unavailability by providing written-response solutions for the prompt and effective continuation or resumption of mission-critical services in the event of a disaster.

[1] The definitions in this section are adapted from the glossary provided by *Disaster Recovery Journal* at *www.drj.com/resources/tools/glossary-2.html* (as of May 17, 2017) and used with permission.

The purpose of this plan is to establish a process to relocate critical systems on substitute hardware at a geographically dispersed site in a timely, well-orchestrated manner.

In addition, this plan has a preventive component that fulfills Presidential Decision Directive 63 on Critical Infrastructure Protection (see 63 Fed. Reg. 41804 (Aug. 5, 1998)), which requires federal agencies to identify mission-critical infrastructure components and develop a plan to protect them.

It is important to note that this disaster recovery plan is a component of business continuity.

1.3 Applicability

This disaster recovery plan applies to facility-level disruptions. A *facility-level disruption* is an event that renders a facility inoperable. This catastrophic scenario requires the availability of information technology resources to restore services at the alternate site in [location].

This plan applies to the continuity, recovery, and reconstitution of the [court name] housed at [location] and not to the specific business functions performed by the various units within the court. The business functions are the responsibility of the executive management at each division(s), which develop and execute business continuity and continuity of operations plans, as well as business recovery plans.

1.4 Scope

This disaster recovery plan focuses on the recovery and continued operation of system components that support mission-critical systems and mission-essential services in the event of a disaster.

For the purposes of this plan, a *disaster* is a major incident that seriously disrupts or is expected to disrupt operations for 24 hours or more and requires:

- the reassignment of personnel to disaster recovery activities;
- the use of additional vendor/contractor support to accomplish recovery requirements; and/or
- the acquisition of special funding to support equipment replacement and other recovery-related costs that are outside the scope of normal day-to-day operations.

If the level of effort required to accomplish these requirements falls within the scope of a disaster as defined above, then a disaster declaration should be issued, and disaster recovery plan processes and procedures should be initiated. If the level of effort required does not, then the [court IT unit] should conduct the recovery actions as part of day-to-day operations.

1.5 Disaster Recovery Plan Phases

This disaster recovery plan establishes action steps and clear lines of responsibility for recovery efforts. The plan consists of the following phases:

- **Site evacuation.** If necessary, the disaster recovery manager (DR Manager) will order the evacuation of the [court facility] data center and turn over the control of the equipment within the facility to [alternate facility].

- **Notification and activation phase.** In this phase, members of the disaster recovery team (DR Team) are notified and the DR Manager is notified to activate the team.

- **Assessment and reporting phas.** DR Team members report to the scene, evaluate conditions, and develop a formal recommendation for the DR Manager on whether to declare a disaster.

- **Strategy review and declaration phase.** This phase includes procedures for finalizing strategies and recovery actions and for declaring a disaster.

- **Post-declaration activation and administrative phase.** This phase provides procedures for notifying personnel, offsite storage retrieval, travel, and personnel scheduling. It also provides a form for documenting personnel locations and requesting travel arrangements.

- **Continuity of services and initial recovery phase.** If directed by the DR Manager, the DR Team will take action to quickly recover and continue providing the [court name] data center housed at [court facility] services to the extent allowed by conditions and, if necessary, at a degraded level until the restoration of normal operations. If conditions warrant, the DR Team will relocate and recover the [court name] data center housed at [court facility] operations at the alternate site in [location].

- **Full recovery and reconstitution of normal operations phase.** As conditions stabilize, the DR Team will take action to reestablish the [court name] data center housed at [location] operations to the [alternate location] facility. Depending on the damage that occurred, [court entity] will repair facilities, repair damaged equipment, return platforms to operation, reload applications, re-initiate network connectivity, and restore normal computer operations and associated procedures. If the site is not salvageable, an alternate site will be selected and reconstructed to a level equivalent to that of the original site.

- **Return phase.** This phase includes instructions for salvage and media reclamation activities as well as site restoration.

- **Preparedness phase.** This phase includes guidelines for updating the plan, testing the plan, and validating information within the plan (e.g., contact names, vendor names, and plan currency).

1.6 Assumptions

- The disruption disables only the [primary facility name] site; the [secondary site name] is unaffected.
- Offsite storage locations for critical backup files and information are intact and accessible.
- The recovery is performed in accordance with the procedures that have been set forth within this disaster recovery plan.
- A sufficient number of qualified personnel are available to perform recovery responsibilities.
- Backups and rotation practices are performed as scheduled.
- The backup and recovery strategies are performed as implemented and tested.
- Entities external to the company, such as customers, vendors, government agencies, and others, are reasonably cooperative during the recovery period.

2.0 DISASTER RECOVERY APPROACH

The [court name] disaster recovery approach provides a [describe model here].

3.0 COMMUNICATIONS PLAN

The key to the successful implementation of this disaster recovery plan is overcoming the technical hurdles to reestablishing production systems at the [primary court hosting facility]. However, to coordinate within any business continuity plan, proper communication throughout the execution is critical.

- **E-mail.** E-mail will be one of the primary communication methods due to the speed of transmission and the ability to disseminate information to a large audience quickly. However, because e-mail is dependent on hardware and network functionality, this medium may not be available during a declared disaster.
- **One-on-one phone call.** At times, immediate acknowledgment of the communication or interactive decision making between individuals is required. In those situations, voice calls are preferred.
- **Conference bridge.** Upon the declaration of a disaster, a conference bridge for conference calls will be set up. This is the preferred method for facilitating quick, interactive, multi-party decisions.
- **Text message.** Text messaging is an alternative method for providing status reports or for quick, two-way communications between individuals.

- **Status line.** A status line provides a listen-only, updatable, recorded status message accessible by all stakeholders. This method is effective for secondary stakeholders who do not need continuous, up-to-the-minute status reports.

During a declared disaster, all communications will require an acknowledgment to ensure receipt of the information. Each communication should provide instructions for acknowledgment.

3.1 Status Reporting

3.1.1 Pre-Declaration

Depending on the nature of the disaster, before declaration there may be an executive conference call to discuss whether the event warrants a disaster declaration. An example scenario is if a nearby chemical spill required the evacuation of the data center. Since the duration of such an evacuation would be unknown, a conference call would be appropriate to discuss options available other than a declared disaster.

3.1.2 Post-Declaration and Coordination

After a declaration, status reports will immediately commence. Within the first 24 hours, the [responsible court IT unit, e.g., service desk] will be the primary center for all communications. Immediately upon declaration, the Emergency Operations Center (see section 4.15) will open a conference bridge and it will remain open until the DR Manager requests the bridge be turned off.

The [responsible court IT unit] will begin contacting individuals as described in Appendix B.

Because of the dynamic nature of staffing, the [responsible court IT unit] will contact [appropriate court management and executive staff] within the [court name]. Anyone on the conference call can then request that other individuals be contacted to join the call.

After declaration, the DR Manager will announce a conference call for the first status meeting. This meeting should take place upon completion of notifying all key stakeholders and contacts, but no more than 3 hours after disaster declaration. The meeting will provide answers to the following questions:

- What is the extent of the disaster?
- What resources are incapacitated?
- Who is on the DR Team?
- What is the estimated arrival time of the restoration media, such as disk(s), replica appliance(s) or pulling down backup data from a remote or cloud location at [alternate facility name]?

- What are the status reporting expectations during the interval between this call and arrival onsite?

3.1.3 Post-Declaration and Onsite Execution

As soon as the DR Manager arrives onsite (where "onsite" may be in the form of establishing a conference call line), he or she will send status reports every 4 hours via e-mail and text message, or as required or requested. In addition to the scheduled status reports, the disaster recovery plan requires reporting the completion of certain milestones.

The DR Manager will hold a conference call 6 hours after the recovery efforts have begun to discuss the progress made and any issues. During this call, the time of the next conference call will be determined.

Other status reporting mechanisms may be used as deemed appropriate throughout the declaration.

3.1.4 Post-Disaster

To declare the end of a disaster, the DR Manager will establish a conference call to communicate to the DR Team the end of the disaster.

4.0 DISASTER RECOVERY TEAM POSITIONS AND ASSIGNED ROLES AND RESPONSIBILITIES

Appendix I contains a worksheet listing the names of individuals in each of the roles described below. (Note that a team member may take on more than one role, just as more than one team member may be required to execute a single role.)

4.1 Disaster Recovery Manager

When a disaster or disaster drill condition is declared, the DR Manager will be the focal point for all disaster recovery activities. The primary responsibility of the DR Manager is to ensure the successful execution of the disaster recovery plan. To be successful in that task, the DR Manager will be the focal point for all communications.

Throughout the year, the DR Manager will also be responsible for maintaining the disaster recovery plan.

4.2 Account Manager

During a declaration, the Account Manager will be a primary stakeholder for all communications. This role will be an escalation point for all parties. The Account Manager will work closely with the DR Manager to ensure clear and accurate communications with

the [Court Name] Executive Management. The Account Manager will also mediate decision making between [designated entities].

4.3 Executive Management—[Court Name]

During a declaration, the [court name] Executive Management Team will be a co-primary stakeholder for all communications.

4.4 Executive Management—[External DR Provider Name]

During a declaration, the [external DR provider] Executive Management Team will be a primary stakeholder for all communications. Depending on the severity and nature of the disaster, the Executive Management Team will play an integral role in communications between [designated parties].

4.5 Backup Administrator

During a declaration, the Backup Administrator will be responsible for assisting with rebuilding the environment at the [alternate facility name] facility and executing the procedure to restore the systems from the backup media.

Throughout the year, the Backup Administrator will be responsible for maintaining backup hardware, backup applications and backup schedules and strategies, including the and data restore process.

4.6 Storage Administrator

During a declaration, the Storage Administrator will be responsible for assisting with rebuilding the environment at the [alternate facility name] facility and executing the procedure to restore the systems from the production [backup data source].

Throughout the year, the Storage Administrator will be responsible for maintaining the storage area network replication and restore process.

4.7 Network Administrator

During a declaration, the Network Administrator will be responsible for ensuring connectivity to all necessary resources. This will include all tasks required to ensure network communications between the [alternate facility name] site and the end users. In the case of multiple network administrators, the primary responsibility for connectivity lies with the company designated as owning network functions.

Throughout the year, the Network Administrator will be responsible for maintaining the network restore process.

4.8 Network Software Support

When a disaster or disaster drill condition is declared, the Network Software Support Analyst will work with the Network Administrator to implement changes necessary to accommodate the recovered systems' connectivity to the [court name] environment. They will monitor and work to resolve any issues that may arise during the recovery period.

4.9 Unix Administrator

When a disaster or disaster drill condition is declared, the Unix Administrator will be responsible for the operational restoration of all Unix platform servers. The Unix Administrator will work closely with the Backup Administrator to ensure the proper restoration of data at the right time. In addition, the Unix Administrator will be responsible for the hardware verification.

Throughout the year, the Unix Administrator will be responsible for maintaining the Unix system restore process.

4.10 Windows Administrator

When a disaster or disaster drill condition is declared, the Windows Administrator will be responsible for the operational restoration of all Intel platform servers. The Windows Administrator will work closely with the Backup Administrator to ensure the proper restoration of the data at the right time. In addition, the Windows Administrator will be responsible for the hardware verification.

Throughout the year, the Windows Administrator will be responsible for maintaining the Windows system restore process.

4.11 Applications Software Support

When a disaster or disaster drill condition is declared, the Applications Software Support Analyst will work closely with the Backup Administrator to ensure the proper restoration of the data at the right time. They will monitor and work to resolve any issues that may arise during the recovery period.

4.12 Database Support

When a disaster or disaster drill condition is declared, the Database Support Analyst will work with the Applications Software Support Analyst to implement changes necessary to accommodate the recovered systems connectivity to the [court name]. They will monitor and work to resolve any issues that may arise during the recovery period.

4.13 Middleware Support

When a disaster or disaster drill condition is declared, the Middleware Support Analyst will work with the Applications Software Support Analyst to implement changes necessary to accommodate the recovered systems' connectivity to the [court name]. They will monitor and work to resolve any issues that may arise during the recovery period.

4.14 Service Desk

During a declaration, the [responsible court IT entity, e.g., service desk] will play a pivotal role in communications for the first 24 hours of the declaration. The [responsible court IT entity] will be the first point of contact by anyone working on the disaster recovery plan. The [responsible court IT entity] will then execute a communications plan to notify all parties involved and to set up the initial conference call. In addition, working with the DR Manager, the [responsible court IT entity] will be the central repository for all incoming information and will have all of the following readily available:

- Status of the declaration event
- List of incapacitated assets
- Status of team formation
- Travel plans for all traveling team members

4.15 Emergency Operations Center

The Emergency Operations Center is the location identified for the assembly of the DR Team immediately following the declaration of a disaster. The DR Team will manage and coordinate recovery and reconstitution activities from this location. It is also where the DR Team will meet, whether in person or through a communications medium, to report the status of their actions.

The Emergency Operations Center will be located in the [location name], if feasible. If an alternative location is chosen, the DR Team will clearly communicate that location to all invested parties.

4.16 Training, Testing, and Exercising the Disaster Recovery Team

New DR Team members will learn the disaster recovery processes and procedures by virtue of trainings and knowledge transfer exercises. The DR Manager will provide members with up-to-date copies of this disaster recovery plan. The DR Manager will also periodically test DR Team members on aspects of the disaster recovery plan policies, processes, and procedures that are unique to system operations and essential to recovery and reconstitution. The DR Manager will conduct annual formal tests and exercises of the team. A disaster recovery plan evaluation form will be completed by a designated DR Team member

following each test or exercise, and the DR Manager will use the information to make any necessary modifications to refine plan processes and procedures.

5.0 DISASTER RECOVERY PLAN

[Document the steps needed to complete the recovery of the primary hosting facility to an alternate location]

5.1 Site Evacuation

5.1.1 Evacuation Procedure

5.2 Notification and Activation Phase

5.2.1 Notification Procedures

5.2.2 Establish Crisis Management Center

5.2.3 Incoming Telephone Call Procedures

5.2.4 Alert External Service Provider(s)

5.2.5 Activate Conference Bridge

5.2.6 Notify Help Desk

5.2.7 Notify Alternate Hosting Facility(s)

5.2.8 Alert Offsite Data Vaulting Facility

5.2.9 [Continue as needed]

5.3 Assessment and Reporting Phase

5.3.1 Damage Assessment Phase

5.3.1.1 Facility/site damage

5.3.1.2 Office and storage areas

5.3.1.3 Network capabilities

5.3.1.4 Platform damage and operability

5.3.1.5 Application status

5.3.1.6 Database status

5.3.1.7 Forms locations

5.3.2 DR Team Report Recommendations to the DR Manager

5.4 Strategy Review and Declarations Phase

5.4.1 Review Recovery Strategies

5.4.2 Information Technology Strategy

5.4.3 Criteria

5.4.4 Declaration

5.5 Post-Declaration Activation and Administrative Phase

5.5.1 Activation Decision

5.5.2 Personnel Activation and Notification Procedures

5.5.2.1 Brief team members

5.5.2.2 Track and schedule personnel

5.5.2.3 Arrange travel and transportation

5.5.3 Administrative Procedures

5.5.3.1 Ensure court policy

5.5.3.2 Ensure employee well-being

5.5.3.3 Monitor and report recovery process

5.5.3.4 Act as advisor or liaison for recovery teams

5.5.3.5 Maintain recovery-related record keeping

5.5.3.6 Documentation of administrative procedures

5.5.4 Tape Shipping Methodology

5.5.4.1 Retrieve offsite storage tapes and bins

5.5.5 Put Vendors on Notice

5.6 Continuity of Services and Initial Recovery Phase

5.6.1 Recovery Phase

5.7 Return Phase

5.7.1 Return to Production Site

5.7.1.1 Oversee site restoration

5.7.1.2 Interim or primary site restoration activities

5.7.1.3 Site restoration checklist

5.7.2 Approach for Plan Deactivation

5.7.2.1 Post-disaster DR Team brief

5.7.2.2 DR Team deactivation

5.7.3 Preparedness Phase

5.7.3.1 Maintain preparedness

5.7.3.1.1 Maintain current recovery preparedness

5.7.3.1.2 Review and validate requirements and strategies

6.0 DISASTER RECOVERY PLAN TESTING

6.1 Objectives

6.2 Scheduling

6.3 Success Criteria

6.4 Noncontributing Factors

6.5 Environmental Change Coordination

7.0 PERSONNEL ACTIVATION AND NOTIFICATION PROCEDURES; TELEPHONE LOG

8.0 CALL LISTS

9.0 APPLICATIONS TECHNICAL RECOVERY PLANS

10.0 APPENDIXES

10.1 Appendix B: [contact list]

10.2 Appendix I: [worksheet—DR Team Positions]

CALIFORNIA JUDICIAL BRANCH

Next Generation Hosting Framework

A Guide for the California Judicial Branch

VERSION 1.0

JANUARY 18, 2017

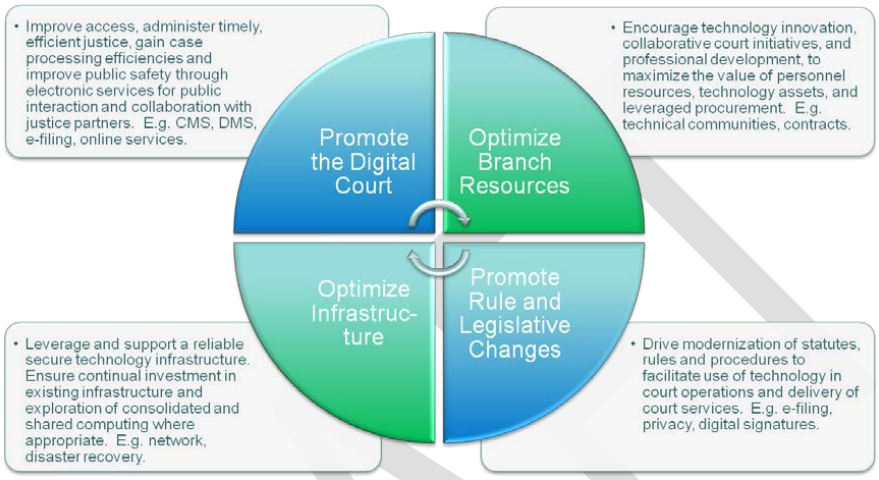
Table of Contents

1.0 Introduction....2
2.0 Definitions....3
3.0 Next Generation hosting Framework....4
3.1 Scope of Next Generation Hosting Strategy....4
3.2 Organizational Characteristics....5
3.3 Organizational Assumptions....10
3.4 Documentation Structure....11
4.0 Purpose of Next Generation Hosting....11
5.0 Next Generation hosting options and Recommedations....11
5.1 Data center options....11
5.2 Service level defintion and recommations....13
5.3 Branch wide Inventory Assets....14
5.4 Branchwide requirements....16
6.0 Branch-wide recommendations....18
7.0 Using Next generation hosting framework....19
7.1 Use Inventory checklist....19
7.2 Use Technology Roadmap....19

1.0 INTRODUCTION

In October 2014, the California Judicial Branch adopted the Strategic Plan for Technology for 2014-2018 and the Tactical Plan for Technology for 2014-2016. There are four technical goals defined within the strategic plan:

Goal One: Promote the Digital Court
Goal Two: Optimize Branch Resources
Goal Three: Optimize Infrastructure
Goal Four: Promote Rule and Legislative Changes



In accordance with Goals One, Two and Three, the Judicial Branch Tactical Plan outlined the Next Generation Hosting Initiative. While this initiative is expressly called out under Goal Three, the reality is this type of hosting solution has a direct impact on the branch's ability to accomplish three of its strategic goals to: Promote the Digital Court and Optimize Branch Resources and Infrastructure.

