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

October 26, 2018
10:00 AM - 12:00 PM
Teleconference

Advisory Body Members Present:	Hon. Sheila F. Hanson, Chair; Hon. Louis R. Mauro, Vice Chair; Mr. Jake Chatters; Mr. Brian Cotta; Mr. Adam Creiglow; Hon. Julie R. Culver; Hon. Tara Desautels; Mr. Jason Galkin; Hon. Michael S. Groch; Hon. Samantha P. Jessner; Hon. Kimberly Menninger; Hon. James Mize; Mr. Snorri Ogata; Mr. Darrel Parker; Hon. Alan G. Perkins; Hon. Donald Segerstrom; Hon. Peter Siggins; Hon. Bruce Smith; Ms. Jeannette Vannoy; Mr. Don Willenburg; Mr. David H. Yamasaki
Advisory Body Members Absent:	Assembly member Marc Berman; Hon. Daniel Buckley; Ms. Alexandra Grimwade; Mr. Paras Gupta; Hon. Joseph Wiseman
Others Present:	Justice Marsha Slough; Mr. Rob Oyung; Mr. Zlatko Theodorovic; Mr. Mark Dusman; Ms. Jamel Jones: Mr. Richard Blalock; Ms. Camilla Kieliger; Ms. Fati Farmanfarmaian; Ms. Nicole Rosa; Ms. Jessica Craven; Ms. Jackie Woods; and other JCC staff present

OPEN MEETING

Call to Order and Roll Call

The chair called the meeting to order at 10:00 AM and took roll call.

Approval of Minutes and Public Comment

The advisory body reviewed and approved the minutes of the August 27, 2018 Information Technology Advisory Committee meeting. There were no public comments for today's meeting.

DISCUSSION AND ACTION ITEMS (ITEMS 1–7)

Item 1

Chair's Report

Presenter: Hon. Sheila F. Hanson, Chair

Update: Judge Hanson called the meeting to order, welcomed members, and provided the following updates: ITAC has three new members who are attending their first ITAC meeting today, they are Presiding Judge Donald Segerstrom, Superior Court of Tuolumne; Mr. Jake Chatters, CEO, Superior Court of Placer; and Mr. Adam Creiglow, CIO, Superior Court of Marin. On behalf of Judge Hanson and Justice Mauro she welcomed the new members and members reappointed to continue their terms with ITAC.

Judge Hanson reminded all members of the existing liaison appointments, shown on the roster in the materials, and asked that if anyone is interested in changing their current appointment, or if any of the new members are interested in serving as a liaison they should let her, or Justice Mauro know. Unless she hears otherwise, the appointments stand.

As a follow-up to the California Courts Protective Order Registry (CCPOR) discussion from the August 27, 2018 ITAC meeting regarding that system's governance and usage policy, the Chair advised that staff will initiate a discussion on this topic with the Family and Juvenile Law Advisory Committee. Judge Hanson would like Judge Kimberly Menninger and Mr. Rob Oyung to participate in this discussion and report back to ITAC.

Judge Hanson shared that the Judicial Council voted to approve the rule proposals submitted by ITAC on behalf the Rules & Policy Subcommittee, chaired by Justice Peter Siggins; and the Joint Appellate Technology Subcommittee, chaired by Justice Louis Mauro. Amending the rules was a year-long process and a significant undertaking that involved research, deliberation, consensus, and a complex comment process that both subcommittees worked hard to complete.

Lastly, Judge Hanson thanked members for completing the ITAC Member Survey. With over half of members responding, the feedback was positive, and a couple of suggestions included having more technology showcases and/or education sessions. She and Justice Mauro will investigate further.

Item 2

Judicial Council Technology Committee Update (JCTC)

Update on activities and news coming from this internal oversight committee.

Presenter: Hon. Marsha Slough, Chair, JCTC

Update: Justice Slough thanked ITAC for their continued dedication and provided a JCTC update since the August ITAC meeting. JCTC has met twice, conducted an orientation for new JCTC and ITAC members, and provided updates of both committees' activities to the Judicial Council at its September meeting.

At the September 10 JCTC meeting, ITAC status updates were provided for: workstream activities; the *Strategic Plan for Technology;* the proposed updates to the Judicial Branch Information Security Framework; and the establishment of an Information Security Outreach Program.

At the October 15 JCTC meeting, the JCTC took action to recommend that the Judicial Council adopt the proposed updates to the Judicial Branch Information Security Framework at their November meeting.

Justice Slough shared key updates to the proposed *Strategic Plan for Technology*, noting the overall tone has changed to be more future-focused and concise. It features a new executive summary and "guiding principles" organized into user-friendly categories. The streamlined plan is modeled after the California Department of Technology (DOT) plan. It also now uses metrics reframed as "measures for success", the detailed focus areas have

now been transitioned to the Tactical Plan Workstream, and content relating to dependencies and referencing specific technologies was eliminated. There was a two-week branch and a four-week public comment period, feedback was reviewed and incorporated as appropriate. JCTC will review and consider approving the final draft of the plan before submitting it to the Judicial Council for adoption at their November meeting. Justice Slough added her appreciation for the Tactical Plan Workstream as it is working on the complementary document to the Strategic Plan; both serve s important guiding documents for judicial branch technology.

Item 3

(a) Branch Budget Update

Update on the status of the branch budget, along with any technology-related discussions with the Department of Finance and/or with Legislators.

Presenter: Mr. Zlatko Theodorovic, Director, Budget Services

Update: Mr. Theodorovic advised that the Department of Finance (DOF) is building a new budget for this fiscal year, as there is an additional $1 Billion over the $2.3 Billion increase from last year. The judicial branch has been very engaged working with the DOF on the transition budget while the DOF looks at the new governor and administration, and its policy direction. Technology has been supported in the past and hopefully will continue to be supported with the new administration.

(b) Technology Budget Change Proposal Update

Overview and update regarding the Technology Budget Change Proposals (BCPs) status.

Presenter: Mr. Robert Oyung, Chief Operating Officer and Interim Chief Information Office

Update: Mr. Oyung reported that as of July 2018, the Judicial Council approved the Fiscal Year (FY) 2019/20 BCPs. Of the 15 BCPs submitted to DOT, 5 were technology related and are strong contributions to the branch strategic technology plans. These BCPs were a collaboration with all courts and are listed by their BCP priority in the branches' submission to the DOT. The technology BCPs are as follows (as prioritized by the Judicial Council): (1) Case Management (CMS) replacements for trial courts – Phase III; (2) Implementation of Phoenix System Roadmap; (5) Judicial Branch Business Intelligence and Data Analytics using Identity Management for data sharing; (8) Digitizing Documents; and (14) Futures Commission Directives for the expansion of technology in the courts. This information is also in the materials.

Mr. Oyung will facilitate a discussion with ITAC again in a few months to discuss FY 20/21 BCPs, and the future investments needed for the judicial branch.

Item 4

IT Community Development Workstream Update

Report on the IT Community Development Workstream's recent progress.

Presenter: Ms. Jeannette Vannoy, ITAC Member; Chief Information Officer, Superior Court of California, County of Napa

Update: Judge Perkins invited Ms. Vannoy to provide an update for ITAC. This workstream is focused on promoting culture as a branch IT community to drive technological change through resource sharing, education, and collaboration. The workstream plans to survey the courts to identify needs, key resources; develop recommendations; partner with education to develop a plan to keep branch abreast of technology trends; identify and evaluate technology tools; and pilot solutions along with Judicial Council IT. There are three workstream tracks: Resources (Jeannette Vannoy and Darrel Parker), Education (Judge McNamara and Mark Dusman), and Tools (Jeannette Vannoy and Jamel Jones). These tracks are outlined in detail in the materials.

Item 5

Tactical Plan Workstream Update

Report on the Tactical Plan Workstream's progress since the last in-person ITAC meeting.

Presenter: Hon. Sheila F. Hanson, ITAC Chair; and
Executive Sponsor for the Tactical Plan Workstream

Update: Judge Hanson, Executive Sponsor advised this workstream has made considerable progress since the August update. She reminded members of the technology planning governance structure via a slide in their materials. Since the August meeting, 17 new ideas were prioritized; and of those, 3 new initiatives were selected for inclusion in the updated plan. The new initiatives selected: Enterprise Resource Management – Provide upgrades and new services to enable the courts to manage their staff, financial, and facilities resources; Online Dispute Resolution – Explore policies, techniques, and technology to enable online resolution for disputes; and Security Roadmap – Advance branchwide IT security. Subject Matter Experts (SMEs) drafted descriptions for each initiative, which were then circulated to workstream members for comment. The workstream is half-way through their process and is looking forward to refining and drafting the plan for comment by ITAC, the branch, and the public.

Item 6

2018 Annual Agenda - Date Extension Requests (Administrative)

Futures Commission Directive – Remote Video Appearances for Most Non-Criminal Hearings
Request extension of estimated completion date to December 2018.
Hon. Samantha Jessner, Executive Sponsor

Digital Evidence Workstream

Request extension of estimated completion date to December 2018 ~~March 2018~~.

Hon. Kimberly Menninger, Executive Sponsor

Action: Judge Hanson approved the above date extensions and instructed staff to make the appropriate technical amendments to the annual agenda.

Item 7

2019 Annual Agenda Planning (Discussion)

Facilitated session to initiate planning of the ITAC 2019 Annual Agenda, including a review of the process and discussion of project topics (in progress and emerging) for consideration.

Presenters: Ms. Jamel Jones, Supervisor, Information Technology

Mr. Richard Blalock, Senior Business Systems Analyst, Information Technology

Mr. Blalock referenced the slides provided in the materials to discuss the 2019 Annual Agenda for ITAC and provide an overview of the process to members. Continuing for 2019 are the Futures Commission Directives, 9 workstreams, and 2 subcommittees. Next steps include staff working with leads to draft annual agenda project descriptions, then a draft will be circulated to ITAC members in late November, at the December 3 meeting ITAC members will discuss and finalize the proposed 2019 Annual Agenda, and finally it will go to the JCTC in January for their approval.

Judge Michael Groch suggested a future workstream to consider would be to automate the jury selection process, saving time for jurors and the court. A workstream could look at and/or improve technology to help selection process. For example, a system where jurors provide general info that would be asked in court; also knowing the diversity of jurors prior to selection could benefit judges but might also be shared with lawyers. Ms. Heather Pettit recalled companies that offer something similar and offered to do more research and share with ITAC. Additionally, Mr. Snorri Ogata advised that Los Angeles is using something similar and he could demo for ITAC.

ADJOURNMENT

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

Approved by the advisory body on enter date.

Electronic

PRIVACY RESOURCE GUIDE

Rev. 10/31/18

FOR THE CALIFORNIA TRIAL AND APPELLATE COURTS AND THE JUDICIAL BRANCH

FIRST EDITION
JANUARY 1, 2019

JUDICIAL COUNCIL OF CALIFORNIA
INFORMATION TECHNOLOGY ADVISORY COMMITTEE

Privacy Resource Guide

For the California
Trial and Appellate Courts
and the Judicial Branch

First Edition
January 1, 2019

Privacy Resource Guide

Table of Contents

10.1 Information Systems Controls Framework Template

10.2 How to Use the Information Systems Control Framework

Appendices

Appendix 1: Court records designated confidential by statute or rule
Appendix 2: Sample privacy statement for court websites
Appendix 3: Sample terms of use for court websites

1. Introduction

1.1 Background

Privacy is a fundamental right guaranteed by the California Constitution. (Cal. Const., art I, § 1; see *Westbrook v. County of Los Angeles* (1994) 27 Cal.App. 157, 164–166.) To protect people's privacy, numerous laws have been enacted that provide for the confidentiality of various kinds of personal information. In adjudicating cases, courts have a major role in enforcing these laws and protecting the privacy rights of citizens. Courts also are involved in protecting people's privacy rights through their own day-to-day operations, including preserving the integrity of confidential and sealed records, ensuring that sensitive data is secure, and protecting private personal information.

On the other hand, access to information concerning the conduct of the public's business is also a fundamental right of every citizen. (Cal. Const., art I, § 3(b); see *NBC Subsidiary (KNBC-TV) v. Superior Court of Los Angeles County* (1999) 20 Cal.4th 1178, 1217–1218 (substantive courtroom proceedings in ordinary civil cases are "presumptively open").) Courts are obligated to conduct their business in an open and transparent manner. (See also Cal. Rules of Court, rule 10.500.) Similarly, court records are presumed to be open and must be made accessible to the public unless made confidential or sealed. (See Cal. Rules of Court, rule 2.550(c).)[1] Openness and accessibility are important to preserve trust and confidence in the judicial system; and they are necessary to carry on the regular, ongoing business of the courts.[2]

1.2 Purpose of the Privacy Resource Guide

The purpose of this resource guide is to assist the trial and appellate courts—and more generally the judicial branch—to protect the privacy interests of persons involved with the California court system while providing the public with reasonable access to the courts and the records to which they are entitled.

The resource guide provides assistance in two ways. First, it provides information about the legal requirements that guide the courts' activities and operations relating to protecting the privacy of persons involved with the court system. Second, the guide provides practical advice for courts on the best practices for carrying out their obligations to protect people's privacy.

The creation of the resource guide at this time is important, among other reasons, because of the major transition underway that is transforming the courts from a paper-based physical system to one that relies increasingly on electronic records and other forms of technology to conduct business. With this change, much information in the courts that was practically obscure can now

[1] All references to rules in this resource guide are to the California Rules of Court, unless otherwise indicated.

[2] In recognition of the special role that courts play in conducting the people's business, the Legislature has in some instances exempted the courts from laws enacted to protect personal privacy. (See, e.g., Civ. Code, § 1798.3(b)(1) [excluding from the definition of "agency" covered by the Information Privacy Act of 1977 "[a]ny agency established under Article VI of the California Constitution"—that is, the courts].)

be made available remotely in easily searchable format. It requires careful analysis and the deliberate institution of new practices to ensure that proper privacy protections are now in place.

1.3 Key Definitions

As used in this resource guide, unless the context or subject matter otherwise requires:

(1) "Court record" means any document, paper, or exhibit filed by the parties to an action or proceeding; any order or judgment of the court; any item listed in Government Code section 68151, excluding any reporter's transcript for which the reporter is entitled to receive a fee for any copy. The term does not include the personal notes or preliminary memoranda of judges or other judicial branch personnel. (Cal. Rules of Court, rule 2.502.)

(2) A "document" may be in paper or electronic form.

(3) "Electronic record" means a court record that requires the use of an electronic device to access. The term includes both a document that has been filed electronically and an electronic copy or version of a record that was filed in paper form. (See, e.g., Cal. Rules of Court, rule 8.82(2).) Electronic records may be in the form of data.

(4) "Adjudicative record" means any writing prepared for or filed or used in a court proceeding, the judicial deliberation process, or the assignment or reassignment of cases and of justices, judges (including temporary and assigned judges), and subordinate judicial officers, or of counsel appointed or employed by the court. (Cal. Rules of Court, rule 10.500(c)(1).)

(5) "Confidential record" is a record that based on statute, rule, or case law is not open to inspection by the public. Confidential records are sometimes also not available to certain parties or persons.