In order to truly achieve Goals One and Two, the hosting solution must take into account the requirements for those goals. For example, one set of objectives to Promote the Digital Court is:

- Extended access and services to the public, including electronic filing and enhanced access for those with limited English proficiency;
- Enhanced judicial and administrative decision-making;
- Data and information sharing across the courts;
- Enhanced collaboration and cooperation between and among courts;
- Enhanced collaboration and cooperation with local and statewide justice partners to promote public safety.

How each of these objectives are met, is a direct result of the data center and function within.

This framework makes recommendations based upon the strategic and tactical plan and best likelihood for achieving the defined goals and objectives. These are not mandatory requirements but rather a common framework that can be leveraged to help individual courts identify hosting solutions that are appropriate for their local environment. The Workstream recognizes many of the recommendations are not feasible in today's climate, due to the budget and resource constraints. The intention is for the framework to provide court leadership with the foundation and guidance to move towards these strategic goals and objectives.

2.0 DEFINITIONS

"Cloud Computing," a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services),which can be rapidly provisioned and released with minimal managerial effort. These resources typically reside on the Internet instead of a local data center.

"Data Center," a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g. air conditioning, fire suppression) and various security devices.

"Data Loss," is any process or event that results in **data** being corrupted, deleted and/or made unreadable by a user and/or software or application.

"Hosted Solutions," for the purposes of this survey, refers to the physical servers supporting and storing court data whether provided internally, by the branch data center, or a vendor either locally, offsite, or via cloud hosting.

"Infrastructure as a service (IaaS)," The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

"Local Hosting Solution," a local trial court's data center, managed, resourced, supported, and funded by that trial court.

"Platform as a service (PaaS)," is a category of cloud computing services that provides a platform allowing customers to develop, run and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.

"Service Level," measures the performance of a system. Certain goals are defined and the service level gives the percentage to which those goals should be achieved.

"Software as a service (SaaS)," is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted on the Internet. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users using a thin client via a web browser.

"System Outage/Downtime," The term downtime is used to refer to periods when a system is unavailable. **Downtime** or **outage** duration refers to a period of time that a system fails to provide or perform its primary function. Reliability, availability, recovery, and unavailability are related concepts.

"Vendor Hosted Solution," Cloud computing vendors that have the capability of delivering SaaS, IaaS, and PaaS technical solutions.

3.0 NEXT GENERATION HOSTING FRAMEWORK

3.1 SCOPE OF NEXT GENERATION HOSTING STRATEGY

The California Courts Technology Center (CCTC) current hosting model for information technology applications and services was developed largely based upon the strategy of centrally hosting the court case management systems and other shared applications. The branch-wide strategy of hosting the court case management systems has changed; therefore, the branch must reevaluate its hosting model to ensure resources and opportunities are utilized effectively in alignment with the new strategic direction while addressing the needs of the courts.

As hosting models and technology evolve, the most cost-effective, branch-wide strategy for application and services hosting can be enabled through a combination of selective consolidation, virtualization, and implementation of secure private and public cloud environments. The goal of this tactical initiative will be to determine an updated model for branch-wide hosting, including all judicial branch entities.

Major Tasks

- Complete needs assessment; define branch recommended services levels; develop implementation recommendations; and determine necessary funding changes.
- Develop toolset for courts to utilize when determining needs and funding requirements.
- Publish findings including hosting implementation toolset and branch suggested service levels.
- Finalize product, service, and maintenance contract procurement with vendor partners.
- Assist judicial branch entities with decommissioning old services and implementing new services in alignment with the needs assessment and transition plan.

Dependencies

- The needs assessment should align with the strategy and roadmap for the Digital Court initiatives.

Types of Courts Involved

All courts—Supreme Court, Courts of Appeal, and superior courts. All courts and the Judicial Council will benefit from an updated branch-wide hosting model, tightly aligned with current and anticipated future business requirements.

Workstream Phases

Phase 1: Develop Educational Information and Hold Summit

- Develop Educational Information and Hold Summit, if necessary
- Define top solutions in the industry.
- Define the pros and cons of each solution
- Provide examples of court applications that could use each solution
- Provide example cost information by solution.
- Include road mapping tool to assist courts in evaluating local needs and identifying hosting solutions for themselves.
- Produce Next Generation Hosting Information Tool
- Determine if a summit on the topic is necessary, and if so, hold the summit.

Phase 2: Define Branch-Level Hosting Requirements

- Identify strategies that could be implemented or utilized across the branch

- Survey courts (all levels) on types of applications they envision being hosted at more central level
- Capture hosting requirements based on Judicial Council decisions on branch-wide applications.
- Define service level requirements for branch-level host site.
- Produce Next Generation Hosting Final Report and Requirements.

3.2 ORGANIZATIONAL CHARACTERISTICS

As part of its 2015 annual agenda, the Information Technology Advisory Committee (ITAC) (formerly Court Technology Advisory Committee), Projects Subcommittee surveyed trial courts on two related topics: disaster recovery preparedness and planning for future hosting of court data ("Next Generation Hosting"). All courts should be concerned about the impact of disasters of all kinds, whether resulting from extreme weather events, earthquake, or by malicious entities. Budget and resource constraints impact the ability of individual courts and the branch as a whole to be prepared for and recover from such disasters. A corollary to these concerns is the effect migration has to new hosting environments and will have on disaster recovery preparedness and planning.

A survey was disseminated on June 1, 2015 to the Court Information Technology Management Forum (CITMF), and responses were collected through June 19, 2015. Responses were obtained from 49 of the 53 members, a 92 percent response rate. CITMF members are the IT leaders from each of the trial courts.

The survey intended to identify: the existing resources; unmet needs; near-future objectives of the trial courts, individually and collectively; and to determine how the branch may best facilitate solutions. The survey questionnaire was divided into two parts: Disaster Recovery Framework Assessment and Next Generation Hosting Needs Assessment.

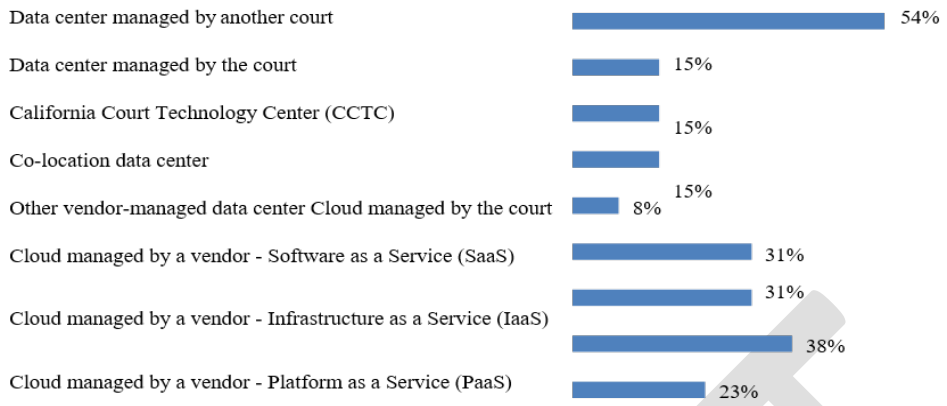
The Next Generation Hosting Solutions Needs Assessment was designed to gather information on:

- Current court practices regarding their hosting solutions;
- The considerations and requirements of courts in selecting new hosting solutions; and
- Envisioned court strategy for next generation hosting, including specific products, services, and providers, along with general approaches, alternatives, and benefits.

The Disaster Recovery Framework Assessment findings, perhaps not surprisingly, disclose a broad range of approaches and readiness to address disaster responses, varying by court size and budget resources. The survey also shows that courts do not have only one way of hosting their systems, but use more than one hosting solution.

The following graphs outline the results of the Next Generation Hosting section of the survey:

Current Judicial Branch Hosting Solutions



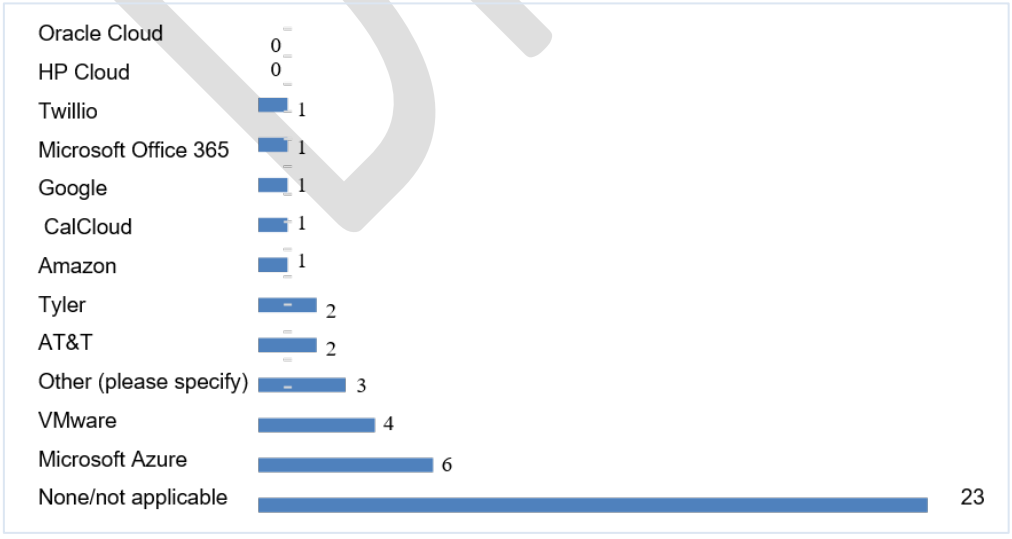
Comments:

#	Other (please specify)
1	County managed data center but all court equipment is court owned and managed.
2	Moving to Office 365.
3	We do have servers onsite at this court location; however, SAIC manages those servers.
4	We do lease some VMware VM's from our county partners.

Current Cloud/Virtualization Vendor Solutions

The second graph lists the vendors used for those courts using cloud hosting. For purposes of this survey, cloud hosting refers to services provided to customers via multiple connected servers on the Internet that comprise a cloud, as opposed to being provided by a locally hosted single server or virtual servers.

Cloud Hosting Vendors Currently Used by the Courts
Answered: 38



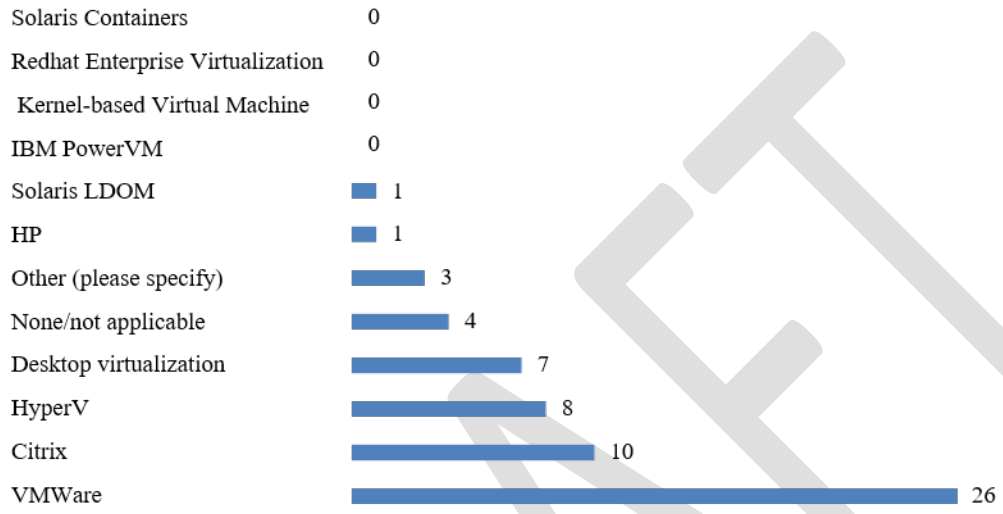
Other mentions were:

- We use cloud hosting for inbound mail screening and forwarding.

- Barracuda Backup is based both on site and in the cloud.
- ADP–time and attendance, payroll, HR. Websites hosted at a web hosting provider.

The third graph lists the virtualization technologies currently deployed in the courts. Virtualization in this context refers to the act of creating a virtual (rather than physical) version of a resource, including—but not limited to—a virtual computer hardware platform, operating system (OS), storage device, or computer network.

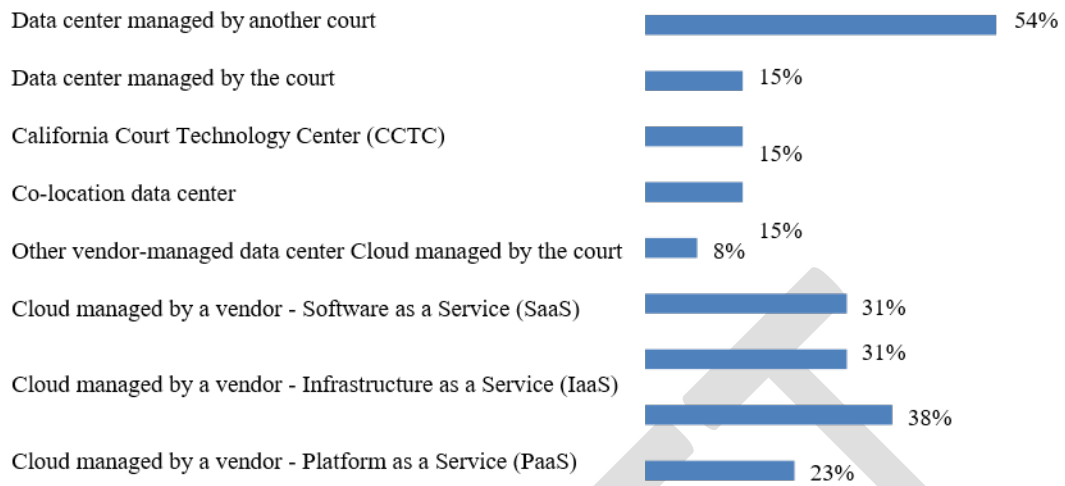
Virtualization Technologies Currently Deployed by the Courts



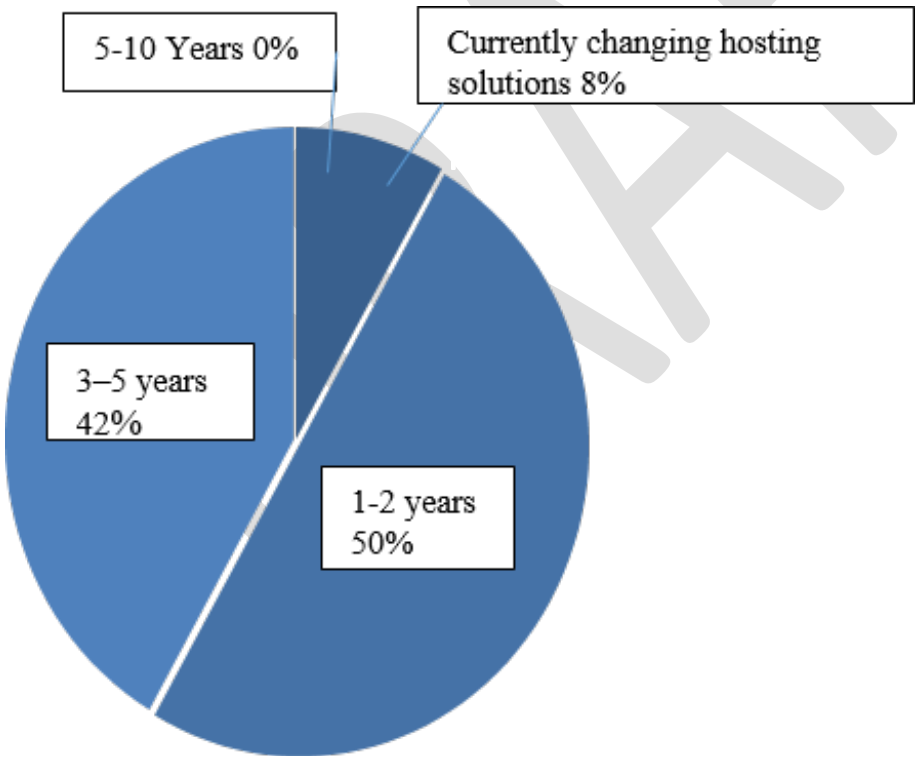
COURTS' SHORT TERM AND LONG TERM GOALS

Of the courts who answered, 34 percent are planning to move to a different hosting solution, most indicating the move should occur in one to five years. Roughly half of those planning to move to a different hosting solution are considering moving to a data center managed by the court (with one-third considering a combination of court and outsourced staff), and almost all responses indicated considering cloud management. The primary reason for making the move was improved cost efficiencies (62 percent).