(6) "Judicial administrative record" means any writing containing information relating to the conduct of the people's business that is prepared, owned, used, or retained by a judicial branch entity regardless of the writing's physical form or characteristics, except an adjudicative record. The term "judicial administrative record" does not include records of a personal nature that are not used in or do not relate to the people's business, such as personal notes, memoranda, electronic mail, calendar entries, and records of Internet use. (Cal. Rules of Court, rule 10.500(c)(2).)

(7) "Protected personal information" includes any information that can be used to identify, or describe, an individual such as his or her name, social security number, physical description, biometric records, home address, home telephone number, financial information, and medical or employment history.

(8) A "redacted version" is a version of a record from which all portions that disclose materials contained in a sealed, conditionally sealed, or confidential record have been removed. (See Cal. Rules of Court, rule 8.45(b)(6).)

(9) "Rule" means a rule of the California Rules of Court.

(10) An "unredacted version" is a version of a record or a portion of a record that discloses materials contained in a sealed, conditionally sealed, or confidential record. (See Cal. Rules of Court, rule 8.45(b)(7).)

(11) "Sealed record" means a record that by court order is not open to inspection by the public. (See Cal. Rules of Court, rule 2.550(b)(2).)

(12) "Writing" means any handwriting, typewriting, printing, photographing, photocopying, electronic mail, text messaging, fax, and every other means of recording on any tangible thing any form of communication or representation, including letters, words, pictures, sounds, symbols, or combinations, regardless of the manner in which the record has been stored. (Cal. Rules of Court, rule 10.500(c)(6); Evid. Code, § 250.)

2. Privacy in Court Records

2.1 Confidential and Sealed Records in the Trial Courts

Protection of privacy is an important major reason for making court records confidential or for sealing them. By making a document confidential or sealing it, the public and sometimes others are prevented by law from obtaining access to sensitive personal information or other information that might adversely affect a person's privacy. By respecting and enforcing the confidentiality or sealing, courts assist in protecting and preserving persons' privacy. However, there may be other reasons for making a document confidential or for sealing it besides protecting privacy. For example, confidentiality or sealing may be used to ensure the safety of witnesses, to protect trade secrets, or to preserve legally recognized privileges. This section focuses on records that are confidential or sealed in the trial courts principally or at least in part for reasons of protecting privacy interests.

Subsection 2.1.1 provides a nonexhaustive list of types of cases and proceedings and of specific records[3] that are exempt from the presumption of public disclosure by statute, regulation, court rule, or case law. Some records by law are strictly confidential and others may be confidential in particular circumstances. In addition to the records described in this section, there are many other confidential records discussed under more specific headings later in this resource guide and described in Appendix 1.

[3] Judicial Council forms may sometimes constitute the record or part of the record in a case. Any Judicial Council form that is labeled or entitled "CONFIDENTIAL" must not be disclosed, except as authorized by law.

Sealed records in the trial courts are discussed in subsection 2.1.2.

2.1.1 Confidential records

Records of Adoption Proceedings

Documents related to an adoption proceeding are not open to the public. Only the parties, their attorneys, and the Department of Social Services may review the records. The judge can authorize review by a requestor only in "exceptional circumstances and for good cause approaching the necessitous." (Fam. Code, § 9200(a).) Any party to the proceeding can petition the court to have redacted from the records, before copy or inspection by the public, the name of the birth parents and information tending to identify the birth parents. (Fam. Code, § 9200(b).)

Records of Juvenile Proceedings

Welfare and Institutions Code section 827 and California Rules of Court, rule 5.552, establish broad restrictions on the disclosure of juvenile court records. These laws reflect a general policy that, with certain limited exceptions, juvenile court records should remain confidential. (*In re Keisha T.* (1995) 38 Cal.App.4th 220, 225.) Specifically, section 827(a)(1)(P) permits juvenile court records to be inspected only by certain specified persons and "any other person who may be designated by court order of the judge of the juvenile court upon filing a petition." There is also an exception to this rule of confidentiality for certain records in cases brought under Welfare and Institutions Code section 602, in which the minor is charged with one or more specified violent offenses. (Welf. & Inst. Code, § 676.) In such cases, the charging petition, the minutes, and the jurisdictional and dispositional orders are available for public inspection (Welf. & Inst. Code, § 676(d)), unless the juvenile court judge enters an order prohibiting disclosure (Welf. & Inst. Code, § 676(e)). Thus, except for records enumerated in Welfare and Institutions Code section 676, if a record is part of a juvenile court file, it should be kept confidential and disclosed only as permitted under Welfare and Institutions Code section 827 and California Rules of Court, rule 5.552. Juvenile court records may also be subject to sealing orders under Welfare and Institutions Code sections 389, 781, and 786 (see § 2.1.2, "Sealed records").

Juvenile court records should remain confidential regardless of a juvenile's immigration status. (Welf. & Inst. Code, § 831(a).) Juvenile information may not be disclosed or disseminated to federal officials absent a court order upon filing a petition under Welfare and Institutions Code section 827(a). (Welf. & Inst. Code, § 831(b)–(c).) Juvenile information may not be attached to any documents given to or provided by federal officials absent prior approval of the presiding judge of the juvenile court under Welfare and Institutions Code section 827(a)(4). (Welf. & Inst. Code, § 831(d).) "Juvenile information" includes the "juvenile case file" as defined in Welfare and Institutions Code section 827(e), as well as information regarding the juvenile such as the juvenile's name, date or place of birth, and immigration status. (Welf. & Inst. Code, § 831(e).)

Dismissed petitions: The court must order sealed all records related to any petition dismissed under Welfare and Institutions Code section 786 that are in the custody of the juvenile court, law enforcement agencies, the probation department, and the Department of Justice. The procedures

for sealing these records are stated in Welfare and Institutions Code section 786 and rule 5.840 of the California Rules of Court.

Special Immigrant Juvenile Findings

In any judicial proceedings in response to a request that the superior court make the findings necessary to support a petition for classification as a special immigrant juvenile, information regarding the child's immigration status that is not otherwise protected by the state confidentiality laws must remain confidential and must be available for inspection only by the court, the child who is the subject of the proceeding, the parties, the attorneys for the parties, the child's counsel, and the child's guardian. (Code Civ. Proc., § 155(c).)

In any judicial proceedings in response to a request that the superior court make the findings necessary to support a petition for classification as a special immigrant juvenile, records of the proceedings that are not otherwise protected by state confidentiality laws may be sealed using the procedure in California Rules of Court, rules 2.550 and 2.551. (Code Civ. Proc., § 155(d).)

Confidentiality of Records in Civil Cases

Unlawful Detainer Proceedings

Court files and records in unlawful detainer proceedings are not publicly available except for access to limited civil case records and including the court file, index, and register of actions only to persons specified by statute under Code of Civil Procedure section 1161.2(a)(1)(A)–(D). (Code Civ. Proc., § 1161.2.) In addition, access to limited civil records in unlawful detainer proceedings shall be allowed only:

- To a person by order of court if judgment is entered for the plaintiff after trial more than 60 days since filing of the complaint (Code Civ. Proc., § 1161.2(a)(1)(F));
- Except in cases involving residential property based on section 1161a as indicated in the caption of the complaint, to any other person 60 days after the complaint has been filed if the plaintiff prevails in the action within 60 days of filing the complaint, in which case the clerk shall allow access to any court records in the action. If a default or default judgment is set aside more than 60 days after the complaint was filed, section 1161.2 shall apply as if the complaint had been filed on the date the default or default judgment is set aside (Code Civ. Proc., § 1161.2(a)(1)(F));
- In the case of a complaint involving residential property based on section 1161a as indicated on the caption of the complaint, to any other person, if 60 days have elapsed since the complaint was filed with the court, and as of that date, judgment against all defendants has been entered for the plaintiff, after a trial. (Code Civ. Proc., § 1161.2(a)(1)(G).)