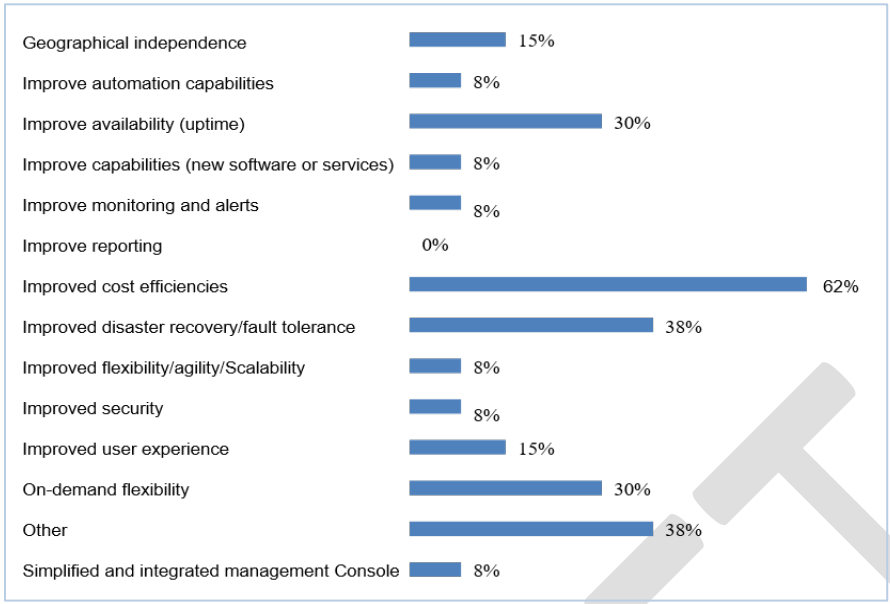
Types of Hosting solutions being considered



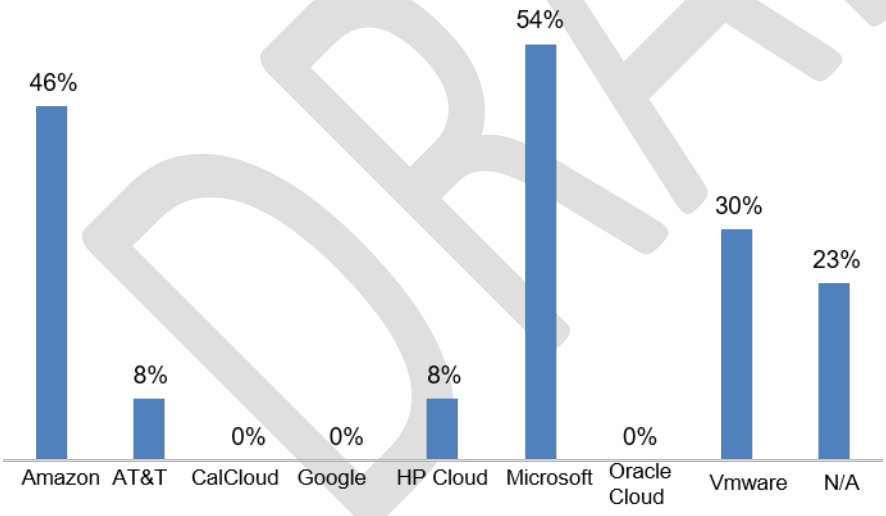
Time Frame for Courts to Move to New Hosting Solution



Reasons Courts Are Seeking a New Hosting Solution

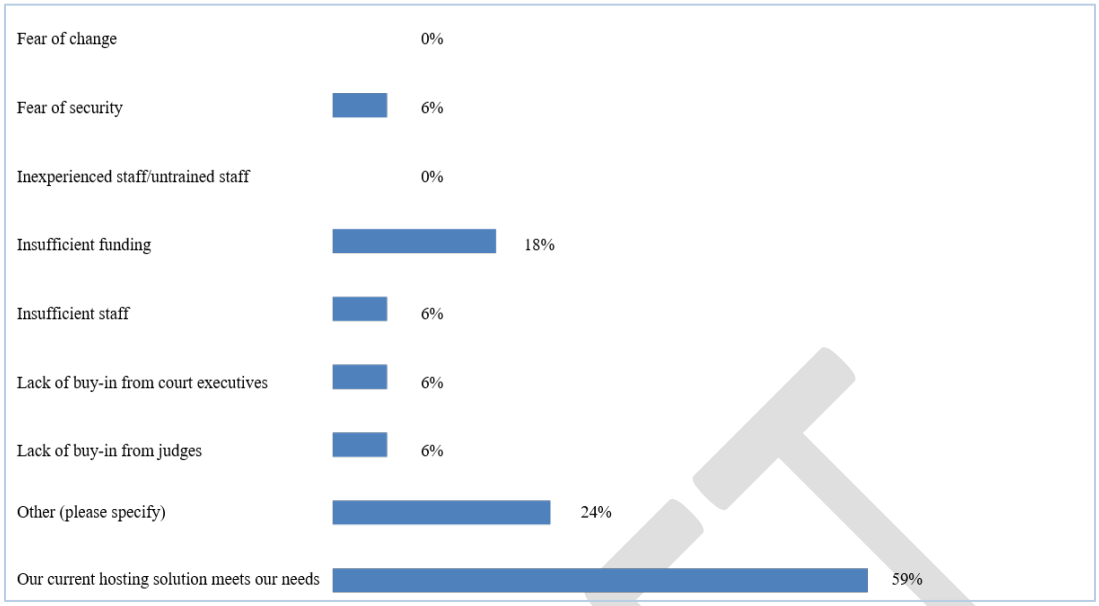


For those courts considering cloud hosting solutions, the graph below shows the list of vendors currently being considered.



Lastly, it is important to analyze why some courts are not moving to new data center solutions. The graph below identifies some very clear reasons, such as no need, implementing new CMS (Other), or no funding.

Reasons for Courts Not Seeking a New Hosting Solution



CONCLUSION

Although the data was generated in 2015, it outlines several key elements that are still relevant:

- Of the 34 percent who are looking to move to a cloud solution, 9 percent of the courts are looking to change within the next 5 years
- 62 percent are looking to make a change to cost efficiencies
- Many courts are already starting to work with vendors on cloud solutions, such as Microsoft and Amazon
- 42 percent of courts are not seeking a new solution because of insufficient funding, fear of security, insufficient staff, and lack of buy-in from judges and court executives.

Since this survey was conducted, CITMF surveyed the trial courts in June 2016 on the use of Office 365, and 13 courts have now moved to Office 365, a significant change from six courts just one year prior.

3.3 ORGANIZATIONAL ASSUMPTIONS

Due to the diversity as seen in the data above, where courts are in varying levels of technical maturity, the Workstream had to determine some basic assumptions to meet the goals and objectives set forth in the strategic and tactical plans. The Workstream recognizes that some of the assumptions may be broad in scope, but are necessary when determining a path to the future.

ASSUMPTIONS:

1. All courts are utilizing or moving to modern Case Management Systems (CMS) within the next five years
2. Current court facilities meet requirements for cloud hosting
3. Courts have adequate internet bandwidth
4. Funding can be obtained
5. Resources will be determined based on solution selected
6. Output from the Disaster Recovery Workstream will be utilized where appropriate

3.4 DOCUMENTATION STRUCTURE

The Next Generation Framework contains four key elements:

- Recommended service level definitions, and timeframes
- Recommend court asset inventory sheet with court defined service levels
- Sample roadmap for long-term planning and court roadmap template, including estimate cost sheet for cloud hosting solutions
- Sample court inventory with service levels and solution and budget estimate template

These documents are tools for courts use to define data hosting requirements and create plans to move to a next generation hosting data center.

4.0 PURPOSE OF NEXT GENERATION HOSTING

As technology evolves, so do courts' needs and business practices. The courts' hosting model must partake in this evolution as well. Twenty-first century business and technology prioritizes accessibility and flexibility – a next generation hosting solution is necessary for the courts to maintain these priorities for both its external and internal users. A new hosting solution can be accomplished through a combination of selective consolidation, virtualization, and implementation of secure private and public cloud environments. The goal of this tactical initiative will be to determine an updated model for branch-wide hosting, including all judicial branch entities. The following tasks are recommended for the purpose of the Workstream:

- Outline industry best practices for hosting in an educational manner
- Develop matrix of solutions with pros, cons, and example applications hosted including costs
- Produce a roadmap tool for use by courts in evaluating options
- Consider educational summit on hosting options and hold summit if appropriate
- Identify requirements for centralized hosting
- Recommend a branch-level hosting strategy

5.0 NEXT GENERATION HOSTING OPTIONS AND BRANCH ASSETS

For each of the hosting solutions investigated by the technical team, the Workstream created pros and cons for each solution as well as a list of items to be aware of in any hosting solution.

5.1 DATA CENTER OPTIONS

Based upon review of the Hosting and Disaster Recovery Assessments, as well as court ideas and strategies, the following solutions are to be investigated:

- Branch Data Center (Centrally Hosted) - CCTC Model, Judicial Council Managed, Court Managed
- Court Hosted Data Center - Court Managed, Limited size
  - Discussion of Regional Data Centers
  - Regional Applications
- Infrastructure as a Service (CLOUD)
- Software as a Service (CLOUD)
- Individual Courts – Hosting their own needs

Branch Data Center: ALL MODELS

For any branch data center solution, trial courts would still have servers/infrastructure required at the courthouse. The follow on-premises solutions include:

- Active Directory
- File/Document Store(s)
- Database(s) – potentially some or all
- Interactive Voice Response (IVR)
- VoIP
- Jury
- Networking

Branch Data Center: Vendor Hosted (Current CCTC Model)

PROS	CONS
Provides Full Service - Including desktop solutions	Need Cost Allocation Model - How?
Removes operational pressure from court	Licenses are not included
Vendor does updates/anti-virus	Lack of control from the Court
Vendor manages Active Directory	Generally more costly
Vendor manages servers locally and at CCTC	Very little input in specific technology solutions being deployed at Data Center
Courts are able to negotiate work with vendor for updates, hardware refresh, etc. - Madera, Lake, San Benito and Modoc, like a local data center would with court users	Connectivity Costs
Local Hardware choices remain with Court, such as servers and desktops	
No need for in-depth technical knowledge within the court	

Branch Data Center: Judicial Council Hosted

When the Workstream reviewed a Judicial Council (JC) hosted data center, the concept generated many questions and concerns, due to the level of complexity. Some of the key items that would need to be resolved included:

- New governance structure for security and network operations;
- JC staff would need to provide on-premises support services, contract with a vendor, or look to regional support;
- Need to create a new billing model for courts;
- Would need to analyze static costs of owning space or another data center already in place.

PROS	CONS
Larger quantity and get better pricing	JC Staff would have to hire subject matter experts
Branch is in full control of its Branch assets	Courts would be limited to common requirements
All Branch solutions in one location	Limited flexibility for being agile. Must plan forward.
Better pricing on software/hardware licensing	Connectivity cost

Will have the economies of Scale of other hosting solutions, like Microsoft or Amazon.	
	Forecasting becomes more important for determining future cost
	Need to build out facility to specific standards, required by Department of General Services

Branch Data Center: Virtual or Cloud

Once the Workstream vetted the more traditional data center models, complexity of the issues became very apparent, so the group focused on the most likely scenario for success, which is a hybrid of both an on-premises data center and a virtual data center. Because of the various requirements and technical diversity across the branch, utilizing a hybrid approach is most realistic, with the long-term goal of virtualizing as much of the data center as possible.

PROS	CONS
Good starting point for cloud hosting	Likely dependent upon a single vendor model
Provides Agility and Flexibility	Each court needs to have the expertise to work in a hybrid environment
Since two environments are available, Disaster Recovery can be more easily implemented	

Local Data Center

All courts today have their own local data center, running most of their applications. If the court has existing resources and expertise the local data center can prove to be a more cost effective model than the cloud hosting model.

PROS	CONS
Local Control	May or may not be higher costs, depending on existing resources
Provides Agility and Flexibility	Requires on-site court resources
	Requires court data center
	Should adhere to Department of General Services requirements for data centers.

5.2 SERVICE LEVEL DEFINTION AND TIMES

In evaluating the types of hosting solutions, it is critical to define the judicial branch's hours of operations and service requirements. After evaluation of all of the courts' technology services, the Workstream is proposing judicial branch recommendations for hours of business, service level definitions, and service level time frames:

Judicial Branch recommended hours of business:

Next Generation Hosting services should be 24/7 hours of operation.

Judicial Branch recommended Service Level Definitions:

- Critical: damage or disruption to a service that would stop court operations, public access or timely delivery of justice, with no viable work-around.
- High: damage or disruption to a service that would hinder court operations, public access or timely delivery of justice. A work-around is available, but may not be viable.
- Medium: damage or disruption to a specific service that would impact a group of users, but has a viable work-around.
- Systems Support: damage or disruption to a specific service that would not impact court operations, public access or timely delivery of justice and a viable work-around is available.

Judicial Branch recommended Service Level Agreement (SLA) times:

SLA Type	SLA Criteria	Local Data Center	Cloud
Critical	Max Time Recovery	4 hours	1 hours
Critical	Max Data Loss	1 hour	5 minutes
High	Max Time Recovery	6 hours	2 hours
High	Max Data Loss	1 hour	30 minutes
Moderate	Max Time Recovery	24 hours	24 hours
Moderate	Max Data Loss	1 Business day	1 Business day
Low	Max Time Recovery	48 hours	48 hours
Low	Max Data Loss	N/A	N/A

5.3 BRANCH WIDE ASSETS AND SERVICES LEVELS

In collaboration with the Disaster Recovery Workstream and court experts, the following list provides an inventory of court technology assets and recommended service levels in a live/production environment.

Requirement	Recommended Service Level
Infrastructure	
Internet	Critical
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical
Active Directory/DNS/DHCP	Critical
Servers (local, virtual, File, Print)	Critical
Security Device- ATT Monitoring-Internal/IDS	Critical
Virus protection	Critical
Storage	Critical
Middleware	High

Requirement	Recommended Service Level
Infrastructure	
Back-up Appliance	High
Desktops (Local, virtual, thin client)	High
Load Balancers	High
Proxy's	High
UPS/Generator/ Power	High
Data center Cooling	High
Statewide Security Access parameters (All Workstreams)	High
System Monitoring/Solarwinds	High
Spam filter	Moderate
Public Information Kiosks / Electronic signs	Moderate
Queueing system- Qmatic/Qflow	Moderate
Facilities automation	Moderate
Physical Monitoring-Temperature	Moderate
Helpdesk- IT Systems	Moderate

Requirement	Recommended Service Level
Systems	
Case Management	Critical
Jury Management	Critical
Website - Public Service Portal	Critical
E-filing	High
Communications/VoIP/Analog/Faxes	High
CCPOR/CLETS	High
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High
IVR/Call Routing	High
Electronic/Video Recording and Playback (FTR)	Moderate
Facilities Requirements- Assisted Listening (ADA)	Moderate
Building Access Controls	Moderate
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate
Court Call/Telephonic/Video appearance	Moderate
VRI - Video Remote Interpreting	Moderate
Physical Security- Video Surv.	Moderate
Video/Meeting/Conference Systems	Low

Requirement	Recommended Service Level
Applications	
E-Mail/SMTP	High
MS Office	High
Payroll Systems- Policy/Union	Moderate
Lexis Nexis	Moderate
West Law	Moderate
Jury Instructions	Moderate
Adobe (Acrobat)	Moderate
X-spouse	Moderate
Judicial workbench (CMS Component)	Moderate
SAP/Financial	Moderate
Mobile device management	Moderate
Real-time court reporting	Moderate
HR Systems (Non-SAP)	Moderate
Electronic Evidence (Policy)	Moderate
CAFM	Low
Web browser (Internet Explorer/Chrome)	Low
Locally developed applications**	Court discretion

5.4 BRANCHWIDE NEXT GENERATION RECOMMENDED SOLUTIONS

After careful review of the various solutions available, the Workstream determined the two best solutions for moving forward were either local installation or cloud services. As previously noted, courts are still required to provide many local IT solutions, such as kiosks, network equipment, and local storage., However, the majority of the court applications can run in a cloud environment. If a court has the necessary infrastructure (Internet) and the cost is equal or less than that of a local installation, the court should move to Cloud Services.

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Infrastructure			
Internet			✓
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	✓		✓

Servers (local, virtual, File, Print)	✓		✓
Security Device- ATT Monitoring-Internal/IDS	✓		✓
Virus protection	✓		✓
Storage	✓		✓
Active Directory/DNS/DHCP	✓		✓
Middleware	✓		✓
Back-up Appliance	✓		✓
Desktops (Local, virtual, thin client)	✓		✓
Load Balancers	✓		✓
Proxy's	✓		✓
UPS/Generator/ Power	✓		
Data center Cooling	✓		
Statewide Security Access parameters (All Workstreams)	✓		✓
System Monitoring/Solarwinds	✓		✓
Spam filter			✓
Public Information Kiosks / Electronic signs	✓		
Queueing system- Qmatic/Qflow			✓
Facilities automation			✓
Physical Monitoring-Temperature			✓
Helpdesk- IT Systems			✓

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Systems			
Case Management	✓	✓	✓
Jury Management	✓		✓
Website - Public Service Portal			✓
E-filing			✓
Communications/VoIP/Analog/Faxes	✓		
CCPOR/CLETS			✓
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	✓		
IVR/Call Routing	✓		✓
Video/Meeting/Conference Systems			✓
Electronic/Video Recording and Playback (FTR)	✓		✓
Facilities Requirements- Assisted Listening (ADA)	✓		
Building Access Controls	✓		

E-Warrants_PC Dec/Ipad/Magistrate phone			✓
Court Call/Telephonic/Video appearance			✓
VRI - Video Remote Interpreting			✓
Physical Security- Video Surv.	✓		✓

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Applications			
E-Mail/SMTP			✓
MS Office	✓		✓
Payroll Systems- Policy/Union			✓
Lexis Nexis			✓
West Law			✓
Jury Instructions	✓		✓
Adobe (Acrobat)			✓
X-spouse			✓
Judicial workbench (CMS Component)			✓
SAP/Financial			✓
Mobile device management			✓
Real-time court reporting	✓		
HR Systems (Non-SAP)			✓
Electronic Evidence (Policy)	✓		✓
CAFM			✓
Web browser (Internet Explorer/Chrome)			✓
Locally developed applications**	✓		✓

6.0 BRANCH-WIDE RECOMMENDATIONS

After significant analysis the Workstream has determined the following recommendations for ITAC and the Judicial Council Technology Committee:

- If the courts have the abilityand the opportunity and the cost is less than a local solution they should to move to a cloud solution;
- Adopt the recommended branch services levels and hours of operation for all data center solutions;
- Recommendation to remove VMWare vendor to future Master Service Agreement (MSA) or branch-wide agreement;

- Create new support model for defining branch impacting technology initiatives, such as next generation hosting;
- Approve phase two of next generation hosting Workstream; including pilot court and cloud service agreements;
- Microsoft is the office and email standard across the branch, whether using Exchange or Office 365; and
- Host a Webinar for Courts to become educated on Next Generation Hosting Framework.

7.0 USING NEXT GENERATION HOSTING FRAMEWORK

7.1 RECOMMENDED SERVICE LEVELS, INVENVETORY ASSETS AND SOLUTIONS

See attachment A

7.2 USE INVENTORY CHECKLIST TEMPLATE

See attachment B.

7.3 USE TECHNOLOGY ROADMAP TEMPLATE

See attachment C.

NEXT GENERATION HOSTING JUDICIAL BRANCH RECOMMENDATIONS

Hours of Operation

Data center operations and availability is 24 hours a day, 7 days a week.

Service level definitions

Critical: damage or disruption to a service that would stop court operations, public access or timely delivery of justice, with no viable work-around.