An exception excludes records of mobile home park tenancies from this code section if the caption in the complaint indicates clearly that the complaint seeks to terminate a mobile home park tenancy; those records are not confidential. In addition, effective January 1, 2011, access to

court records in unlawful detainer proceedings is permanently limited to persons specified in the statute in the case of complaints involving residential property based on section 1161a (holding over after sale under execution, mortgage, or trust deed [foreclosures]) as indicated in the caption of the complaint, unless 60 days have elapsed since filing of the complaint and judgment has been entered, after a trial, for the plaintiff and against all defendants. (Code Civ. Proc., § 1161.2.) The complaints in these actions shall state in the caption: "Action based on Code of Civil Procedure section 1161a." (Code Civ. Proc., § 1166(c).)

False Claims Act Cases

The documents initially filed in cases under the False Claims Act are confidential under Government Code section 12650 et seq. The complaint and other initial papers should be attached to a Confidential Cover Sheet—False Claims Action (form MC-060). The cover sheet contains a place where the date on which the sealing of the records in the case expires.

Confidential Records in Criminal Proceedings

Search warrants

It is within the court's discretion to seal the court documents and records of a search warrant until the warrant is executed and returned, or until the warrant expires. (Pen. Code, § 1534(a).) Thereafter, if the warrant has been executed, the documents and records shall be open to the public as a judicial record. Evidence Code sections 1040 and 1041 establish exceptions to the public status of executed search warrants; these provisions allow public entities to refuse disclosure of confidential official information and an informant's identity when disclosure is against the public interest. When a search warrant is valid on its face, a public entity bringing a criminal proceeding may establish the search's legality without revealing to the defendant any confidential official information or an informant's identity. (Evid. Code, § 1042(b).) When a search warrant affidavit is fully or partially sealed pursuant to Evidence Code sections 1040 through 1042, the defense may request a motion to quash or traverse the search warrant. The court should conduct an in camera hearing following the procedure established in *People v. Hobbs* (1994) 7 Cal.4th 948.

Police reports

There is no specific statute, rule, or decision addressing the confidentiality of a police report once it has become a "court record." Generally speaking, a police report that has been used in a judicial proceeding or is placed in a court file is presumed to be open to the public. Many police reports, however, contain sensitive or personal information about crime victims, witnesses, and other third parties. Penal Code section 1054.2(a)(1) provides that defense counsel may not disclose the address or telephone number of a victim or witness to the defendant or his or her family. Similarly, law enforcement agencies are prohibited from disclosing the address and phone number of a witness or victim, or an arrestee or potential defendant. (Pen. Code, § 841.5.) We suggest that courts should require that personal information be redacted *before* the report is filed with the court or used in a judicial proceeding.

Probation reports

Probation reports filed with the court are confidential *except* that they may be inspected

- by anyone up to 60 days after either of two dates, whichever is earlier: (1) when judgment is pronounced, or (2) when probation is granted;
- by any person pursuant to a court order;
- if made public by the court on its own motion; and
- by any person authorized or required by law. (Pen. Code, § 1203.05.)

Confidential Records in Family Law proceedings

Child custody investigation and evaluation reports

These reports must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officer, court employee or family court facilitator for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person upon order of the court for good cause. (Fam. Code §§ 3025.5, 3111, & 3118; Evid. Code, § 730.)

Child custody mediation proceedings and reports

Child custody mediation proceedings and all communication, verbal or written, from the parties to the mediator are confidential. If the mediator is authorized by local rule to issue a report to the court containing recommendations as a "Child Custody Recommending Counselor," the report must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officer, court employee or family court facilitator for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person upon order of the court for good cause. (Fam. Code, §§ 3025.5, 3177, & 3183.)

Written statements of issues and contentions by counsel appointed for child

These written statements must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officer, court employee or family court facilitator for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person, upon order of the court, for good cause. (Fam. Code, §§ 3025.5, 3151(b).)

Parentage Act documents

Records in Uniform Parentage Act proceedings, except the final judgment, are not open to the public. (Fam. Code, § 7643(a).) If a judge finds that a third party has shown good cause and finds exceptional circumstances, the court may grant that person access to the records. (*Ibid.*) This includes records from paternity actions.

Family conciliation court records

These records are confidential. The judge of the family conciliation court can grant permission for a party to review certain documents. (Fam. Code, § 1818(b).)

Proceeding to terminate parental rights
Documents related to such proceedings are confidential; only persons specified by law may review the records. (Fam. Code, § 7805.)

Support enforcement and child abduction records
Support enforcement and child abduction records are generally confidential; these records may be disclosed to persons specified by statute only under limited circumstances. In certain instances, the whereabouts of a party or a child must not be revealed to the other party or his or her attorneys. A local child support agency must redact such information from documents filed with the court. (Fam. Code, § 17212.)

Confidential Records in Probate Proceedings

Confidential Guardian Screening Form (form GC-212)
This mandatory Judicial Council form regarding the proposed guardian is confidential. It is used by the court and by persons or agencies designated by the court to assist in determining whether a proposed guardian should be appointed. (Cal. Rules of Court, rule 7.1001(c).)

Confidential Supplemental Information (form GC-312)
This form regarding the proposed conservatee is confidential. It shall be separate and distinct from the form for the petition. The form shall be made available only to parties, persons given notice of the petition who have requested this supplemental information, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, 1821(a).)

Confidential Conservator Screening Form (form GC-314)
This mandatory Judicial Council form is confidential. (Cal. Rules of Court, rule 7.1050(c).)

Reports regarding proposed conservators or guardianship
An investigative report created pursuant to Probate Code section 1513 concerning a proposed guardianship is confidential and available only to parties served in the action or their attorneys (generally, parents, legal custodian of child). An investigative report created pursuant to Probate Code section 1826 regarding the proposed conservatee is confidential and available only to those persons specified by statute. Under the statute, the reports on proposed conservatees shall be made available only to parties, persons given notice of the petition who have requested the report, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the reports on guardianships and conservatorships exclusively to persons entitled thereto. (Prob. Code, §§ 1513(d), 1826(n).)

Investigator's review reports in conservatorships

These reports are confidential. The information in the reports may be made available only to parties, persons identified in section 1851(b), persons given notice who have requested the report or appeared in the proceeding, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interests of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, §§ 1851(b) & (e).) Subdivision (b) provides for special restricted treatment of attachments containing medical information and confidential criminal information from California Law Enforcement Telecommunications System (CLETS). Although the attachments are not mentioned in subdivision (e), it is recommended, to be consistent with subdivision (b), that they be treated as confidential except to the conservator, conservatee, and their attorneys.

Certification Forms

Certification of counsel of their qualifications (form GC-010) and certification of completion of continuing education (form GC-011): The forms state that they are "confidential for court use only." They are governed by rule 7.1101, which states that the certifications must be submitted to the court but not lodged or filed in a case file. (Cal. Rules of Court, rule 7.1101(h)(6).)

Confidential Records in Protective Order Proceedings

Confidential CLETS Information Form

A Judicial Council form, *Confidential CLETS Information* **(**form CLETS-001), has been developed for petitioners in protective order proceedings to use to submit information about themselves and the respondents to be entered through the CLETS into the California Restraining and Protective Order System (CARPOS), a statewide database used to enforce protective orders. This form is submitted to the courts by petitioners in many types of protective order proceedings, including proceedings to prevent domestic violence, civil harassment, elder and dependent adult abuse, private postsecondary school violence, and juvenile cases. The information on the forms is intended for the use of law enforcement. The form is confidential. Access to the information on the form is limited to authorized court personnel, law enforcement, and other personnel authorized by the California Department of Justice to transmit or receive CLETS information. The form~~s~~ must not be included in the court file. (Cal. Rules of Court, rule 1.51.)