High: damage or disruption to a service that would hinder court operations, public access or timely delivery of justice. A work-around is available, but may not be viable.
Medium: damage or disruption to a specific service that would impact a group of users, but has a viable work-around.
Systems Support: damage or disruption to a specific service that would not impact court operations, public access or timely delivery of justice and a viable work-around is available.

Production service level agreement times

SLA Type	SLA Criteria	Local Data Center	Cloud
Critical	Max Time Recovery	4 hours	1 hours
Critical	Max Data Loss	1 hour	5 minutes
High	Max Time Recovery	6 hours	2 hours
High	Max Data Loss	1 hour	30 minutes
Moderate	Max Time Recovery	24 hours	24 hours
Moderate	Max Data Loss	1 Business day	1 Business day
Low	Max Time Recovery	48 hours	48 hours
Low	Max Data Loss	N/A	N/A

Inventory Assets with Services Level and viable solution

Requirement	Service Level	Applicable Solution		
		Local	Private Data Center	Cloud
Infrastructure				
Internet	Critical			✓
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical	✓		✓
Servers (local, virtual, File, Print)	Critical	✓		✓
Security Device- ATT Monitoring-Internal/IDS	Critical	✓		✓
Virus protection	Critical	✓		✓
Storage	Critical	✓		✓
Active Directory/DNS/DHCP	Critical	✓		✓
Middleware	High	✓		✓
Back-up Appliance	High	✓		✓
Desktops (Local, virtual, thin client)	High	✓		✓
Load Balancers	High	✓		✓
Proxy's	High	✓		✓
UPS/Generator/ Power	High	✓		
Data center Cooling	High	✓		
Statewide Security Access parameters (All workstreams)	High	✓		✓
System Monitoring/Solarwinds	High	✓		✓
Spam filter	Moderate			✓
Public Information Kiosks / Electronic signs	Moderate	✓		
Queueing system- Qmatic/Qflow	Moderate			✓
Facilities automation	Moderate			✓
Physical Monitoring-Temperature	Moderate			✓
Helpdesk- IT Systems	Moderate			✓

Requirement	Service Level	Applicable Solution		
		Local	Private Data Center	Cloud
Systems				
Case Management	Critical	✓	✓	✓
Jury Management	Critical	✓		✓
Website - Public Service Portal	Critical			✓
E-filing	High			✓
Communications/VoIP/Analog/Faxes	High	✓		
CCPOR/CLETS	High			✓
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High	✓		
IVR/Call Routing	High	✓		✓
Video/Meeting/Conference Systems	Low			✓
Electronic/Video Recording and Playback (FTR)	Moderate	✓		✓
Facilities Requirements- Assisted Listening (ADA)	Moderate	✓		
Building Access Controls	Moderate	✓		
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate			✓
Court Call/Telephonic/Video appearance	Moderate			✓
VRI - Video Remote Interpreting	Moderate			✓
Physical Security- Video Surv.	Moderate	✓		✓

Requirement	Service Level	Applicable Solution		
		Local	Private Data Center	Cloud
Applications				
E-Mail/SMTP	High			✓
MS Office	High	✓		✓
Payroll Systems- Policy/Union	Moderate			✓
Lexis Nexis	Moderate			✓
West Law	Moderate			✓
Jury Instructions	Moderate	✓		✓
Adobe (Acrobat)	Moderate			✓
X-spouse	Moderate			✓
Judicial workbench (CMS Component)	Moderate			✓
SAP/Financial	Moderate			✓
Mobile device management	Moderate			✓
Real-time court reporting	Moderate	✓		
HR Systems (Non-SAP)	Moderate			✓
Electronic Evidence (Policy)	Moderate	✓		✓
CAFM	Low			✓
Web browser (Internet Explorer/Chrome)	Low			✓
Locally developed applications**	Court discretion	✓		✓

Roadmap Pricing Matrix (will be finalized with Phase 2):

Requirement	Service Level	Cloud Solution				
Infrastructure			X-Large /Branch	Large	Medium	Small
Internet	Critical	✓				$$
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical	✓				
Servers (local, virtual, File, Print)	Critical	✓				$
Security Device- ATT Monitoring-Internal/IDS	Critical	✓				$$
Virus protection	Critical	✓				
Storage	Critical	✓				
Active Directory/DNS/DHCP	Critical	✓	$$		$$	
Middleware	High	✓				
Back-up Appliance	High	✓	$			
Desktops (Local, virtual, thin client)	High	✓				
Load Balancers	High	✓				
Proxy's	High	✓				
UPS/Generator/ Power	High					
Data center Cooling	High					
Statewide Security Access parameters (All workstreams)	High	✓				
System Monitoring/Solarwinds	High	✓	$		$$	$
Spam filter	Moderate	✓	$			
Public Information Kiosks / Electronic signs	Moderate					
Queueing system- Qmatic/Qflow	Moderate	✓				
Facilities automation	Moderate	✓				
Physical Monitoring-Temperature	Moderate	✓				
Helpdesk- IT Systems	Moderate	✓				

Extra Large /Branch	$$$	$1,000,000-$5,000,000	**Medium Court:**	$$$	$150,000-$250,000
	$$	$200,000-$999,999		$$	$50,000-$150,000
	$	$15,000-$199,999		$	$5,000-$50,000
Large Court:	$$$	$250,000-$500,000	**Small Court:**	$$$	$30,000-$60,000
	$$	$xxxxxx.xx-$xxxxx		$$	$10,000-$30,000
	$	$xxxxxx.xx-$xxxxx		$	$1,000-$10,000

Requirement	Service Level	Cloud				
Systems			X-Large /Branch	Large	Medium	Small
Case Management	Critical	✓	$$$	$$$	$$$	$$$
Jury Management	Critical	✓	$$		$$	$
Website - Public Service Portal	Critical	✓	$$		$	
E-filing	High	✓	$$			
Communications/VoIP/Analog/Faxes	High					
CCPOR/CLETS	High	✓				
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High					
IVR/Call Routing	High	✓				
Video/Meeting/Conference Systems	Low	✓				$
Electronic/Video Recording and Playback (FTR)	Moderate	✓				
Facilities Requirements- Assisted Listening (ADA)	Moderate					
Building Access Controls	Moderate					
E-Warrants/ PC Dec/Ipad/Magistrate phone	Moderate	✓				
Court Call/Telephonic/Video appearance	Moderate	✓				
VRI - Video Remote Interpreting	Moderate	✓				$
Physical Security- Video Surveillance	Moderate	✓				

Extra Large /Branch	$$$	$1,000,000-$5,000,000
	$$	$200,000-$999,999
	$	$15,000-$199,999
Large Court:	$$$	$250,000-$500,000
	$$	$xxxxxx.xx-$xxxxx
	$	$xxxxxx.xx-$xxxxx

Medium Court:	$$$	$150,000-$250,000
	$$	$50,000-$150,000
	$	$5,000-$50,000
Small Court:	$$$	$30,000-$60,000
	$$	$10,000-$30,000
	$	$1,000-$10,000

Requirement	Service Level	Cloud				
Applications			X-Large /Branch	Large	Medium	Small
E-Mail/SMTP	High	✓	$$ O365	$$$ O365	$ Email	$$ O365
MS Office	High	✓				
Payroll Systems- Policy/Union	Moderate	✓				$
Lexis Nexis	Moderate	✓				$
West Law	Moderate	✓				$
Jury Instructions	Moderate	✓				
Adobe (Acrobat)	Moderate	✓				
X-spouse	Moderate	✓				
Judicial workbench (CMS Component)	Moderate	✓				
SAP/Financial	Moderate	✓				
Mobile device management	Moderate	✓				
Real-time court reporting	Moderate					
HR Systems (Non-SAP)	Moderate	✓				
Electronic Evidence (Policy)	Moderate	✓				
CAFM	Low	✓				
Web browser (Internet Explorer/Chrome)	Low	✓				
Locally developed applications**	Court discretion	✓				

Extra Large /Branch	$$$	$1,000,000-$5,000,000
	$$	$200,000-$999,999
	$	$15,000-$199,999
Large Court:	$$$	$250,000-$500,000
	$$	$xxxxxx.xx-$xxxxx
	$	$xxxxxx.xx-$xxxxx

Medium Court:	$$$	$150,000-$250,000
	$$	$50,000-$150,000
	$	$5,000-$50,000
Small Court:	$$$	$30,000-$60,000
	$$	$10,000-$30,000
	$	$1,000-$10,000

Court Data Center Inventory list and Service Levels

Recommend Service Level				Court Defined Service Level			
SLA Type	**SLA Criteria**	**Local Data Center**	**Cloud**	**SLA Type**	**SLA Criteria**	**Local Data Center**	**Cloud**
Critical	Max Time Recovery	4 hours	1 hours	**Critical**	Max Time Recovery		
Critical	Max Data Loss	1 hour	5 minutes	**Critical**	Max Data Loss		
High	Max Time Recovery	6 hours	2 hours	**High**	Max Time Recovery		
High	Max Data Loss	1 hour	30 minutes	**High**	Max Data Loss		
Moderate	Max Time Recovery	24 hours	24 hours	**Moderate**	Max Time Recovery		
Moderate	Max Data Loss	1 Business day	1 Business day	**Moderate**	Max Data Loss		
Low	Max Time Recovery	48 hours	48 hours	**Low**	Max Time Recovery		
Low	Max Data Loss	N/A	N/A	N/A	N/A		

Requirement	**Recommend Service Level**	**Court Service Level**	**Applicable Solution**		**Estimated Amount $$ from Road Map**			
			Local	**Cloud**	**Year 1**	**Year 2**	**Year 3**	**Year 4**
Infrastructure								
Internet	Critical							
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical							
Servers (local, virtual, File, Print)	Critical							
Security Device- ATT Monitoring-Internal/IDS	Critical							
Virus protection	Critical							
Storage	Critical							
Active Directory/DNS/DHCP	Critical							
Middleware	High							
Back-up Appliance	High							
Desktops (Local, virtual, thin client)	High							
Load Balancers	High							
Proxy's	High							
UPS/Generator/ Power	High							
Data center Cooling	High							
Statewide Security Access parameters (All workstreams)	High							
System Monitoring/Solarwinds	High							
Spam filter	Moderate							
Public Information Kiosks / Electronic signs	Moderate							
Queueing system- Qmatic/Qflow	Moderate							
Facilities automation	Moderate							
Physical Monitoring-Temperature	Moderate							
Helpdesk- IT Systems	Moderate							
					$0.00	$0.00	$0.00	$0.00
					ESTIMATED STRATEGIC BUDGET			**$0.00**

Requirement	**Recommend Service Level**	**Court Service Level**	**Applicable Solution**		**Estimated Amount $$ from Road Map**			
			Local	**Cloud**	**Year 1**	**Year 2**	**Year 3**	**Year 4**
Systems								
Case Management	Critical							
Jury Management	Critical							
Website - Public Service Portal	Critical							
E-filing	High							
Communications/VoIP/Analog/Faxes	High							
CCPOR/CLETS	High							
DMV- Justice Partners Branch and local (Lan/Wan- Connec	High							
IVR/Call Routing	High							
Video/Meeting/Conference Systems	Low							
Electronic/Video Recording and Playback (FTR)	Moderate							
Facilities Requirements- Assisted Listening (ADA)	Moderate							
Building Access Controls	Moderate							
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate							
Court Call/Telephonic/Video appearance	Moderate							
VRI - Video Remote Interpreting	Moderate							
Physical Security- Video Surv.	Moderate							
					$0.00	$0.00	$0.00	$0.00
					ESTIMATED STRATEGIC BUDGET			$0.00

Requirement	Recommend Service Level	Court Service Level	Applicable Solution		Estimated Amount $$ from Road Map			
			Local	Cloud	Year 1	Year 2	Year 3	Year 4
Applications								
E-Mail/SMTP	High							
MS Office	High							
Payroll Systems- Policy/Union	Moderate							
Lexis Nexis	Moderate							
West Law	Moderate							
Jury Instructions	Moderate							
Adobe (Acrobat)	Moderate							
X-spouse	Moderate							
Judicial workbench (CMS Component)	Moderate							
SAP/Financial	Moderate							
Mobile device management	Moderate							
Real-time court reporting	Moderate							
HR Systems (Non-SAP)	Moderate							
Electronic Evidence (Policy)	Moderate							
CAFM	Low							
Web browser (Internet Explorer/Chrome)	Low							
Locally developed applications**	Court discretion							
					$0.00	$0.00	$0.00	$0.00
					ESTIMATED STRATEGIC BUDGET			$0.00

SAMPLE ROADMAP

Costs are samples from existing trial courts

Budget Year 1: $200,000 Budget Year 2: $300,000 Budget Year 3: $250,000 Budget Year 4: $250,000.00

Requirement	Service Level	Cloud Solution				
Infrastructure			X-Large/Branch	Large	Medium	Small
Internet	Critical	✓				$$
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical	✓				
Servers (local, virtual, File, Print)	Critical	✓				$
Security Device- ATT Monitoring-Internal/IDS	Critical	✓				$$
Virus protection	Critical	✓				
Storage	Critical	✓				
Active Directory/DNS/DHCP	Critical	✓	$$		$$	
Middleware	High	✓				
Back-up Appliance	High	✓	$			
Desktops (Local, virtual, thin client)	High	✓				
Load Balancers	High	✓				
Proxy's	High	✓				
UPS/Generator/ Power	High					
Data center Cooling	High					
Statewide Security Access parameters (All workstreams)	High	✓				
System Monitoring/Solarwinds	High	✓	$		$$	$
Spam filter	Moderate	✓	$			
Public Information Kiosks / Electronic signs	Moderate					
Queueing system- Qmatic/Qflow	Moderate	✓				
Facilities automation	Moderate	✓				
Physical Monitoring-Temperature	Moderate	✓				
Helpdesk- IT Systems	Moderate	✓				

Extra Large/Branch	$$$	$1,000,000-$5,000,000	**Medium Court:**	$$$	$150,000-$250,000
	$$	$200,000-$999,999		$$	$50,000-$150,000
	$	$15,000-$199,999		$	$5,000-$50,000
Large Court:	$$$	$250,000-$500,000	**Small Court:**	$$$	$30,000-$60,000
	$$	$xxxxxx.xx-$xxxxx		$$	$10,000-$30,000
	$	$xxxxxx.xx-$xxxxx		$	$1,000-$10,000

Requirement	Service Level	Cloud				
Systems						
Case Management	Critical	✓	$$$	$$$	$$$	$$$
Jury Management	Critical	✓	$$		$$	$
Website - Public Service Portal	Critical	✓	$$		$	
E-filing	High	✓	$$			
Communications/VoIP/Analog/Faxes	High					
CCPOR/CLETS	High	✓				
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High					
IVR/Call Routing	High	✓				
Video/Meeting/Conference Systems	Low	✓				$
Electronic/Video Recording and Playback (FTR)	Moderate	✓				
Facilities Requirements- Assisted Listening (ADA)	Moderate					
Building Access Controls	Moderate					
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate	✓				
Court Call/Telephonic/Video appearance	Moderate	✓				
VRI - Video Remote Interpreting	Moderate	✓				$
Physical Security- Video Surv.	Moderate	✓				

Extra Large/Branch	$$$	$1,000,000-$5,000,000	**Medium Court:**	$$$	$150,000-$250,000
	$$	$200,000-$999,999		$$	$50,000-$150,000
	$	$15,000-$199,999		$	$5,000-$50,000
Large Court:	$$$	$250,000-$500,000	**Small Court:**	$$$	$30,000-$60,000
	$$	$xxxxxx.xx-$xxxxx		$$	$10,000-$30,000
	$	$xxxxxx.xx-$xxxxx		$	$1,000-$10,000

Requirement	Service Level	Cloud				
Applications						
E-Mail/SMTP	High	✓	$$ O365	$$$ O365	$ (Email Only)	$$ O365
MS Office	High	✓				
Payroll Systems- Policy/Union	Moderate	✓				$
Lexis Nexis	Moderate	✓				$
West Law	Moderate	✓				$
Jury Instructions	Moderate	✓				
Adobe (Acrobat)	Moderate	✓				
X-spouse	Moderate	✓				

Judicial workbench (CMS Component)			Moderate	✓			
SAP/Financial			Moderate	✓			
Mobile device management			Moderate	✓			
Real-time court reporting			Moderate				
HR Systems (Non-SAP)			Moderate	✓			
Electronic Evidence (Policy)			Moderate	✓			
CAFM			Low	✓			
Web browser (Internet Explorer/Chrome)			Low	✓			
Locally developed applications**			Court discretion	✓			
Extra Large/Branch	$$$	$1,000,000-$5,000,000			**Medium Court:**	$$$	$150,000-$250,000
	$$	$200,000-$999,999				$$	$50,000-$150,000
	$	$15,000-$199,999				$	$5,000-$50,000
Large Court:	$$$	$250,000-$500,000			**Small Court:**	$$$	$30,000-$60,000
	$$	$xxxxxx.xx-$xxxxx				$$	$10,000-$30,000
	$	$xxxxxx.xx-$xxxxx				$	$1,000-$10,000

Requirement	Recommended Service Level
Infrastructure	
Internet	Critical
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical
Active Directory/DNS/DHCP	Critical
Servers (local, virtual, File, Print)	Critical
Security Device- ATT Monitoring-Internal/IDS	Critical
Virus protection	Critical
Storage	Critical
Middleware	High
Back-up Appliance	High
Desktops (Local, virtual, thin client)	High
Load Balancers	High
Proxy's	High
UPS/Generator/ Power	High
Data center Cooling	High
Statewide Security Access parameters (All workstreams)	High
System Monitoring/Solarwinds	High
Spam filter	Moderate
Public Information Kiosks / Electronic signs	Moderate
Queueing system- Qmatic/Qflow	Moderate
Facilities automation	Moderate
Physical Monitoring-Temperature	Moderate
Helpdesk- IT Systems	Moderate

Technology Initiatives to Optimize Branch Resources

Expand Collaboration within the Branch IT Community

Description

This initiative is intended to identify opportunities for sharing technical resources, advancing technology leadership, and expanding collaboration throughout the judicial branch. During the tactical plan revision process, judges, CEOs, and CIOs identified that, although there are experienced technological staff branchwide, insufficient technology resources within individual courts continues to be a challenge. A skilled technologist who understands the business of the courts and court systems is a unique and treasured resource. Furthermore, the branch is competing with private industry for talent. A strategy should be developed to increase the sharing of technical resources throughout the branch by conducting a needs assessment and determining additional opportunities for how best to share these unique resources.

In addition to skilled technologists, strong information technology (IT) leaders with access to industry resources are required to achieve the branch strategic technology goals. Opportunities for education and access to industry resources for IT leaders can provide exposure to information and networks while expanding capabilities and increasing IT leadership skills. Court IT leaders will be better suited to meet the leadership and technological needs of the courts with continued professional development. A survey can be conducted to determine the needs and interests of the court and Judicial Council IT leaders. A strategy would then be developed to determine how best to pursue relevant opportunities (e.g., statewide membership in the Court IT Officers Consortium (CITOC), an annual IT summit aligned with the branchwide tactical plan, continuing education opportunities, industry research, and advisory group memberships).

Aside from the need for skilled IT resources, the branch has adopted an IT governance model that relies on collaboration. Technology initiatives managed by statewide workstreams, the Court Information Technology Management Forum (CITMF), and court-to-court collaborations have proven successful in recent years across the branch and between courts. In order to further support this collaborative model, the branch should adopt tools to work together more effectively, encourage innovation, and increase technological maturity throughout the branch. Resources and talent can be better leveraged across the branch by utilizing a statewide collaboration platform. Branch CEOs and CIOs can also help assess individual court IT capabilities through an IT peer consulting program to include informal audits, visitation programs, and the like.

Major Tasks

Resource Sharing

- Conduct an IT resource needs survey.
- Identify opportunities and priorities.
- Brainstorm strategies and costs (e.g., develop centers of excellence, shared services, and centralized resources, and augment staff with vendor support).
- Make recommendations for leveraging branch technical resources.

IT Leadership Development

- Expand CIO Executive Board membership.
- Establish branchwide CITOC membership.
- Evaluate branchwide Gartner Group membership.
- Hold an annual IT summit aligned with the branchwide tactical plan.
- Conduct an IT leadership needs survey to identify additional priorities.
- Brainstorm strategies and costs.

Increased Collaboration to Support Innovation

- Identify collaboration tools currently used within the branch.
- Identify priority collaboration needs (e.g., a central repository of IT policies, applications, and best practices).
- Increase the use of Microsoft Office 365 messaging and web conference capabilities.
- Determine CEO/CIO interest in an IT peer consulting program.
- Develop program based on interest.
- Determine costs.

Dependencies

- Branchwide support and open collaboration.
- Program management support for conducting surveys and consolidating results.
- Funding for recommended strategies.
- Common platforms and development tools.
- Sponsorship of IT leadership development and participation.

Funding Requirements

One-Time

- Judicial Council program support to conduct the needs assessment.
- Establishment of a branch collaboration platform
- Travel for face-to-face collaboration and participation in initiative development.

Ongoing

- Judicial Council program support as required.
- Annual memberships—CITOC, CIO Executive Board, Gartner Group.
- IT summit development and coordination.
- Travel for face-to-face collaboration and participation in events (e.g., IT summit, IT peer consulting program, etc.).
- Maintenance and licensing of branch collaboration platform.

Potential Funding Sources

- Cost agreements for shared resources.
- BCP for necessary funding.

Types of Courts Involved

- All small, medium, and large courts statewide
- Trial and appellate courts
- Consortiums (e.g., case management specific, statewide initiatives, etc.)

Sample Timeline

Milestone	Time Frame
Initiative launch	Q1 2017
Draft initial assessment	Q4 2017
Final assessment report	Q3 2018

Information Technology Advisory Committee
Q2 2017 Status Report

June 2017

This report was provided at the **June 9, 2017** ITAC meeting. Status updates are submitted by workstream sponsors and subcommittee chairs.

Profile

1. Tactical Plan Update

Summary	Update Tactical Plan for Technology for Effective Date 2017-2018
ITAC Resource	Workstream
Sponsor(s) or Chair(s)	Hon. Terence L. Bruiniers PM: Ms. Kathleen Fink
JCC Resources	JCIT (Kathleen Fink, Jamel Jones)
Project Authorized	☒ Yes. Approved in 2016 Annual Agenda (1/11/2016); reapproved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Approved by ITAC Chair (5/3/2016) and JCTC (6/3/2016); forwarded to E&P (staff).
Project Active	☐ No. Project was completed and workstream has sunset.
Expected Outcomes	1. Tactical Plan for Technology 2017-2018
Expected Completion	April 2017

Status Report

1. Tactical Plan Update

Highlight: Updated Tactical Plan adopted by the Judicial Council, effective immediately. Workstream is now complete.

Major Tasks	Status	Description
(a) Complete circulation of updated Tactical Plan for public comment and revise, as needed.	Complete	The Tactical Plan for Technology 2017-2018 was circulated for public comment between December 16, 2016 and January 23, 2017. During the formal comment period, two commentators agreed with the proposal if modified, and four did not indicate their position on the proposal as a whole, but provided comments on specific aspects of the proposal. Overall, the feedback was constructive and generally helped to further clarify ambiguities. Revisions were incorporated where the workstream agreed it was appropriate.
(b) Finalize and submit for approval to the JCTC and the Judicial Council.	Complete	The red-lined Tactical Plan for Technology 2017-2018 and the chart of public comments were circulated to ITAC for action by email to recommend Judicial Council adoption of the Tactical Plan 2017-2018. ITAC and the JCTC approved the recommendation. Justice Bruiniers, Judge Hanson, and Rob Oyung presented the updated plan to the Judicial Council at its March 24 meeting, during which it was approved. The update became effective immediately.

Profile

2. Next Generation Hosting Strategy

Summary	Assess Alternatives for Transition to a Next-Generation Branchwide Hosting Model
ITAC Resource	Workstream
Sponsor(s) or Chair(s)	Hon. Jackson Lucky, Mr. Brian Cotta PM: Ms. Heather Pettit
JCC Resources	JCIT (Donna Keating and other SMEs, as needed)
Project Authorized	☒ Yes. Approved in 2016 Annual Agenda (1/11/2016); reapproved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Approved by ITAC Chair (8/21/2015) and JCTC (9/15/2015); forwarded to E&P (staff).
Project Active	☒ Yes, meeting ad-hoc.
Expected Outcomes	1. Assessment Findings: Best practices, Solution Options 2. Educational Document for Courts 3. Host 1-Day Summit on Hosting 4. Recommendations For Branch-level Hosting
Expected Completion	June 2017

Status Report

2. Next Generation Hosting Strategy

Highlight: Draft deliverables—best practices, roadmap template, requirements, and recommendations—readied for presentation and input from ITAC.

Major Tasks	Status	Description
(a) Define workstream project schedule and detailed tasks.	Complete	A high-level project schedule/plan was developed and progressively detailed as topics completed.
(b) Outline industry best practices for hosting (including solution matrix with pros, cons, example applications, and costs).	In Progress-circulating	Draft framework, roadmap tool, data center (infrastructure, systems, applications) inventory, and recommendations drafted by the workstream for preview to ITAC at its June 9 meeting. Refer to meeting materials. Following incorporation of further input, deliverables will be readied for final approval—targeting the August ITAC meeting.
(c) Produce a roadmap tool for use by courts in evaluating options.	In Progress-circulating	See item (b) above.
(d) Consider educational summit on hosting options, and hold summit if appropriate.	In Progress	Still under evaluation, but likely not to happen as a dedicated summit specific to this workstream.
(e) Identify requirements for centralized hosting.	In Progress-circulating	See item (b) above.
(f) Recommend a branch-level hosting strategy.	In Progress-circulating	See item (b) above.

Profile

3. Disaster Recovery Framework

Summary	Document and Adopt a Court Disaster Recovery Framework
ITAC Resource	Workstream
Sponsor(s) or Chair(s)	Hon. Alan Perkins, Mr. Brian Cotta PM: Mr. Brian Cotta
JCC Resources	JCIT (Michael Derr)
Project Authorized	☒ Yes. Approved in 2016 Annual Agenda (1/11/2016); reapproved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Approved by ITAC Chair (4/21/2016) and JCTC Chair (4/27/2016); forwarded to E&P (staff).
Project Active	☒ Yes, meeting ad-hoc.
Expected Outcomes	1. Disaster Recovery Framework Document and Checklist 2. BCP Recommendations
Expected Completion	June 2017

Status Update

3. Disaster Recovery Framework

Highlight: Draft final deliverables—framework document, adaptable plan, and "how to" guide—readied for presentation to ITAC.

Major Tasks	Status	Description
(a) Develop model disaster recovery guidelines, standard recovery times, and priorities for each of the major technology components of the branch.	In Progress-circulating	The **framework document** provides guidelines including of recovery times, backup and high availability options, scenario planning, application, etc. This document is complete, copy-edited, and readied for presentation to ITAC at June 9 meeting. Following the ITAC meeting, review/comment to be solicited from branch CIO's and CEO's, prior to gaining ITAC final approval.
(b) Develop a disaster recovery framework document that could be adapted for any trial or appellate court to serve as a court's disaster recovery plan.	In Progress-circulating	The **adaptable plan/template document** is complete and will be used by a court to create its disaster recovery plan. The template has been readied for presentation to ITAC at its June 9 meeting. Following the ITAC meeting, review/comment to be solicited from branch CIO's and CEO's, prior to gaining ITAC final approval.
(c) Create a plan for providing technology components that could be leveraged by all courts for disaster recovery purposes.	Complete	The framework document includes recommendations for courts to leverage and pattern themselves after. The plan is to identify technologies that are in use and available today that courts can use or purchase; and, any needs beyond the resources of the branch are recommended to be addressed via BCP for FY19-20 funding.
(d) Develop recommendations for a potential BCP (e.g., if it is appropriate to fund a pilot, to assist courts, or to purchase any products). (Note: Drafting a BCP would be a separate effort.)	Complete	The workstream recommends that ITAC move forward with developing a BCP seeking FY19-20 funds and keeping the following in mind: (a) Fall 2017- Courts be resurveyed regarding their DR posture since many will have changed; (b) January 2018- BCP leads prepare initial funding request and concept documents; (c) May/June/July 2018- BCP leads complete full BCP for submission to JCC Budget Office August 1 The ITAC Chair will need to designate a lead to co-draft the BCP with JCC support.
(e) Coordinate and plan with JCIT regarding operational support, if appropriate.	Not Started	Not relevant until/if BCP gets approved. N/A at this time.

Profile

4. E-Filing Strategy

Summary	Update E-Filing Standards; Develop Provider Certification and a Deployment Strategy
ITAC Resource	Workstream
Sponsor(s) or Chair(s)	Hon. Sheila F. Hanson PM: Mr. Snorri Ogata
JCC Resources	JCIT (Edmund Herbert), Legal Services (Patrick O'Donnell, Andrea Jaramillo), Procurement (Paula Coombs)
Project Authorized	☒ Yes. Approved in 2016 Annual Agenda (1/11/2016); reapproved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Approved by ITAC Chair (8/21/2015) and JCTC (9/15/2015); forwarded to E&P (staff).
Project Active	☒ Yes, meeting ad-hoc.
Expected Outcomes	1. Selection of Statewide EFMs 2. Certification Program 3. E-Filing Roadmap and Implementation Plan 4. Selection of Identity Management Service/Provider
Expected Completion	December 2017

Status Update

4. E-Filing Strategy

Highlight: Five vendors respond with proposals to solicitation for statewide e-filing managers. General fund loan to provide support for branch e-filing included in Governor's May Revise.

Major Tasks	Status	Description
(a) Develop and issue an RFP for statewide E-Filing Managers (EFMs).	Complete	The workstream completed and posted the RFP.
(b) Select statewide EFMs.	In Progress	Five proposals were submitted from Vendors for selection as a Statewide E-Filing Manager (EFM). The proposals are currently being evaluated and scored. There will be an opportunity for the responding vendors to demo their products. Then a bidder's conference will be held ahead of final selection, expected in July 2017.
(c) Develop the E-Filing Service Provider (EFSP) selection/certification process.	In Progress	The request for a general fund loan to provide staffing to assist in developing and maintaining a statewide e-filing environment that promotes, enables, and assists full court participation in e-filing was included in the Governor's May Revise, and is pending final passage/signature. If approved, the positions will establish and support e-filing standards management, certification, and e- implementation services along with integration with an identity management system and preferred financial gateways. The loan would be repaid through a nominal court cost recovery fee (estimated to be $0.30 per e-filing transaction). Meanwhile, MTG consulting was hired to assist in developing the certification process for EFSPs seeking to access the California e-filing business. The group is exploring the possibility of using the IJIS Institute's Springboard Certification process.
(d) Develop the roadmap for an e-filing deployment strategy, approach, and branch solutions/alternatives.	Complete	At its June 2016 meeting the Judicial Council approved the Workstream's roadmap recommendations. Recommendations included: statewide policies, high-level functional requirements, and direction for ITAC to undertake and manage a procurement process to select multiple EFMs. Further, a proposed deployment timeline was submitted as part of the BCP request.

Continued next page.

Status Update

4. E-Filing Strategy (continued)

Highlight: Five vendors respond with proposals to solicitation for statewide e-filing managers. General fund loan to provide support for branch e-filing included in Governor's May Revise.

Major Tasks	Status	Description
(e) Report on the plan for implementation of the approved NIEM/ECF standards, including effective date, per direction of the Judicial Council at its June 24, 2016 meeting.	Not Started	All 5 bidders have indicated full support for ECF/NIEM.
(f) Identify and select and identity management service/provider.	In Progress	In an action by email, ITAC approved/supported the development of a BCP to support a Single Sign on solution statewide. It will be considered by the Judicial Branch Budget Committee on June 15. Meanwhile, the leads of the Self-Represented Litigants, Next Generation Hosting Strategy, and E-Filing Strategy Workstreams and staff have met with Gartner and the California Department of Technology to discuss possible strategies and approaches.
(g) Coordinate and plan with JCIT regarding operational support, if appropriate.	Not Started	

Profile

5. Self-Represented Litigants (SRL) E-Services

Summary	Develop Requirements and a Request for Proposal (RFP) for Establishing Online Branchwide Self-Represented Litigants (SRL) E-Services
ITAC Resource	Workstream
Sponsor(s) or Chair(s)	Hon. Robert Freedman, Hon. James Mize PM: Mr. Brett Howard
JCC Resources	JCIT (Mark Gelade) and CFCC (Karen Cannata, Diana Glick)
Project Authorized	☒ Yes. Approved in 2016 Annual Agenda (1/11/2016); reapproved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Approved ITAC Chair (4/5/2016) and JCTC (4/14/2016); forwarded to E&P (staff).
Project Active	☒ Yes, meeting monthly with breakout working groups meeting in between.
Expected Outcomes	1. SRL Portal Requirements Document 2. Request for Information (RFI) and Request for Proposal (RFP)
Expected Completion	December 2017

Status Update

5. Self-Represented Litigants (SRL) E-Services

Highlight: BCP Concept document drafted, submitted, and approved by ITAC and the JCTC.

Major Tasks	Status	Description
(a) Develop requirements for branchwide SRL e-capabilities to facilitate interactive FAQ, triage functionality, and document assembly to guide SRLs through the process, and interoperability with the branchwide e-filing solution. The portal will be complementary to existing local court services.	In Progress	• SRL E-Services In-Person Meeting held on February 15, 2017, in San Francisco-JCC Offices, to begin brainstorming requirements and scope. At this meeting, the Workstream determined the need to move forward with an RFI to collect information on SRL E-services and costing for those services. An RFP would then be developed to send to vendors to bid on specific services. • Meeting held with JCC Procurement staff on March 6, 2017, to discuss coordination and assistance on RFI (Request for Information) • RFI Draft is in progress and is targeted for review by the workstream at the end of June. • Submitted Initial Funding Request (IFR, pre-budget change proposal) to secure funds for the development of the SRL E-Services solution as well as ongoing maintenance for the solution. The IFR/Concept were approved/supported by ITAC and JCTC. The Judicial Branch Budget Committee will review all IFRs/Concepts on June 15 for formal approval to move forward with developing a full BCP.
(b) Determine implementation options for a branch-branded SRL E-Services website that takes optimal advantage of existing branch, local court, and vendor resources.	Not Started	
(c) Coordinate and plan with JCIT regarding operational support, if appropriate.	Not Started	
Note: In scope for 2017 is development of an RFP; out of scope is the actual implementation.		

Profile

6. Video Remote Interpreting (VRI) Pilot

Summary	Consult As Requested and Implement Video Remote Interpreting Pilot (VRI) Program
ITAC Resource	Workstream
Sponsor(s) or Chair(s)	Hon. Terence L. Bruiniers PM: Lisa Crownover
JCC Resources	Court Operations Special Services Office (Olivia Lawrence, Doug Denton, Lisa Crownover, Anne Marx); JCIT (Jenny Phu, Fati Farmanfarmaian)
Project Authorized	☒ Yes. Approved in 2016 Annual Agenda (1/11/2016); reapproved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Approved by ITAC Chair (8/20/2016) and JCTC (9/8/2016); forwarded to E&P (staff).
Project Active	☒ Yes, meeting ad-hoc.
Expected Outcomes	1. Implementation of VRI Pilot Program 2. Recommendations for Updated Technical Standards
Expected Completion	September 2018

Status Update

6. Video Remote Interpreting (VRI) Pilot

Highlight: All vendor contracts executed, courtroom sites identified, project website launched. Team is on track to launch pilot in July 2017.

Major Tasks	Status	Description
In cooperation and under the direction of the Language Access Plan Implementation Task Force (LAPITF) Technological Solutions Subccommittee (TSS): (a) Support implementation of the Assessment Period of the VRI pilot program (including kickoff, court preparations, site visits, and deployment), as requested.	In Progress	• In March 2017, the Video Response Interpreting (VRI) Pilot Project web page (http://www.courts.ca.gov/VRI.htm) was launched on the California courts public website, and the preliminary evaluation report was completed. • In May 2017, the contracts for Paras & Associates (vendor), Connected Justice Consortium (vendor), and the San Diego State University Research Foundation (independent evaluator) were executed. • Vendor site visits are being scheduled for June 2017. • Meetings with Workstream members are underway on the training plan. • Team anticipates meeting its goal to commence the VRI pilot in July 2017.
(b) Review pilot findings; validate, refine, and amend, if necessary, the technical standards.	Not Started	
(c) Identify whether new or amended rules of court are needed (and advise the Rules & Policy Subcommittee for follow up).	Not Started	
(d) Consult and collaboratewith LAPITF, as needed, in preparing recommendations to the Judicial Council on VRI implementations.	Not Started	
(e) Coordinate and plan with JCIT regarding operational support, if appropriate.	Not Started	

Profile

7. Intelligent Forms Phase I: Scoping

Summary	Investigate Options for Modernizing the Electronic Format and Delivery of Judicial Council Forms
ITAC Resource	Workstream
Sponsor(s) or Chair(s)	Hon. Jackson Lucky PM: Camilla Kieliger
JCC Resources	Legal Services (Camilla Kieliger), JCIT (TBD)
Project Authorized	☒ Yes. Approved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Membership approved by ITAC Chair 4/27/2017; and by JCTC Chairs 5/5/2017.
Project Active	☒ Yes, meeting bi-weekly.
Expected Outcomes	1. Recommendations on approach to modernize forms 2. BCP Recommendations
Expected Completion	September 2017

Status Update

7. Intelligent Forms Phase I: Scoping

Highlight: Held kickoff meeting on May 16; meeting bi-weekly.