Protecting information about a minor in Protective Order Cases

Family Code Section 527.6 was amended and Code of Civil Procedure Section 6301.5 was added to permit a minor or minor's legal guardian to petition the court to make information relating to a minor confidential when issuing a domestic violence or civil harassment restraining order to protect the private information of vulnerable minors who are the victims of domestic abuse and human trafficking. The standard for granting these requests is essentially the same standard for the sealing of records under rule 2.550 of the California Rules of Court. The information that can be kept confidential includes the minor's name, address and other information relating to the minor. New California Rules of Court 3.1161 and 5.382 provide a consistent procedure for making requests for confidentiality, making orders on a request for confidentiality, and protecting information made confidential by the court. The minor or the minor's legal guardian can request

that the information relating to the minor be kept confidential at any time during the case, using the new forms, *Request to Keep Minor's Information Confidential* (forms CH-160 and DV-160). Using the *Order on Request to Keep Minor's Information Confidential* (forms CH-165 and DV165), the court expressly finds all of the following:

1. The minor's right to privacy overcomes the right of public access to the information.
2. There is a substantial probability that the minor's interest will be prejudiced if the information is not kept confidential.
3. The order to keep the information confidential is narrowly tailored. 4. No less restrictive alternative exists to protect the minor's privacy.

When a confidentiality order has been issued, the party will use the *Notice of Order Protecting Information of a Minor* (forms CH-170 and DV-170) as a cover sheet for the requesting party to serve with the order and with the documents that contain information the court has ordered be protected (confidential). The cover sheet will provide notice to the party (often the restrained person) being served with unredacted documents that the documents contain confidential information subject to a confidentiality order. *Cover Sheet for Confidential Information* (forms CH-175 and DV-175) will be used as a cover sheet for any documents that include confidential information, subsequently filed in the protective order proceedings. This form alerts the clerk that the documents contain confidential information, so that the court can file the unredacted documents in the court's confidential files and make a determination as to who would be responsible for redaction of the documents so that redacted versions can be placed in the public files. This cover sheet can also be used in any other civil proceedings to alert the court in that proceeding that a confidentiality order exists protecting the minor's information.

Subpoenaed business records

Subpoenaed business records of nonparty entities are confidential until otherwise agreed to by the parties, introduced as evidence, or entered into the record. (Evid. Code, § 1560(d).)

Pitchess motions

Police officer personnel records are confidential and shall not be disclosed in any criminal or civil proceeding. (Pen. Code, § 832.7.) In criminal cases where the confidential personnel file of a peace officer may contain evidence relevant to the defense, a motion to discover relevant information may be brought by way of a *Pitchess* motion (*Pitchess v. Superior Court* (1974) 11Cal.3d 531). The process for requesting court review for possible discovery of limited police officer personnel file information is codified in Evidence Code sections 1043–1046. If a defendant establishes good cause for disclosure, the trial court must screen the personnel files in camera for evidence that may be relevant to the defense. The court must examine the personnel files, make a record of the items reviewed and, if relevant, reveal the name, address and phone number of any prior complainants and witnesses and dates of prior incidents. (*City of Santa Cruz v. Municipal Court* (1999) 49 Cal.3d 74, 84.) The court must order any disclosure not be used for any purpose other than in the underlying court proceeding. The *Pitchess* motion hearing transcript is sealed.

Medical records

The following federal and California statutes limit disclosure of medical records by medical providers, health care plans, or contractors. The laws do not impose obligations on the courts as to handling, management, and retention of medical records in court records. However, courts should place appropriate protections on medical records that have been filed confidentially or under seal.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA and related federal regulations (42 U.S.C. § 1320d et seq., 45 C.F.R. § 160 et seq. & 164 et seq.) set standards for medical information held by covered entities, defined as: (1) a health plan, (2) health-care clearinghouse, or (3) a health-care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA provisions. (45 C.F.R. § 160.102(a).) Generally, courts participating in CalPERS Health Program, county-sponsored health plans, the Trial Court Benefits Program administered by the Judicial Council, or other fully insured plans are not covered entities subject to HIPAA, and therefore, the privacy rules of HIPAA do not directly apply to courts in their judicial function. (See 45 C.F.R. parts 160–164.) However, HIPAA prohibits covered entities from disclosing medical records or protected health information ("PHI") without a patient's signed authorization or a signed court order. (45 C.F.R. § 164.508; 45 C.F.R. § 164.512(e)(1).) Parties responsible for maintaining confidentiality of information under HIPAA should request that such information be filed under seal pursuant to rules 2.550 and 2.551 of the California Rules of Court.

Because a court may meet the definition of "plan sponsor" under HIPAA (45 C.F.R. § 164.103), a court may have to comply with two minimal privacy obligations under HIPAA: (1) the "nonwaiver" provision, which prohibits a requirement that an individual waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility; and (2) the "nonretaliation" provision, which forbids retaliatory action against individuals for exercising rights under HIPAA. Courts should consult with their human resources departments for appropriate personnel policy language.

California Confidentiality of Medical Information Act (Civ. Code, § 56–56.37)

The Confidentiality of Medical Information Act governs the disclosure of medical information by health-care providers. (Civ. Code, § 56 et seq.) Courts are generally not health-care providers covered by the act and are not directly subject to the law's confidentiality provisions. (Civ. Code, § 56.05(m).) A limited exception may occur when a court employs a health-care provider, such as a clinical social worker, to conduct assessments and other services for a collaborative court. In these limited circumstances, the medical information is likely confidential, and court staff should use an authorization for release of medical information to discuss pertinent information with other collaborative court team members. (Civ. Code, § 56.10(a).) California law prohibits medical providers, health-care service plans, or contractors from disclosing a patient's medical information, without authorization, or, among other things, a court order. (Civ. Code, § 56.10(b)(1).) A party submitting such medical information should submit the information pursuant either to a protective order and/or a motion to seal. (See rule 2.551.)

- **[Practice Tip**: When parties submit medical information, including medical records or other records containing PHI, without seeking a protective order or filing a motion to seal, a court may, if it identifies such information, issue on its own motion a qualified protective order filing such information under seal.]

Psychiatric records or reports

Records of mental health treatment or services for the developmentally disabled, including Lanterman-Petris-Short (LPS) Act proceedings

Under Welfare and Institutions Code sections 5328 and 5330, the following records are confidential and can be disclosed only to recipients authorized in Welfare and Institutions Code section 5328: records related to the Department of Mental Health (Welf. & Inst. Code, § 4000 et seq.); Developmental Services (Welf. & Inst. Code, § 4400 et seq.); Community Mental Health Services (Welf. & Inst. Code, § 5000 et seq.); services for the developmentally disabled (Welf. & Inst. Code, § 4500 et seq.); voluntary admission to mental hospitals (Welf. & Inst. Code, § 6000 et seq.); and mental institutions (Welf. & Inst. Code, § 7100 et seq.).

Psychiatric records or reports in criminal cases

Reports prepared at the request of defense counsel to determine whether to enter or withdraw a plea based on insanity or mental or emotional condition are confidential. (Evid. Code, § 1017.) However, most psychiatric reports prepared at the court's request are presumed open to the public. (See Evid. Code, § 1017 [report by a court-appointed psychotherapist]; Evid. Code, § 730 [report by a court-appointed expert]; Pen. Code, § 288.1 [report on sex offender prior to suspension of sentence]; Pen. Code, § 1368 [report concerning defendant's competency]; and Pen. Code, §§ 1026, 1027 [report on persons pleading not guilty by reason of insanity].)

Reports concerning mentally disordered prisoners

Reports under Penal Code section 4011.6 to evaluate whether prisoners are mentally disordered are confidential. (Pen. Code, § 4011.6.)