Major Tasks	Status	Description
Investigate, prioritize and scope a project, including: (a) Evaluate Judicial Council form usage (by courts, partners, litigants) and recommend a solution that better aligns with CMS operability and better ensures the courts' ability to adhere to quality standards and implement updates without reengineer.	Not Started	The workstream membership was approved May 5, and the team held its kickoff meeting by teleconference on May 16. The kickoff included an introduction of members, their skillsets, and interests along with an orientation to the workstream's charge. Members were assigned homework: provide overview of forms consumption at each court; advantages and obstacles encountered in local form processing and reported by end users. The team established a bi-weekly standing meeting schedule and also began to use Slack as their method for communication/collaboration. The next meeting will be held June 6.
(b) Address form security issues that have arisen because of the recent availability and use of unlocked Judicial Council forms in place of secure forms for e-filing documents into the courts; seek solutions that will ensure the forms integrity and preserves legal content.	Not Started	
(c) Investigate options for redesigning forms to take advantages of new technologies, such as document assembly technologies.	Not Started	
(d) Investigate options for developing a standardized data dictionary that would enable "smart forms" to be efficiently electronically filed into the various modern CMSs across the state.	Not Started	
(e) Explore the creation and use of court generated text-based forms as an alternative to graphic forms.	Not Started	

Profile

8 – 12. Rules & Policy Subcommittee Projects

Summary	*Various Projects, refer to following slides*
ITAC Resource	Rules & Policy Subcommittee
Sponsor(s) or Chair(s)	Hon. Peter J. Siggins PM: N/A
JCC Resources	Legal Services (Patrick O'Donnell, Andrea Jaramillo, Jane Whang, Camilla Kieliger), JCIT (Fati Farmanfarmaian)
Project Authorized	☒ Yes. Approved in 2017 Annual Agenda (1/9/2017).
Membership Est'd	☒ Rules & Policy Subcommittee
Active	☒ Yes, meeting ad-hoc.
Expected Outcomes	1. Rule and/or Legislative Proposal(s), if appropriate
Expected Completion	Ongoing

Status Update

8. Modernize Rules of Court for Trial Courts

Highlight: Subcommittees reviewed both proposals' comments and staff analysis and recommendations, and voted to advance the legislative proposal to ITAC and CSCAC.

Major Tasks	Status	Description

(a) In collaboration with other advisory committees, continue review of rules and statutes in a systematic manner and develop recommendations for more comprehensive changes to align with modern business practices (e.g., eliminating paper dependencies).	In Progress	• In collaboration with CSCAC's Unlimited Case and Complex Litigation Subcommittee, ITAC's Rules and Policy Subcommittee, reviewed and considered comments and staff analysis for rules proposals (effective January 2018):
		  • Rules 2.250-2.259: The rules proposal makes amendments to trial court electronic filing and service rules in the California Rules of Court. The rule amendments would reduce redundancies and improve consistency between electronic filing and service provisions of California Rules of Court and the Code of Civil Procedure. The proposal also includes amendments to make limited organizational changes to the rules to improve their logical ordering.
		And legislative proposal (effective January 2019):
		  • Legislative Proposal for Electronic Service: The proposal amends the Civil Code and Code of Civil Procedure. The purpose of the amendments is to provide clarity about and foster the use of electronic service. The proposed amendments authorize electronic service for certain demands and notices consistent with Code of Civil Procedure sections 1010.6 and 1013b (section 1013b will be a new provision of the Code of Civil Procedure and it codifies proof of electronic service provisions currently found in the Rules of Court). The proposal also clarifies that the broader term "service" is applicable rather than "mailing" in certain code sections consistent with Judicial Council-sponsored legislation related to those sections.
		• The subcommittees agreed with staff analysis and recommendations. The subcommittees voted to approve the legislative proposal for ITAC and CSCAC's consideration. Because of pending legislation (AB 976) that may impact the rules proposal, the subcommittees are holding on the rules proposal until the outcome of the legislation is known.

Note: Projects include rule proposals to amend rules to conform to Judicial Council-sponsored legislation to be introduced in 2017. For example, if the legislation is enacted, the rules on e-filing and e-service (Cal. Rules of Court, rule 2.250-2.275) to be amended by January 1, 2018 to replace the current "close of business" provisions in the rules. Additional codes sections that would benefit from review and amendments to modernizing them include Code Civ. Proc. § 405.23, 594, 680.010-724.260; Civ. Code § 1719; Gov. Code § 915.2; and Labor Code § 3082.

Status Update

9. Standards, Rules and/or Legislation for E-Signatures

Highlight: New rules on electronic signatures were circulated and are in review; new members of a CEAC subcommittee have been appointed to work on developing standards.

Major Tasks	Status	Description
(a) Develop rule proposal to amend Code of Civil Procedure section 1010.6(b)(2) and Cal. Rules of Court, rule 2.257, to authorize electronic signatures on documents filed by the parties and attorneys.	In Progress	Legislation is pending that will amend Code of Civil Procedure section 1010.6 on electronic signatures on documents filed into the courts. Conforming changes to the rules of court have been circulated for public comment and are under review.
(b) CEAC Records Management Subcommittee to develop standards governing electronic signatures for documents filed into the court to be included in the "Trial Court Records Manual" with input from the Court Information Technology Managers Forum (CIOs). Rules & Policy Subcommittee to review.	Starting	New members have been appointed to the CEAC Records Management Subcommittee that will be developing standards for electronic signatures on documents filed into the courts.

Status Update

10. Rules for Remote Access to Records for Justice Partners

Highlight: A Joint Ad Hoc Subcommittee has been approved and is being formed to implement this project.

Major Tasks	Status	Description
(a) In collaboration with the Criminal Law Advisory Committee, amend trial court rules to facilitate remote access to trial court records by state and local justice partners, parties, and their attorneys.	In Progress	The Judicial Council oversight committees for several advisory committees have (1) approved the amendment of the committees' Annual Agendas to include this rules project, and (2) the formation of an ad hoc joint subcommittee to develop the rules on remote access to court records by parties, their attorneys, and justice partners. The membership of the joint subcommittee is being finalized and the subcommittee will meet soon. The goal of this project is to develop a set of rules to be adopted by the Judicial Council by January 1, 2019.

Status Update

11. Standards for Electronic Court Records as Data

Highlight: Members of CEAC Records Management Subcommittee have been appointed and will start working on this project.

Major Tasks	Status	Description
(a) CEAC Records Management Subcommittee -- in collaboration with the Data Exchange Workstream governance body (TBD) -- to develop standards and proposal to allow trial courts to maintain electronic court records as data in their case management systems to be included in the *Trial Court Records Manual* with input from the Court Information Technology Managers Forum (CITMF). Rules & Policy Subcommittee to review.	Starting	New members have been appointed to serve on the CEAC Records Management Subcommittee. During the coming year, the subcommittee will review the section in the *Trial Court Records Manual* on creating and maintaining records in electronic format; and will develop new provisions relating to creating and maintaining records in the form of data.
(b) Determine what statutory and rule changes may be required to authorize and implement the mainentance of records in the form of data; develop proposals to satisfy these changes.	Starting	Same as above.

Status Update

12. Rules for E-Filing

Highlight: Refer to Project #8

Major Tasks	Status	Description
(a) Evaluate current e-filing laws, rules, and amendments. Projects may include reviewing statutes and rules governing Electronic Filing Service Providers (EFSP) and filing deadlines.	In Progress	Ongoing.
(b) Develop rule proposals to implement the legislative proposal developed in 2016, which amends e-filing laws and rules (Code of Civil Procedure section 1010.6 and California Rules of Court, rule 2.250 et seq.).	In Progress	Refer to Project #8.
Note: This effort will be informed by the E-Filing and SRL E-Services Workstreams, and the CMS Data Exchange governance body (TBD) for any additional rules development needed.		

Status Update

13. Privacy Policy (Privacy Resource Guide)

Co-sponsored by the Rules & Policy and Joint Appellate Technology Subcommittees

Highlight: The overall framework and partial draft text of a Privacy Resource Guide (PRG) have been prepared during this period.

Major Tasks	Status	Description
(a) Continue development of a comprehensive statewide privacy policy addressing electronic access to court records and data to align with both state and federal requirements.	In Progress	During April-June, Judge Julie R. Culver and staff have been preparing a draft Privacy Resource Guide that will assist the branch in addressing privacy issues; this preliminary draft will be presented to the committee.
(b) Continue development of a model (local) court privacy policy, outlining the key contents and provisions to address within a local court's specific policy.	In Progress	The Privacy Resource Guide will include a section on best privacy practices for local courts and model templates for them to use; this section has been outlined but has not yet been drafted.

Profile

14 – 15. Joint Appellate Subcommittee Projects

Summary	*Various Projects, refer to following slides*	
ITAC Resource	Joint Appellate Technology Subcommittee	
Sponsor(s) or Chair(s)	Hon. Louis R. Mauro	PM: N/A
JCC Resources	Legal Services (assignment pending), JCIT (Julie Bagoye)	
Project Authorized	☒ Yes. Approved in 2017 Annual Agenda (1/9/2017).	
Membership Est'd	☒ Joint Appellate Technology Subcommittee	
Active	☒ Yes, meeting ad-hoc.	
Expected Outcomes	1. Recommendations, as needed	
Expected Completion	Ongoing (availability as issues arise)	

Status Update

14. Modernize Rules for the Appellate Courts

Highlight: Reviewed rule amendments relating to format for electronic reporter's transcripts.

Major Tasks	Status	Description
(a) In collaboration with other advisory committees, continue review of rules and statues in a systematic manner and develop recommendations for more comprehensive changes to align with modern business practices (e.g., eliminating paper dependencies).	In Progress	JATS reviewed a proposal from the Appellate Advisory Committee for amendments to the rules on the format of the record in appellate proceedings that would address the format for electronic court reporter's transcripts.
Note: Projects may include the appellate rules regarding format and handling of records filed electronically in the appellate courts.		

15. Consult on Appellate Court Technological Issues

Highlight: Reviewed legislative proposal regarding fees for electronic filing in appellate courts.

Major Tasks	Status	Description
(a) The Joint Appellate Technology Subcommittee (JATS) will provide input on request on technology related proposals considered by other advisory bodies as to how those proposals may affect, or involve, the appellate courts. JATS will consult on appellate court technology aspects of issues, as requested.	In Progress	JATS reviewed a proposal from the Administrative Presiding Justices Advisory Committee to amend the Government Code sections relating to appellate court fees to: (1) clarify that an appellate court's electronic filing service provider may charge a reasonable fee for its services, (2) allow an appellate court to contract with its electronic filing service provider to receive a portion of the fees collected by that provider, and (3) authorize the appellate courts to charge a fee to recover costs incurred for providing electronic filing.

Technology Innovations Grants by Category

#	Court	Program Name	Category	Amount
49	Orange Superior Court	**Improving Court Management Through the Use of Analytics** Establish an interactive, real-time data dashboard with relevant case information from a variety of data systems.	Analytics/Dashboard	$938,851.34
32	Santa Barbara Superior Court	**Instant Family Law Orders** Enhance the way a copy of the court's orders after a hearing are produced by integrating a Microsoft Surface Pro tablet with the court's case management system to produce an order after the hearing within minutes of the conclusion of the court's proceedings.	Automate manual process	$312,926.00
39	5th District Court of Appeal	**Modernize the Transcript Assembly Program** Enhance the current Transcript Assembly Program software being utilized in the majority of trial courts within the 5th District Court of Appeal to automate the manual staff process.	Automate manual process	$793,000.00
21	Los Angeles Superior Court	**Self-help Traffic Avatar (Gina) Expansion** Establish a self-help traffic avatar in both Monterey and Merced Superior Courts to assist customers with paying tickets, scheduling court dates, and registering for traffic school.	Avatar	$59,373.00
27	Riverside Superior Court	**Traffic Avatar** Establish an interactive virtual avatar that will assist online customers with traffic related inquiries.	Avatar	$67,124.93
38	Yolo Superior Court	**Online Interactive Multilingual Tool** Establish an online interactive multilingual tool (avatar) for Small Claims, Unlawful Detainer and Traffic cases.	Avatar	$91,500.00

Technology Innovations Grants by Category

#	Court	Program Name	Category	Amount
9	Sacramento Superior Court	**Monitor and Measure the Achievement of Program Goals** Enhance the existing collaborative courts by increasing its capacity to monitor and measure the achievement of program goals and effectiveness by inputting data into a case management system designed specifically for collaborative courts, developing data collection tools and protocols, and developing and issuing dashboard reports.	Collaborative Courts Analytics/Dashboard	$311,849.00
1	Alameda Superior Court	**Collaborative Court Management Information System** Enhance the existing management information system for use across collaborative court programs to better promote collaborative justice principles through more effective program analysis and evaluation.	Collaborative Courts CMS	$114,223.00
15	Sonoma Superior Court	**Veterans Court Enhancements** Enhance the existing Veterans Court by increasing the current caseload, creating of program materials, expanding treatment services, creating a greater website presence, improving overall case management and coordination, and developing a participant tracking system.	Collaborative Courts CMS	$56,476.00
46	Orange Superior Court	**Automating the Courtroom Check-in** Establish an application to automate the courtroom check-in process and the payment of trial court fees utilizing a Customer Relationship Management platform to save and track customer information and incorporate mobile technology with functionality to send text reminders to litigants and attorneys.	CRM & Mobile App	$246,190.00
45	Monterey Superior Court	**Cloud Based Disaster Recovery Solution** Establish a cost-effective and resilient solution for a timely recovery of vital network and computer systems necessary for business continuity and restoring essential court functions and services to the public.	Disaster Recovery	$209,361.00

Technology Innovations Grants by Category

#	Court	Program Name	Category	Amount
42	Los Angeles Superior Court	**E-filing Technical Capabilities** Establish Identity Management which ensures secure and consistent access to digital services across providers, and affordable financial gateways to lower the overall costs of digital commerce that all Electronic Filing Managers and Electronic Filing Service Providers will need to leverage to ensure e-filers have a consistent and cost-effective e-filing experience.	Identify Management /Payment Gateway	$114,760.00
22	Monterey Superior Court	**California Court Access App** Establish and deploy a mobile application for smartphones and devices, advanced online access, and a cloud-hosted solution to serve as a remote Clerk's Office available to court users around the clock.	Mobile App	$789,940.00
25	Riverside Superior Court	**Attorney and Litigant Electronic Courtroom Self Check-in** Establish a wireless proximity sensor technology outside each courtroom to enable attorneys and litigants to electronically "touch and check-in to" the courtroom and receive a "check-in alert," all by using their smartphone.	Mobile App	$179,250.67
53	Santa Cruz Superior Court	**SMS Notifications** Establish a solution that interfaces with the court jury system and the case management system to provide SMS notifications to court users and jurors in Santa Cruz County.	Mobile App	$35,760.00
52	San Mateo Superior Court	**Automated Line Queuing System** Establish an automated queuing management system to triage requests for services at the court clerk windows, plan and assign staffing to meet that demand, and to relieve congestion in the clerk offices.	Queuing	$125,000.00
34	Sonoma Superior Court	**Queuing/Appointment/Calendaring System** Establish a new queuing system to include appointments, remote check-in, and email and/or text message (SMS) notifications.	Queuing/Mobile App	$56,586.00

Technology Innovations Grants by Category

#	Court	Program Name	Category	Amount
17	5th District Court of Appeal	**Self-help and Learning Center Website** Establish a self-help and learning center website that would include Judicial Council approved fillable forms, virtual assistance and interviews to assist with forms and document completion, interactive learning, and you-tube instructional videos for self-represented litigants or attorneys unfamiliar with the appellate process.	Self Help Portal	$317,916
19	Contra Costa Superior Court	**California's Virtual Self-help Site** Enhance the current California Virtual Self Help Site by adding animated or virtual help/assistance in four languages, incorporating a "My Case Tracker" portal into the site, Self-Represented Litigant assisted electronic filing and education, and case management system integration.	Self Help Portal	$970,365
23	Orange Superior Court	**Enhance Self-help Portal** Enhance the current Self-help Portal by installing self-check-in kiosks, build and implement a mobile application for cell phones and tablets, integrate the Self-help Portal with the Court's case management system, and purchase hardware to help court users navigate through the court facilities.	Self Help Portal	$326,800.00
26	Riverside Superior Court	**Intelligent Self-help Kiosk** Establish intelligent kiosk systems at all courthouses that will give customers information and direct them to court offices to eliminate the need to wait in line for that same information.	Self Help Portal	$629,292.70
28	San Bernardino Superior Court	**Customer Relationship Management Portal** Establish a Customer Relationship Management Portal to help self-represented litigants access general legal and procedural information about their case type and available options, complete and submit forms for review prior to filing, communicate with self-help staff, register for workshops, and track the status of their active case(s).	Self Help Portal	$430,755.51

Technology Innovations Grants by Category

#	Court	Program Name	Category	Amount
30	San Diego Superior Court	**Access to Information Made Simple** Establish a video appointment system and electronic message board to assist litigants with understanding procedures, completing paperwork, and generally navigating the family court process in a simple and convenient manner.	Self Help Portal	$276,320.00
31	San Mateo Superior Court	**Develop and Provide Expanded Online Self-help** Enhance the court's self-help services by adding on-site and countywide kiosks/workstations, online "live-chat" and "inquiry chat" technology, and updated web-based video and written content for Family Law, Domestic Violence, Guardianships, Conservatorships, and Small Claims.	Self Help Portal	$336,000.00
43	Los Angeles Superior Court	**Justice System Partner and Litigant Portal** Establish a court case access portal that will enable access to certain case data and documents through queries for justice partners and litigants in seven counties (Contra Costa, Los Angeles, Monterey, Orange, San Diego, Santa Clara, and Orange).	Self Help Portal	$637,500.00
47	Orange Superior Court	**Conservatorship Accountability Portal** Enhance the conservatorship accounting process, improve the court's ability to protect assets, and to allow a simplified accounting report process for conservators, guardians, and fiduciaries.	Self Help Portal	$212,972.00
48	Orange Superior Court	**Court User Portal** Establish a new website to serve as a court user portal to allow the public to register for phone/text reminders, submit electronic correspondence to the court, make payments, and view case information.	Self Help Portal	$511,200.00
18	Butte Superior Court	**Remote Video Conferencing Technology** Establish the use of remote video conferencing technology to 13 rural courts (Butte, Glenn, Humboldt, Inyo, Imperial, Lake, Modoc, Nevada, Placer, Shasta, Siskiyou, Tehama, and Trinity) and ensure each court has adequate bandwidth and technological infrastructure to support a self-help program	Video Conferencing	$576,140.00

Technology Innovations Grants by Category

#	Court	Program Name	Category	Amount
		that can be used collaboratively by sharing self-help resources between participating courts.		
29	San Bernardino Superior Court	**Video Conferencing Child Custody Recommending Counseling** Establish Video Conferencing Child Custody Recommending Counseling at three courthouses (San Bernardino, Victorville, and Joshua Tree) to enable all parties to see one another and communicate more effectively through verbal and body language interactions.	Video Conferencing	$35,537.60
36	Ventura Superior Court	**Internet Based Self-help Workshops** Enhance self-help services by offering live, interactive video workshops with groups of up to 25 self-represented litigants on the topics of Dissolution/Legal Separation/Nullities and Request for Orders in Family Law matters, as well as Civil Harassment Restraining Orders, Guardianships and Unlawful Detainers.	Video Conferencing	$932,404.00
8/24[1]	Placer Superior Court	**Video Appearances** Develop a central solution for video appearances across functional areas in the court by installing video conferencing hardware and software in 14 courtrooms and two administrative locations.	Video Hearings	$560,000.00
41	Humboldt Superior Court	**Interactive Video Conferencing System** Establish an interactive video conferencing system to conduct hearings required by the Lanterman-Petris-Short Act in order to reduce undue stress on patients, as well as reduce public safety risks associated with patient transport.	Video Hearings	$170,919.87

Technology Innovations Grants by Category

#	Court	Program Name	Category	Amount
44	Merced Superior Court	**Video Conference Hearings Project** Establish video conferencing equipment in four courtrooms to help streamline the justice process for both criminal defendants and civil respondents by implementing video hearings for preliminary hearings and civil cases with the judge hearing cases located at the Merced Courthouse and the defendant or respondent located in a courtroom at the Los Banos Courthouse.	Video Hearings	$194,540.00
50	Sacramento Superior Court	**Video Conferencing of Mental Health Hearings** Establish video conferencing to conduct mental health hearings, including petitions for writs of habeas corpus, for Riese medication capacity determination, and for time extensions.	Video Hearings	$52,860.00
51	San Bernardino Superior Court	**Remote Video Proceedings** Establish video hearings within the city of Big Bear Lake for traffic infraction arraignments and misdemeanor probation modification matters from the Big Bear jurisdiction.	Video Hearings	$244,698.58

[1] Split funding between Collaborative Courts and Self-help, Family and Juvenile Courts

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date
May 24, 2017

To
Information Technology Advisory Committee
and
Civil and Small Claims Advisory Committee

From
Information Technology Advisory Committee, Rules and Policy Subcommittee
and
Civil and Small Claims Advisory Committee, Unlimited Case and Complex Litigation Subcommittee

Subject
Legislative Proposal (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a)

Action Requested
Please review

Deadline
June 9, 2017

Contact
Andrea L. Jaramillo
916-263-0991 phone
andrea.jaramillo@jud.ca.gov

Background

This spring, the Information Technology Advisory Committee (ITAC) circulated for public comment a legislative proposal that would amend section 1719 of the Civil Code and sections 405.22, 405.23, 594, 659, 660, and 663a of the Code of Civil Procedure. Specifically, this legislative proposal would (1) authorize the courts to electronically serve a written demand for payment on the drawer of a bad check when the court is the payee of the check and the drawer of the check is accepting electronic service in the matter to which the check pertains; (2) authorize a party asserting a real property claim to electronically serve a notice of pendency of the action on

other parties or owners when those parties or owners are already accepting electronic service in the action; (3) authorize electronic service of notices of intention to move for a new trial or vacate judgment; and (4) amend certain deadlines tied to dates of "mailing" to be tied instead to dates of "service." The proposal originates from ITAC's modernization project to amend statutes and California Rules of Court to facilitate electronic filing and service and to foster modern e-business practices.

Four commenters submitted specific comments in response to the Invitation to Comment. To facilitate the committees' review of the comments and discussion, the attached materials include the proposed amendments with drafter's notes immediately following each proposed amendment that received public comment. The drafter's notes list the specific comments received in response to the proposal, and are followed by analysis from staff.

On May 23, 2017, ITAC's Rules and Policy Subcommittee and the Civil and Small Claims Advisory Committee's (CSCAC) Unlimited Case and Complex Subcommittee held a joint meeting to review the comments received and staff analysis of those comments. The subcommittees agreed with the staff analysis and recommendations, and voted to recommend ITAC and CSCAC consider the proposal for Judicial Council sponsorship. Based on the subcommittees' remarks and vote, the staff have updated the comment chart with proposed committee responses.

Recommendation

1. Recommend that the Judicial Council approve the proposal as circulated except with a nonsubstantive modification to Civil Code section 1719(g)(2).[1]

2. Approve the proposed committee responses in the comment chart.

Attachments
1. Text of proposed amendments to Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a with drafter's notes.
2. Comment chart.

[1] A detailed explanation for the recommendation is in the staff analysis immediately following Civil Code section 1719(g)(2) in the attached text of the proposal.

Section 1719 of the Civil Code and sections 405.22, 405.23, 594, 659, 660, and 663a of the Code of Civil Procedure would be amended, effective January 1, 2019, to read:

Civil Code, § 1719.

(a)(1) Notwithstanding any penal sanctions that may apply, any person who passes a check on insufficient funds shall be liable to the payee for the amount of the check and a service charge payable to the payee for an amount not to exceed twenty-five dollars ($25) for the first check passed on insufficient funds and an amount not to exceed thirty-five dollars ($35) for each subsequent check to that payee passed on insufficient funds.

(2) Notwithstanding any penal sanctions that may apply, any person who passes a check on insufficient funds shall be liable to the payee for damages equal to treble the amount of the check if a written demand for payment is mailed by certified mail to the person who had passed a check on insufficient funds and the written demand informs this person of (A) the provisions of this section, (B) the amount of the check, and (C) the amount of the service charge payable to the payee. The person who had passed a check on insufficient funds shall have 30 days from the date the written demand was mailed to pay the amount of the check, the amount of the service charge payable to the payee, and the costs to mail the written demand for payment. If this person fails to pay in full the amount of the check, the service charge payable to the payee, and the costs to mail the written demand within this period, this person shall then be liable instead for the amount of the check, minus any partial payments made toward the amount of the check or the service charge within 30 days of the written demand, and damages equal to treble that amount, which shall not be less than one hundred dollars ($100) nor more than one thousand five hundred dollars ($1,500). When a person becomes liable for treble damages for a check that is the subject of a written demand, that person shall no longer be liable for any service charge for that check and any costs to mail the written demand.

(3) Notwithstanding paragraphs (1) and (2), a person shall not be liable for the service charge, costs to mail the written demand, or treble damages if he or she stops payment in order to resolve a good faith dispute with the payee. The payee is entitled to the service charge, costs to mail the written demand, or treble damages only upon proving by clear and convincing evidence that there was no good faith dispute, as defined in subdivision (b).

(4) Notwithstanding paragraph (1), a person shall not be liable under that paragraph for the service charge if, at any time, he or she presents the payee with written confirmation by his or her financial institution that the check was returned to the payee by the financial institution due to an error on the part of the financial institution.

(5) Notwithstanding paragraph (1), a person shall not be liable under that paragraph for the service charge if the person presents the payee with written confirmation that his or her account had insufficient funds as a result of a delay in the regularly scheduled transfer of, or the posting of, a direct deposit of a social security or government benefit assistance payment.

(6) As used in this subdivision, to "pass a check on insufficient funds" means to make, utter, draw, or deliver any check, draft, or order for the payment of money upon any bank, depository, person, firm, or corporation that refuses to honor the check, draft, or order for any of the following reasons:

(A) Lack of funds or credit in the account to pay the check.

(B) The person who wrote the check does not have an account with the drawee.

(C) The person who wrote the check instructed the drawee to stop payment on the check.

(b)–(c) * * *

(d) In the case of a stop payment, a court may not award damages or costs under this section unless the court receives into evidence a copy of the written demand that, in that case, shall have been sent to the drawer and a signed certified mail receipt showing delivery, or attempted delivery if refused, of the written demand to the drawer's last known address.

(e)–(f) * * *

(g)(1) Notwithstanding subdivision (a), if the payee is the court, the written demand for payment described in subdivision (a) may be mailed to the drawer by the court clerk. Notwithstanding subdivision (d), in the case of a stop payment where the demand is mailed by the court clerk, a court may not award damages or costs pursuant to subdivision (d), unless the court receives into evidence a copy of the written demand, and a certificate of mailing by the court clerk in the form provided for in subdivision (4) of Section 1013a of the Code of Civil Procedure for service in civil actions.

Drafter's Note: *The following was the version circulated for comment.*

(2) In lieu of the mailing provisions of (g)(1), if the payee is the court and the check passed on insufficient funds relates to an action in which the drawer has consented to accept or is required to accept electronic service pursuant to Section 1010.6 of the Code of Civil Procedure, the court clerk may serve the written demand electronically. Notwithstanding subdivision (d), in the case of a stop payment where the demand is electronically served by the court clerk, a court may not award damages or costs pursuant to subdivision (d) unless the court receives into evidence a copy of the written demand, and a certificate of electronic service by the court clerk in the form provided for in subdivision (4) of Section 1013a of the Code of Civil Procedure as modified for electronic service in accordance with Section 1013b of the Code of Civil Procedure.

Drafter's Note: *The following is the non-substantive, technical revision recommended by staff. Staff make this recommendation because in Assembly Bill (AB) 976, the Legislature has revised the wording of proposed Code of Civil Procedure section 1013b, which will be the new code section covering proof of electronic service. The Legislature's revisions were nonsubstantive and improved the clarity of the section. Staff do not anticipate further changes to section 1013b as it was not controversial in the Assembly, but if there are additional changes, staff will alert the subcommittees and committees. There would be adequate time to address the changes before legislative proposals go to the Judicial Council in November.*

(2) In lieu of the mailing provisions of (g)(1), if the payee is the court and the check passed on insufficient funds relates to an action in which the drawer has consented to accept or is required to accept electronic service pursuant to Section 1010.6 of the Code of Civil Procedure, the court clerk may serve the written demand electronically. Notwithstanding subdivision (d), in the case of a stop payment where the demand is electronically served by the court clerk, a court may not award damages or costs pursuant to subdivision (d) unless the court receives into evidence a copy of the written demand, and a certificate of electronic service by the court clerk in the form provided for in subdivision (a)(4) of Section 1013b of the Code of Civil Procedure.

Drafter's Note: *The following comments were received in response to the proposed amendments, as circulated, to Civil Code section 1719(g)(2):*

- Orange County Bar Association. "Agree as Modified - As to the proposed changes to CC section 1719, the following modifications are suggested.

  With very limited exception, parties who have agreed to accept, or who are required to accept, electronic service of documents pursuant to the provisions of CCP section 1010.6, are represented by counsel. For these parties, the email address on file with the court is that of their respective counsel and not that of the actual party. Consequently, a drawer of a check may appear to be a party subject to electronic service in the underlying action, but whose personal email is not the one in the court records. While there is no disagreement with the idea behind the proposal, it is suggested that the proposed language adding subsection (2) to CC section 1719(g) be modified in some manner to ensure that the drawer's personal email address is used and that permission for its use by the court is obtained. To do anything less would result in an insufficient and failed demand under CC section 1719(g)."

Staff analysis: The purpose of the new Civil Code section 1719(g)(2) is to ensure that it is not inconsistent with Code of Civil Procedure section 1010.6, which

allows the courts to "electronically serve any document issued by the court" that does not have to be personally served. (Code Civ. Proc, § 1010.6(a)(3).) Staff disagree with the Orange County Bar Association that using the electronic service address where the drawer of the check is accepting electronic service in the underlying action would "result in an insufficient and failed demand." Where the drawer is accepting electronic service through counsel, counsel would have a professional obligation to the drawer as the client to alert them about the demand.

(3) For purposes of this subdivision, in courts where a single court clerk serves more than one court, the clerk shall be deemed the court clerk of each court.

(h)–(k) * * *

Code of Civil Procedure, § 405.22.

(a) Except in actions subject to Section 405.6, the claimant shall, prior to recordation of the notice, cause a copy of the notice to be mailed, by registered or certified mail, return receipt requested, to all known addresses of the parties to whom the real property claim is adverse and to all owners of record of the real property affected by the real property claim as shown by the latest county assessment roll. If there is no known address for service on an adverse party or owner, then as to that party or owner a declaration under penalty of perjury to that effect may be recorded instead of the proof of service required above, and the service on that party or owner shall not be required. Immediately following recordation, a copy of the notice shall also be filed with the court in which the action is pending. Service shall also be made immediately and in the same manner upon each adverse party later joined in the action.

(b) In lieu of the mailing provisions of (a), a claimant may serve the notice electronically in accordance with Section 1010.6 upon the parties to whom the real property claim is adverse and the owners of record provided that the parties to whom the real property claim is adverse and the owners of record have consented to accept or are required to accept electronic service pursuant to Section 1010.6 in the action to which the notice pertains.

Code of Civil Procedure, § 405.23.

Any notice of pendency of action shall be void and invalid as to any adverse party or owner of record unless the requirements of Section 405.22 are met for that party or owner and a proof of service in the form and content specified in Section 1013a for service by mail or Section 1013b for electronic service has been recorded with the notice of pendency of action.

Drafter's Note: *The following comments were received in response to the proposed amendments to Code of Civil Procedure sections 405.22 and 405.23:*

- Orange County Bar Association. "Disagree – As to the proposed changes to CCP sections 405.22 and 405.23, the following observations are made.

  As a practical matter, it is difficult to see how allowing the service electronically of a notice of pendency of action would be of real benefit. At the time a plaintiff, for example, would want to serve the notice, it would seem unlikely that an adverse party even if required to be served electronically, would have responded so as to have its electronic contact information on file. In that all affected owners of record also must be served notice, it would seem even more unlikely that their respective electronic contact information or consent would be known to the plaintiff. Finally, in that service must be made "immediately" upon each adverse party later joined per CCP section 405.22, it would seem most unlikely their electronic contact information would have been provided. For these reasons, based on the timing considerations involved, the likelihood exists that most if not all of these notices would still be served by mail.

  Beyond the practical considerations, there are differences in the very nature of a notice of pendency of action which set it apart from a pleading, for example. These differences are not just rooted in tradition, but in actual distinction. The use and impact of these notices is serious which is, perhaps, the reason for the heightened requirements associated with their service (these heightened requirements would be lost, of course, were electronic service allowed). Pleadings simply may be mailed, but these notices must be sent registered or certified mail, return receipt requested. Both of these methods allow for tracking and evidence of receipt. Pleadings are filed with the court, while notices are recorded with the county recorder, and require a notary's seal and acknowledgment. Pleading and notices are both public records, but the notice appears in the chain of title giving constructive notice to all who come after. In short, a notice of pendency of action is surrounded by unique considerations, and it should not be equated with, treated like, or served in the manner of a subsequent pleading."

Staff analysis: Regarding the Orange County Bar Association's comment that there is a lack of real benefit as a practical matter. Electronic service of notice of pendency would only apply to a narrow subset of litigants (those that are accepting electronic service in the underlying matter and have not been served a notice of pendency by mail). The service of the notice is a prerequisite to

recordation and it is not clear to staff why mailing should be required as applied to that subset of litigants. Staff disagree that electronic service of the notice causes something about the seriousness of the process to be lost. First, sending certified mail creates a written record of transmission from the United States Postal Service (USPS). Evidence of mailing is essentially officially corroborated by USPS. Similarly, electronic service creates a record of transmission where the technology itself provides a written record to corroborate the sender's claim that they indeed sent the material to the place where the recipient has represented to the court that the recipient can be reached. Second, regarding evidence of receipt, such evidence is not a prerequisite to recordation. The sender using mail must request a return receipt, but the recipient does not actually have to send it back nor does the sender have to have the return receipt to record the notice. While staff disagree with some of the Orange County Bar Association's point, staff recognize that the Orange County Bar Association membership may have more practical experience in this area of law that should be given weight in determining whether to proceed with the notice of pendency provisions in this proposal. In addition, it would potentially create surplusage in the Code of Civil Procedure if, indeed, there is no practical utility to be accomplished in allowing electronic service of a notice of pendency.

In addition to the concerns raised by the Orange County Bar Association, there is a policy consideration depending on the outcome of AB 976. In the current iteration of AB 976, the Assembly has added a provision that would add the following to Code of Civil Procedure section 1010.6. "If a document is required to be served by certified or registered mail, electronic service of the document is not authorized." Similarly, AB 976 adds the following to Code of Civil Procedure section 1020, "Electronic service is not authorized for a notice that requires certified or registered mail." The Senate has not yet considered these provisions. If these provisions are enacted, the Legislature will have expressly manifested its intent to disallow electronic service when registered or certified mail is required. If those provisions remain and the committees believe it would be best to proceed to carve out an exception for a notice of pendency, staff could develop language to add to the proposal to ensure the intent to allow electronic service remains. Such language would be something like, "Notwithstanding the provisions of Code of Civil Procedure sections 1010.6(a)(2)(B) and 1020(b). . . ." Staff will keep the subcommittees and committees informed about the status of AB 976. There would be adequate time to address provisions of AB 976 before legislative proposals go to the Judicial Council in November.

Code of Civil Procedure, § 594.

(a) In superior courts either party may bring an issue to trial or to a hearing, and, in the absence of the adverse party, unless the court, for good cause, otherwise directs, may

proceed with the case and take a dismissal of the action, or a verdict, or judgment, as the case may require; provided, however, if the issue to be tried is an issue of fact, proof shall first be made to the satisfaction of the court that the adverse party has had 15 days' notice of such trial or five days' notice of the trial in an unlawful detainer action as specified in subdivision (b). If the adverse party has served notice of trial upon the party seeking the dismissal, verdict, or judgment at least five days prior to the trial, the adverse party shall be deemed to have had notice.

(b) The notice to the adverse party required by subdivision (a) shall be served electronically in accordance with Section 1010.6 or by mail on all the parties by the clerk of the court not less than 20 days prior to the date set for trial. In an unlawful detainer action where notice is served electronically in accordance with Section 1010.6 or by mail, that service shall be electronically served or mailed not less than 10 days prior to the date set for trial. If notice is not served by the clerk as required by this subdivision, it may be served electronically in accordance with Section 1010.6 or by mail by any party on the adverse party not less than 15 days prior to the date set for trial, and in an unlawful detainer action where notice is served electronically in accordance with Section 1010.6 or by mail, that service shall be electronically served or mailed not less than 10 days prior to the date set for trial. The time provisions of Section 1010.6 and Section 1013 shall not serve to extend the notice of trial requirements under this subdivision for unlawful detainer actions. If notice is served by the clerk, proof thereof may be made by introduction into evidence of the clerk's certificate pursuant to subdivision (3) of Section 1013a, compliance with Section 1013b when service is electronic, or other competent evidence. If notice is served by a party, proof may be made by introduction into evidence of an affidavit or certificate pursuant to subdivision (1) or (2) of Section 1013a, compliance with Section 1013b when service is electronic, or other competent evidence. The provisions of this subdivision are exclusive.