Presentencing diagnostic reports

Under Penal Code section 1203.03, the report and recommendation from the 90-day Department of Corrections presentencing diagnosis should be released only to defendant or defense counsel, the probation officer, and the prosecuting attorney. After the case closes, only those persons listed immediately above, the court, and the Department of Corrections may access the report. Disclosure to anyone else is prohibited unless the defendant consents. (Pen. Code, § 1203.03(b).)

Medical diagnoses and test results

Substance use disorder-related information from qualifying federally assisted programs

The Code of Federal Regulations provides that information that would disclose the identity of a person receiving treatment for a substance use disorder from a qualifying federally assisted program is confidential. (42 C.F.R. § 2.12.) A "qualifying federally assisted program" subject to

the regulations includes a recipient of federal financial assistance in any form, including financial assistance which does not directly pay for the substance use disorder diagnosis, treatment, or referral for treatment; or a program conducted by a state or local government unit that, through general or special revenue sharing or other forms of assistance, receives federal funds that could be (but are not necessarily) spent for the substance use disorder program. (*Id*. at § 2.12(b)(3)(i), (ii).) A "program" is defined to include "an individual or entity (other than a general medical care facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment or referral for treatment. . . ." (*Id*. at § 2.11(a).) Information from collaborative courts involving substance use disorder diagnosis or treatment, such as drug court programs, may be subject to the confidentiality provisions of the federal regulations, depending on whether the program or the court receives federal financial assistance as defined in the regulations. This may include information related to program participants and records identifying the participant and his or her diagnosis and treatment.

Infectious or Communicable Disease Information

Under Health and Safety Code section 120290(h)(1), when alleging a violation of section 120290(a), the prosecuting attorney or the grand jury must substitute a pseudonym for the true name of a complaining witness. The actual name and other identifying characteristics of a complaining witness shall be revealed to the court only in camera, unless the complaining witness requests otherwise, and the court shall seal the information from further disclosure, except by counsel as part of discovery. Under Health and Safety Code section 120290(h)(2), unless the complaining witness requests otherwise, all court decisions, orders, petitions, and other documents, including motions and papers filed by the parties, shall be worded so as to protect the name or other identifying characteristics of the complaining witness from public disclosure.

Under Health and Safety Code section 120290(h)(3), unless the complaining witness requests otherwise, a court in which a violation of this section is filed shall, at the first opportunity, issue an order that prohibits counsel, their agents, law enforcement personnel, and court staff from making a public disclosure of the name or any other identifying characteristic of the complaining witness.

Under Health and Safety Code section 120290(h)(4), unless the defendant requests otherwise, a court in which a violation of this section is filed, at the earliest opportunity, shall issue an order that counsel and their agents, law enforcement personnel, and court staff, before a finding of guilt, not publicly disclose the name or other identifying characteristics of the defendant, except by counsel as part of discovery or to a limited number of relevant individuals in its investigation of the specific charges under this section. In any public disclosure, a pseudonym shall be substituted for the true name of the defendant.

HIV Test Results or Status

No person shall disclose HIV test results without the patient's signed authorization, or except pursuant to Health and Safety Code section 1603.1, 1603.3, or 121022, or any other statute expressly providing an exemption. (Health & Saf. Code, § 120980(g).)

Court records containing results of mandatory AIDS testing for defendants convicted of violating Penal Code section 647(b) are, with certain specified exceptions, confidential. (Former Pen. Code, § 1202.6(f).) HIV test results ordered of defendants charged with certain crimes are also confidential. (Pen. Code, §§ 1202.1, 1524.1.)

Penal Code section 1202.1 requires every person convicted of the following crimes to undergo an HIV test: rape in violation of Penal Code section 261 or 264.1; unlawful intercourse with a person under 18 years of age in violation of Penal Code section 261.5 or 266c; rape of a spouse in violation of Penal Code section 262 or 264.1; sodomy in violation of Penal Code section 266c or 288a; or any offenses if the court finds that there is probable cause to believe that blood, semen, or other bodily fluid capable of transmitting HIV has been transferred from the defendant to the victim during certain offenses or attempts to commit such offenses (sexual penetration in violation of Penal Code section 264.1, 266c, or 289; aggravated sexual assault of a child in violation of Penal Code section 269; lewd or lascivious conduct with a child in violation of Penal Code section 288; continuous sexual abuse of a child in violation of Penal Code section 288.5). The clerk of the court shall transmit the HIV results to the Department of Justice and the local health officer.

Penal Code section 1524.1 provides that, where there is (i) a defendant charged with certain crimes (Pen. Code, §§ 220, 261, 262, 264.1, 266c, 269, 286, 288, 288a, 288.5, 289.5) or with the attempt to commit any of these offenses, ***and*** is the subject of a police report alleging commission of, or of attempt to commit, a separate, uncharged offense that could be charged under those previously cited statutes; or (ii) a minor is the subject of a petition filed in juvenile court alleging commission of crimes under those cited statutes, or attempt to commit any of the offenses, and is the subject of a police report alleging commission of a separate, uncharged offense under those cited statutes, or attempt to commit any of those offenses, at the request of the victim of the uncharged offense, the court may issue a search warrant to obtain an HIV test from the charged defendant or minor upon proper findings of probable cause.

If a court orders HIV tests under Health and Safety Code sections 121055, 121056, and 121060, the court shall order that all persons receiving the results maintain the confidentiality of personal identifying data related to the test results, except as necessary for medical or psychological care or advice. (Health & Saf. Code, § 121065.)

However, HIV status and/or test results under former Penal Code sections 647f and 12022.85, and former Health and Safety Code sections 1621.5, 120290, and 120291 are generally not confidential as they are a required element of a crime or enhanced sentencing and may become part of the public court records in these cases. (Former Pen. Code, § 647f was repealed as of Jan. 1, 2018, by Stats. 2017, ch. 537, § 8; former Health & Saf. Code, § 1621.5 was repealed as of

Jan. 1, 2018, by Stats. 2017, ch. 537, § 2; former Health & Saf. Code, § 120290 was repealed as of Jan. 1, 2018, by Stats. 2017, ch. 537, § 4, and new Health & Saf. Code, § 120290 was added as of Jan. 1, 2018, by Stats. 2017, ch. 537, §5; former Health & Saf. Code, § 120291 was repealed as of Jan. 1, 2018, by Stats. 2017, ch. 537, § 6.)

Further, see above discussion regarding medical diagnoses and tests for discussion about Health and Safety Code section 120290(h)(1) and requirements for sealing information in cases regarding alleged violations of section 120290(a).

Confidential Requests for Disability Accommodation

Under rule 1.100(c), persons with disabilities may request accommodations from the court by submitting form MC-410. Courts must keep this form confidential, unless the applicant waives confidentiality in writing or disclosure is required by law. The applicant's identity and confidential information may not be disclosed to the public or to persons other than those involved in the accommodation process. Confidential information includes all medical information related to the applicant and all oral or written communication from the applicant concerning the request for accommodation. (Cal. Rules of Court, rule 1.100(c)(4).)

2.1.2 Sealed records

General Rules on Sealed Records: Rules 2.500 and 2.551

The main rules on sealed records in the trial courts are contained in rules 2.550 and 2.551 of the California Rules of Court. The premise of these rules is that court records are presumed to be open unless confidentiality is required by law. (Cal. Rules of Court, rule 2.550(c).) A court may only order that a record be filed under seal if it expressly finds facts that establish:

(1) There exists an overriding interest that overcomes the right of public access to the record;

(2) The overriding interest supports sealing the record;

(3) A substantial probability exists that the overriding interest will be prejudiced if the record is not sealed;

(4) The proposed sealing is narrowly tailored; and

(5) No less restrictive means exist to achieve the overriding interest.

(Cal. Rules of Court, rule 2.551(d).) This substantive test is based on the Supreme Court's decision in *NBC Subsidiary (KNBC-TV) v. Superior Court of Los Angeles County* (1999) 20 Cal.4th 1178, 1217–1218.

The right of privacy may qualify as an overriding interest in the proper situation. In *In re Marriage of Burkle* (2006) 135 Cal.App.4th 1045, the court stated: "We have no doubt that, in appropriate circumstances, the right of privacy may be properly described as a compelling or

overriding interest." (*Id.* at p. 1063.) However, the *Burkle* case involved an attempt to close financial records in divorce proceedings under a statute, Family Code section 2024.6, which the court concluded was not narrowly tailored to serve overriding privacy interests. Because less restrictive means exist to achieve the statutory objective, the court found that Family Code section 2024.6 operates as an undue burden on the First Amendment right of public access to court records. Hence, the court concluded that statute is unconstitutional on its face. (*Id.* at p. 1048.)

In circumstances where a court determines that sealing is appropriate, the content and scope of the sealing order is prescribed by rule. The rules provide that the court's order must (1) state the facts that support the findings, and (2) direct the sealing of only those documents and pages, or if reasonably practical, portions of those documents and pages that contain the materials that need to be placed under seal. All other portions of each document or page must be included in the public file. (Cal. Rules of Court, rule 2.550(e).)

The procedures for filing records under seal in the trial courts are contained in rule 2.551. (Cal. Rules of Court, rule 2.551.)

Sealing of specific records in criminal cases

Certain specific criminal court records may be sealed upon a motion and court order under various provisions. (See Appendix 1.)

Sealing of Records in Juvenile Cases

There are three specific statutes and two rules on sealing juvenile records. (Welf. & Inst. Code, §§ 781, 786 & 786.5; Cal. Rules of Court, rules 5.830 & 5.840.) Section 781 and rule 5.830 allow a former ward of the court to petition the court to order juvenile records sealed. If the petition is granted, the court must order the sealing of all records described in section 781. The order must apply in the county of the court hearing the petition and all other counties in which there are juvenile records concerning the petitioner. (Cal. Rules of Court, rule 5.830(a)(4).) All records sealed must be destroyed according to section 781(d). There is also a requirement in section 786 that the court order records sealed for juvenile delinquency cases when the child has satisfactorily completed probation and the offense charged is not listed in Welfare and Institutions Code section 707(b). Specific procedures to dismiss and seal the records of minors who are subject to section 786 are contained in rule 5.840 (Cal. Rules of Court, rule 5.840). There are numerous instances where records sealed under section 786 are allowed to be accessed by various entities without the access being deemed an unsealing (see Welf. & Inst. Code, § 786(g)). Welfare and Institutions Code section 786.5 requires the probation department to seal records for diversion cases when the diversion program has been satisfactorily completed and to provide notice that it has sealed the records or, if it has not, the reason for not doing so. It also provides the right to petition the court for review of a determination that records should not be sealed.

2.2 Confidential and Sealed Records in the Appellate Courts

For appeals and original proceedings in the Supreme Court and Courts of Appeal, specific rules have been adopted relating to sealed and confidential records: rule 8.45 (general provisions), rule 8.46 (sealed records), and rule 8.47 (confidential records).

2.2.1 General provisions

Rule 8.45 provides general requirements for the handling of sealed and confidential records by a reviewing court. These records must be kept separate from the rest of the records sent to the court and must be kept in a secure manner that preserves their confidentiality. (Cal. Rules of Court, rule 8.45(c)(1).) The rule prescribes the format of sealed and confidential records, and states the manner in which these records are to be listed in alphabetical and chronological indexes available to the public. (Cal. Rules of Court, rule 8.45(c)(2).) It describes the special treatment required for records relating to a request for funds under Penal Code section 987.9. (Cal. Rules of Court, rule 8.45(c)(3).)

Rule 8.45 also provides guidance on the transmission of and access to sealed and confidential records. For instance, unless otherwise provided by law, a sealed or confidential record that is part of the record on appeal must be transmitted only to the reviewing court and the party or parties who had access to the record in the trial court and may be examined only by the reviewing court and that party or parties. If a party's attorney but not the party had access to the record in the trial court, only the party's attorney may examine the record. (Cal. Rules of Court, rule 8.45(d)(1).)

2.2.2 Sealed records

Rule 8.46 is the basic rule on sealed records in the reviewing court. First, it provides that if a record sealed by order of the trial court is part of the record on appeal, the sealed record must remain sealed unless the reviewing court orders otherwise. The record on appeal or supporting documents must include the motion or application to seal in the trial court, all documents filed in the trial court supporting or opposing the motion or application to seal, and the trial court order sealing the record. (Cal. Rules of Court, rule 8.46(b)(1)–(2).)

Second, a record filed or lodged publicly in the trial court and not ordered sealed must not be filed under seal in the reviewing court. (Cal. Rules of Court, rule 8.46(c).)

Third, the rule prescribes the procedures for obtaining an order from a reviewing court to seal a record that was not filed in the trial court. (Cal. Rules of Court, rule 8.46(d).)

Fourth, a sealed record must not be unsealed except on order of the reviewing court. The rule prescribes the procedures for seeking to unseal a record in the reviewing court. (Cal. Rules of Court, rule 8.46(e).)

Fifth, the rule prohibits the public filing in a reviewing court of material that was filed under seal, lodged conditionally under seal, or otherwise subject to a pending motion to file under seal. (Cal. Rules of Court, rule 8.46(f).)

2.2.3 Confidential records

Rule 8.47 governs the form and transmission of and access to confidential records (as distinguished from records sealed by court order or filed conditionally sealed) in the appellate courts. (Cal. Rules of Court, rule 8.47(a).) The rule includes a subdivision specifically on how to handle reporter's transcripts and documents filed or lodged in *Marsden* hearings and other in camera proceedings. (Cal. Rules of Court, rule 8.47(b).) It also contains general procedures for handling other confidential records. (Cal. Rules of Court, rule 8.47(c).)

2.3 Privacy in Opinions of the Courts of Appeal

Based on concerns about the need for privacy protection, two rules of court have been adopted relating to the references to specific individuals in opinions and certain other records.

2.3.1 Privacy in appellate opinions

Rule 8.90, adopted effective January 1, 2017, provides guidance on the use of names in appellate court opinions, except for names in juvenile cases that are covered by rule 8.401 (discussed below). The rule states that, to protect personal privacy interests, the reviewing court should consider referring in opinions to people on the following list by first name and last initial or, if the first name is unusual or other circumstances would defeat the objective of anonymity, by initials only:

(1) Children in all proceedings under the Family Code and protected persons in domestic violence prevention proceedings;

(2) Wards in guardianship proceedings and conservatees in conservatorship proceedings;

(3) Patients in mental health proceedings;

(4) Victims in criminal proceedings;

(5) Protected persons in civil harassment proceedings under Code of Civil Procedure section 527.6;

(6) Protected persons in workplace violence prevention proceedings under Code of Civil Procedure section 527.8;

(7) Protected persons in private postsecondary school violence prevention proceedings under Code of Civil Procedure section 527.85;

(8) Protected persons in elder or dependent adult abuse prevention proceedings under Welfare and Institutions Code section 15657.03;

(9) Minors or persons with disabilities in proceedings to compromise the claims of a minor or a person with a disability;

(10) Persons in other circumstances in which personal privacy interests support not using the person's name; and

(11) Persons in other circumstances in which use of that person's full name would defeat the objective of anonymity for a person identified in (1)–(10).