Drafter's Note: *The following comments were received in response to the proposed amendments to Code of Civil Procedure section 594:*

- Superior Court of Los Angeles County. "Code of Civil Procedure § 594(b)

  Page 9, lines 1 through 3 - In order to clarify that the 20 day provision only applies to service by mail, not electronic service, change:

  "…shall be served electronically in accordance with Section 1010.6 or by mail on all parties by the clerk of the court not less than 20 days prior to the date set for trial."

  to

"…shall be served by mail on all parties by the clerk of the court not less than 20 days prior to the date set for trial or electronically in accordance with Section 1010.6."

Staff analysis: There was no intention to have separate time frames for mail and electronic service in Code of Civil Procedure section 594. Any differentiation in time frames would be found in Code of Civil Procedure sections 1010.6 and 1013. Accordingly, staff recommend against the modification in the comment.

- Aderant. "We have reviewed the Invitation to Comment LEG 17-05 and write to request that the proposed amendment to CCP 594(b) be further clarified with respect to the calculation of the 15 and 10-day deadlines for a party to serve notice provided therein.

  As proposed, CCP 594(b) states, in part:

  > If notice is not served by the clerk as required by this subdivision, it may be served electronically in accordance with Section 1010.6 or by mail by any party on the adverse party not less than 15 days prior to the date set for trial, and in an unlawful detainer action where notice is served electronically in accordance with Section 1010.6 or by mail, that service shall be electronically served or mailed not less than 10 days prior to the date set for trial. The time provisions of Section 1010.6 and Section 1013 shall not serve to extend the notice of trial requirements under this subdivision for unlawful detainer actions.

  CCP 1010.6(a)(4) says, "[A]ny period of notice, or any right or duty to do any act or make any response within any period or on a date certain after the service of the document, which time period or date is prescribed by statute or rule of court, shall be extended after service by electronic means by two court days. . . ."

  CCP 1013(a) provides, "[A]ny period of notice and any right or duty to do any act or make any response within any period or on a date certain after the service of the document, which time period or date is prescribed by statute or rule of court, shall be extended . . . 20 calendar days if either the place of mailing or the place of address is outside the United States. . . ."

  The statement that the time provisions in CCP 1010.6 and 1013 shall not "extend the notice of trial requirements under this subdivision for unlawful detainer actions," makes the calculation for non-unlawful detainer actions ambiguous, because it seems to imply that they *do* serve to extend the notice of trial requirements in those cases.

> For example, in a non-unlawful detainer actions, amended CCP 594(b) seems to require notice to be electronically served 15 days + 2 court days prior to the date of trial, pursuant to CCP 594(b) and CCP 1010.6. Similarly, notice served by mail outside of California and outside of the United States, would need to be served 20 and 30 days prior to the date of trial, respectively. Is this correct? Or should the deadline for service of notice in non-unlawful detainer actions served by either method simply be 15 days prior to trial?
>
> If the deadline is meant to be only 15 days before trial, we respectfully request that CCP 594(b) be further amended to eliminate the reference to unlawful detainer actions in the sentence regarding the time provisions of CCP 1010.6 and 1013: "The time provisions of Section 1010.6 and Section 1013 shall not serve to extend the notice of trial requirements under this subdivision ~~for unlawful detainer actions~~."
>
> If extra time under CCP 1010.6 and 1013 is meant to be added to the notice deadline, we respectfully request that CCP 594(b) be further amended to clarify this fact. For example, the time provision sentence could be changed to read, "Except for unlawful detainer actions, the time provisions of Section 1010.6 and Section 1013 shall serve to extend the notice of trial requirements under this subdivision."

Staff analysis: The purpose of the proposal is to allow electronic service of a notice of trial, not to remove special provisions applicable to unlawful detainer actions. The exemption from extensions of time under Code of Civil Procedure section 594(b) only applies to unlawful detainer actions. This is a specific carve-out from extensions of time that the Legislature added in 1977. (Stats.1977, ch. 1257, p. 4762, § 19.5.) Therefore, extensions of time provisions do apply to non-unlawful detainer actions. Accordingly, staff recommend that the committee retain "for unlawful detainer actions" rather than strike it out as suggested by the commenter.

Regarding, changing the language to "Except for language . . .", staff do not find it to add clarity to the existing language of section 594(b) and do not recommend altering the language of section 594(b) beyond the scope of the proposal to allow electronic service for a notice of trial.

Finally, unrelated to the comments, the proposed changes reference Code of Civil Procedure section 1013b, which is currently part of AB 976. Staff do not anticipate an issue with the passage of section 1013b as it was not controversial

in the Assembly, but if there are applicable changes to AB 976, staff will alert the subcommittees and committees.

Code of Civil Procedure, § 659.

(a) The party intending to move for a new trial shall file with the clerk and serve upon each adverse party a notice of his or her intention to move for a new trial, designating the grounds upon which the motion will be made and whether the same will be made upon affidavits or the minutes of the court, or both, either:

(1) After the decision is rendered and before the entry of judgment.

(2) Within 15 days of the date of ~~mailing~~ service of the notice of entry of judgment by the clerk of the court pursuant to Section 664.5, or service upon him or her by any party of written notice of entry of judgment, or within 180 days after the entry of judgment, whichever is earliest; provided, that upon the filing of the first notice of intention to move for a new trial by a party, each other party shall have 15 days after the service of that notice upon him or her to file and serve a notice of intention to move for a new trial.

(b) That notice of intention to move for a new trial shall be deemed to be a motion for a new trial on all the grounds stated in the notice. The times specified in paragraphs (1) and (2) of subdivision (a) shall not be extended by order, ~~or~~ stipulation, ~~or by~~ those provisions of Section 1013 that extend the time for exercising a right or doing an act where service is by mail~~.~~, or those provisions of Section 1010.6 that extend the time for exercising a right or doing an act where service is electronic.

Code of Civil Procedure, § 660.

On the hearing of such motion, reference may be had in all cases to the pleadings and orders of the court on file, and when the motion is made on the minutes, reference may also be had to any depositions and documentary evidence offered at the trial and to the report of the proceedings on the trial taken by the phonographic reporter, or to any certified transcript of such report or if there be no such report or certified transcript, to such proceedings occurring at the trial as are within the recollection of the judge; when the proceedings at the trial have been phonographically reported, but the reporter's notes have not been transcribed, the reporter must upon request of the court or either party, attend the hearing of the motion and shall read his notes, or such parts thereof as the court, or either party, may require.

The hearing and disposition of the motion for a new trial shall have precedence over all other matters except criminal cases, probate matters and cases actually on trial, and it shall be the duty of the court to determine the same at the earliest possible moment.

Except as otherwise provided in Section 12a of this code, the power of the court to rule on a motion for a new trial shall expire 60 days from and after the ~~mailing~~ service of the notice of entry of judgment by the clerk of the court pursuant to Section 664.5 or 60 days from and after service on the moving party by any party of written notice of the entry of the judgment, whichever is earlier, or if such notice has not theretofore been given, then 60 days after filing of the first notice of intention to move for a new trial. If such motion is not determined within said period of 60 days, or within said period as thus extended, the effect shall be a denial of the motion without further order of the court. A motion for a new trial is not determined within the meaning of this section until an order ruling on the motion (1) is entered in the permanent minutes of the court or (2) is signed by the judge and filed with the clerk. The entry of a new trial order in the permanent minutes of the court shall constitute a determination of the motion even though such minute order as entered expressly directs that a written order be prepared, signed and filed. The minute entry shall in all cases show the date on which the order actually is entered in the permanent minutes, but failure to comply with this direction shall not impair the validity or effectiveness of the order.

Code of Civil Procedure, § 663a.

(a) A party intending to make a motion to set aside and vacate a judgment, as described in Section 663, shall file with the clerk and serve upon the adverse party a notice of his or her intention, designating the grounds upon which the motion will be made, and specifying the particulars in which the legal basis for the decision is not consistent with or supported by the facts, or in which the judgment or decree is not consistent with the special verdict, either:

(1) After the decision is rendered and before the entry of judgment.

(2) Within 15 days of the date of ~~mailing~~ service of the notice of entry of judgment by the clerk of the court pursuant to Section 664.5, or service upon him or her by any party of written notice of entry of judgment, or within 180 days after the entry of judgment, whichever is earliest.

(b) Except as otherwise provided in Section 12a, the power of the court to rule on a motion to set aside and vacate a judgment shall expire 60 days from the ~~mailing~~ service of the notice of entry of judgment by the clerk of the court pursuant to Section 664.5, or 60 days after service upon the moving party by any party of written notice of entry of the judgment, whichever is earlier, or if that notice has not been given, then 60 days after filing of the first notice of intention to move to set aside and vacate the judgment. If that motion is not determined within the 60-day period, or within that period, as extended, the effect shall be a denial of the motion without further order of the court. A motion to set aside and vacate a judgment is not determined within the meaning of this section until an order ruling on the motion is (1) entered in the permanent minutes of the court, or (2)

signed by the judge and filed with the clerk. The entry of an order to set aside and vacate the judgment in the permanent minutes of the court shall constitute a determination of the motion even though that minute order, as entered, expressly directs that a written order be prepared, signed, and filed. The minute entry shall, in all cases, show the date on which the order actually is entered in the permanent minutes, but failure to comply with this direction shall not impair the validity or effectiveness of the order.

(c) The provisions of Section 1013 extending the time for exercising a right or doing an act where service is by mail and the provisions of Section 1010.6 extending the time for exercising a right or doing an act where service is electronic shall not apply to extend the times specified in paragraphs (1) and (2) of subdivision (a).

(d)–(e) * * *

Drafter's Note: *The following comments were received in response to the request in the Invitation to Comment for comments in response to the question, "Does the proposal appropriately address the stated purpose?"*

- Orange County Bar Association. "Yes, in light of the modernization project which seeks to "facilitate electronic filing and service and to foster modern e-business practices." It is believed, however, that the anticipated benefits of these efforts should be carefully weighed against certain implications and ramifications for litigants."

Staff analysis: No analysis needed.

Drafter's Note: *The following comments were received, but not tied specifically to one of the proposed legislative amendments or request for specific comments.*

- Mark W. Lomax. "C.C.P. section 411.20 requires the clerk to mail notice regarding a dishonored check for a filing fee, and C.C.P. section 411.21 requires the clerk to mail notice regarding partial payment of a filing fee. I recommend that both sections be amended to permit the notices to be served electronically or by postal mail."

Staff analysis: The comment is outside the scope of the proposal, but staff will incorporate the comment into a report that staff are developing for the Rules and Policy Subcommitee's consideration in the future on suggestions from the public.

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
1.	Aderant By Victoria Katz, Rules Attorney www.aderant.com Email: victoria.katz@aderant.com	NI	We have reviewed the Invitation to Comment LEG 17-05 and write to request that the proposed amendment to CCP 594(b) be further clarified with respect to the calculation of the 15 and 10-day deadlines for a party to serve notice provided therein. As proposed, CCP 594(b) states, in part: If notice is not served by the clerk as required by this subdivision, it may be served electronically in accordance with Section 1010.6 or by mail by any party on the adverse party not less than 15 days prior to the date set for trial, and in an unlawful detainer action where notice is served electronically in accordance with Section 1010.6 or by mail, that service shall be electronically served or mailed not less than 10 days prior to the date set for trial. The time provisions of Section 1010.6 and Section 1013 shall not serve to extend the notice of trial requirements under	The committees appreciate the comment, but the modification suggested in the comment goes beyond the scope of the proposal. The proposal adds electronic service as a mechanism to serve the notice of trial, but is not intended to alter statutory time frames applicable to specific case types.

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
			this subdivision for unlawful detainer actions. CCP 1010.6(a)(4) says, "[A]ny period of notice, or any right or duty to do any act or make any response within any period or on a date certain after the service of the document, which time period or date is prescribed by statute or rule of court, shall be extended after service by electronic means by two court days…." CCP 1013(a) provides, "[A]ny period of notice and any right or duty to do any act or make any response within any period or on a date certain after the service of the document, which time period or date is prescribed by statute or rule of court, shall be extended . . . 20 calendar days if either the place of mailing or the place of address is outside the United States…." The statement that the time provisions in CCP 1010.6 and 1013 shall not "extend the notice of trial requirements under this subdivision for unlawful detainer actions,"	

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
			makes the calculation for non-unlawful detainer actions ambiguous, because it seems to imply that they *do* serve to extend the notice of trial requirements in those cases. For example, in a non-unlawful detainer actions, amended CCP 594(b) seems to require notice to be electronically served 15 days + 2 court days prior to the date of trial, pursuant to CCP 594(b) and CCP 1010.6. Similarly, notice served by mail outside of California and outside of the United States, would need to be served 20 and 30 days prior to the date of trial, respectively. Is this correct? Or should the deadline for service of notice in non-unlawful detainer actions served by either method simply be 15 days prior to trial? If the deadline is meant to be only 15 days before trial, we respectfully request that CCP 594(b) be further amended to eliminate the reference to unlawful detainer actions in the sentence regarding the time provisions of CCP 1010.6 and 1013: "The time	

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
			provisions of Section 1010.6 and Section 1013 shall not serve to extend the notice of trial requirements under this subdivision ~~for unlawful detainer actions~~." If extra time under CCP 1010.6 and 1013 is meant to be added to the notice deadline, we respectfully request that CCP 594(b) be further amended to clarify this fact. For example, the time provision sentence could be changed to read, "Except for unlawful detainer actions, the time provisions of Section 1010.6 and Section 1013 shall serve to extend the notice of trial requirements under this subdivision."	
2.	Lomax, Mark W. Pasadena CA, Email: mlomax1074@gmail.com	AM	C.C.P. section 411.20 requires the clerk to mail notice regarding a dishonored check for a filing fee, and C.C.P. section 411.21 requires the clerk to mail notice regarding partial payment of a filing fee. I recommend that both sections be amended to permit the notices to be served electronically or by postal mail.	The committees appreciate the comment, but it is beyond the scope of this proposal. The committees may consider the suggestion as part of a future proposal.

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
3.	Orange County Bar Association By Michael L. Baroni, President P.O. Box 6130 Newport Beach, CA 92658	A, AM, N	Agree as Modified - As to the proposed changes to CC section 1719, the following modifications are suggested. With very limited exception, parties who have agreed to accept, or who are required to accept, electronic service of documents pursuant to the provisions of CCP section 1010.6, are represented by counsel. For these parties, the email address on file with the court is that of their respective counsel and not that of the actual party. Consequently, a drawer of a check may appear to be a party subject to electronic service in the underlying action, but whose personal email is not the one in the court records. While there is no disagreement with the idea behind the proposal, it is suggested that the proposed language adding subsection (2) to CC section 1719(g) be modified in some manner to ensure that the drawer's personal email address is used and that permission for its use by the court is obtained. To do anything less would result in an insufficient and failed demand under CC section 1719(g).	The committees appreciate the comment, but decline to alter the proposal. If the drawer's counsel receives the notice, that should be sufficient in light of professional ethical obligations that counsel would owe the drawer as client.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated.

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
			Disagree – As to the proposed changes to CCP sections 405.22 and 405.23, the following observations are made. As a practical matter, it is difficult to see how allowing the service electronically of a notice of pendency of action would be of real benefit. At the time a plaintiff, for example, would want to serve the notice, it would seem unlikely that an adverse party even if required to be served electronically, would have responded so as to have its electronic contact information on file. In that all affected owners of record also must be served notice, it would seem even more unlikely that their respective electronic contact information or consent would be known to the plaintiff. Finally, in that service must be made "immediately" upon each adverse party later joined per CCP section 405.22, it would seem most unlikely their electronic contact information would have been provided. For these reasons, based on the timing considerations involved, the likelihood exists that most if	The committees appreciate the comment, but decline to alter the proposal at this time. While the proposed amendments would be applicable to only a narrow subset of litigants, it is reasonable to allow an electronic option for the notice where the litigants are already dealing electronically with one another. Electronic service also provides a sufficient record of transmission.

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
			not all of these notices would still be served by mail. Beyond the practical considerations, there are differences in the very nature of a notice of pendency of action which set it apart from a pleading, for example. These differences are not just rooted in tradition, but in actual distinction. The use and impact of these notices is serious which is, perhaps, the reason for the heightened requirements associated with their service (these heightened requirements would be lost, of course, were electronic service allowed). Pleadings simply may be mailed, but these notices must be sent registered or certified mail, return receipt requested. Both of these methods allow for tracking and evidence of receipt. Pleadings are filed with the court, while notices are recorded with the county recorder, and require a notary's seal and acknowledgment. Pleading and notices are both public records, but the notice appears in the chain of title giving constructive notice to all who come after. In short, a notice of pendency of	

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
			action is surrounded by unique considerations, and it should not be equated with, treated like, or served in the manner of a subsequent pleading. Agree – As to the proposed changes to CCP sections 594, 659, 660, and 663a. **Request for Specific Comments:** Does the proposal appropriately address the stated purpose? Yes, in light of the modernization project which seeks to "facilitate electronic filing and service and to foster modern e-business practices." It is believed, however, that the anticipated benefits of these efforts should be carefully weighed against certain implications and ramifications for litigants.	The committees appreciate the support. The committees appreciate the comment.
4.	Superior Court of Los Angeles County 111 N. Hill Street Los Angeles, CA 90012	AM	**Suggested modifications:** **Code of Civil Procedure § 594(b)** **Page 9, lines 1 through 3 -** In order to clarify that the 20 day provision only applies to service by mail, not electronic service, change:	The committees appreciate the comment, but the modification suggested in the comment goes beyond the scope of the proposal. The proposal adds electronic service as a mechanism to serve the notice of trial, but is not intended to alter the 20 day time frame.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated.

LEG 17-05
Proposed Legislation (Technology): Electronic Service (amend Civil Code section 1719 and Code of Civil Procedure sections 405.22, 405.23, 594, 659, 660, and 663a

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	[Proposed] Committee Response
			"…shall be served electronically in accordance with Section 1010.6 or by mail on all parties by the clerk of the court not less than 20 days prior to the date set for trial." **to** "…shall be served by mail on all parties by the clerk of the court not less than 20 days prior to the date set for trial or electronically in accordance with Section 1010.6."	
5.	Superior Court of San Diego County By Mike Roddy, Court Executive Officer County Courthouse 220 West Broadway San Diego, CA 92101	A	No specific comments.	The committees appreciate the support.

Positions: A = Agree; AM = Agree if modified; N = Do not agree; NI = Not indicated.