2.3.2 Confidentiality in juvenile records and opinions

To protect the anonymity of juveniles involved in juvenile court proceedings, rule 8.401, adopted effective January 1, 2012, provides:

- In all documents filed by the parties in juvenile appeals and writ proceedings, a juvenile must be referred to by first name and last initial; but if the first name is unusual or other circumstances would defeat the objective of anonymity, the initials of the juvenile may be used.

- In opinions that are not certified for publication and in court orders, a juvenile may be referred to either by first name and last initial or by his or her initials. In opinions that are certified for publication, a juvenile must be referred to by first name and last initial; but if the first name is unusual or other circumstances would defeat the objective of anonymity, the initials of the juvenile may be used.

- In all documents filed by the parties and in all court orders and opinions in juvenile appeals and writ proceedings, if use of the full name of a juvenile's relative would defeat the objective of anonymity for the juvenile, the relative must be referred to by first name and last initial; but if the first name is unusual or other circumstances would defeat the objective of anonymity for the juvenile, the initials of the relative may be used.

(Cal. Rules of Court, rule 8.401(a).)

Rule 8.401 also contains provisions regarding access to filed documents. In general, the record on appeal and documents filed by the parties in proceedings under this chapter may be inspected only by the reviewing court and appellate project personnel, the parties or their attorneys, and other persons the court may designate. Filed documents that protect anonymity as required by subdivision (a) may be inspected by any person or entity that is considering filing an amicus curiae brief. And access to records that are sealed or confidential under authority other than Welfare and Institutions Code section 827 is governed by rules 8.45–8.47, and the applicable statute, rule, sealing order, or other authority.

Rule 8.401 also allows the court to limit or prohibit admittance to oral argument. (Cal. Rules of Court, rule 8.401(c).)

2.3.3 Other privacy concerns

In addition, the rules prohibit a document filed in the reviewing court or an appellate opinion from including social security numbers or financial account numbers. (Cal. Rules of Court, rules 1.201, 8.41, & 8.70(c)(2).)

The reviewing court might also consider omitting from an opinion other information that could indirectly identify a person protected under rules 8.90 or 8.401, such as dates, addresses, street names, or names of a school or business.

2.4 Redaction of Trial and Appellate Court Records

2.4.1 Redaction of social security numbers and financial account numbers

California Rules of Court, rules 1.201 and 8.41 impose a duty on the parties or their attorneys to redact certain identifiers (i.e., social security numbers and financial account numbers) from documents filed with the court. It is the responsibility of the filers to exclude or redact the identifiers. The rules state that court clerks will not review each pleading or other paper for compliance with the requirements of the rules. In an appropriate case, the court on a showing of good cause may order a party filing a redacted document to file a *Confidential Reference List* (form MC-120) identifying the redacted information. This form is confidential.

2.4.2 Redaction of social security numbers from documents filed in dissolution of marriage, nullity of marriage, and dissolution cases

In general, petitioners and respondents may redact any social security number from any pleading, attachment, document, or other written materials filed with the court pursuant to a petition for dissolution of marriage, nullity of marriage, or legal separation. (Fam. Code, § 2024.5(a).) However, an abstract of support judgment, the form required pursuant to Family Code section 4014, or any similar form created for the purpose of collecting child or spousal support payments may not be redacted. (Fam. Code, § 2024.5(b).)

2.4.3 Abstracts of judgment or decrees requiring payment of money

The contents of an abstract of judgment or a decree requiring the payment of money are prescribed by Code of Civil Procedure section 674. The section provides that any judgment or decree shall contain *the last four digits* of the social security number and the driver's license number of the judgment debtor if they are known to the judgment creditor. (Code Civ. Proc., § 674(a)(6).)

2.4.4. Redaction of information about victims or witnesses in criminal cases

Law enforcement agencies are prohibited from disclosing the address and phone number of a witness or victim to an arrestee or potential defendant. (Pen. Code, § 841.5.) Similarly, defense counsel may not disclose the address or phone number of a victim or witness to the defendant, his or her family, or anyone else. (Pen. Code, § 1054.2) This information may be contained in police reports and other documents filed with the courts. It is recommended that courts require

that the addresses and phone numbers of victims and witnesses be redacted *before* any document containing that information is filed with the court or used in a judicial proceeding.

2.5 Destruction of Records

2.5.1 Destruction of criminal records

Records of arrest or conviction for marijuana-related offenses
These records include all offenses under Health & Safety Code sections 11357, 11360(b), and any records pertaining to the arrest and conviction of any person under 18 for violations under Health & Safety Code sections 11357 through 11362.9, except for section 11357.5. These records must be destroyed two years from either the date of conviction, the date of arrest if there was no conviction, or two years upon release from custody for persons incarcerated pursuant to the subdivision. (Health & Saf. Code, § 11361.5(a).) Records associated with violations of section 11357(d) shall be retained until the offender turns 18, at which point they are also to be destroyed. (Health & Saf. Code, § 11361.5(a).) This rule is subject to exceptions for records from judicial proceedings and records related to an offender's civil action against a public entity. (See Health & Saf. Code, § 11361.5(d).) Public agencies are prohibited from using information in records subject to destruction, even if they have not yet been destroyed. (Health & Saf. Code, § 11361.7(b).)

3. Access to Court Records

3.1 Public Access to Trial Court Records

Court records are presumed to be open, unless they are confidential as a matter of law or are sealed by court order. Confidential and sealed records are described in sections 2.1 and 2.2 and Appendix 1 of this resource guide.

3.1.1. Public access to paper court records at the courthouse

Paper records that are not confidential or sealed are available at the courthouse for public inspection and copying. These paper records in the past were often costly to locate, inspect, and copy. The difficulties and expenses involved in obtaining these paper records impeded public access but also provided an added level of privacy. This important practical effect of older court business practices was reflected in the "doctrine of practical obscurity," which recognized that obscurity could serve positive purposes with respect to protecting privacy interests.

Increasingly, courts are relying on records created and maintained in electronic format. These records can be searched and made accessible remotely. Thus, if the benefits of "practical obscurity" are to be preserved, this will no longer be a by-product of old paper-based business practices. Instead, providing privacy protection through differential ease of access to court records is a conscious policy choice and requires carefully planned implementation.

3.1.2 Electronic court records

Rules 2.500 through 2.507 of the California Rules of Court first adopted in 2002 are intended to provide the public with reasonable access to trial court records that are maintained in electronic form while protecting privacy interests. These rules prescribe how the public may access electronic records both at the courthouse and remotely.

- Rule 2.500. Statement of purpose
- Rule 2.501. Application and scope
- Rule 2.502. Definitions
- Rule 2.503. Public access
- Rule 2.504. Limitations and conditions
- Rule 2.505. Contracts with vendors
- Rule 2.506. Fees for electronic access
- Rule 2.507. Electronic access to court calendars, indexes, and registers of actions

The rules are not intended to give the public a right of access to any electronic record that they are not otherwise entitled to access in paper form, and do not create any right of access to records sealed by court order or confidential as a matter of law. These rules apply only to trial court records and only to access to court records by the public. They do not prescribe the access to court records by a party to an action or proceeding, by the attorney for a party, or by other persons or entities that may be entitled to such access by statute or rule.

3.1.3 Courthouse and remote access to electronic records

The law requires that court records maintained in electronic form "shall be made reasonably accessible to all members of the public for viewing and duplication as the paper records would have been accessible." (Gov. Code, § 68150(l).) Electronic access must be available at the courthouse and may also be made available remotely.

If a court maintains records in electronic form, it must provide a means for the public to view those records at the courthouse. "Unless access is otherwise restricted by law, court records maintained in electronic form shall be viewable at the courthouse*, regardless of whether they are also accessible remotely*." (Gov. Code, § 68150(*l*) (emphasis added).)

3.1.4 Access by type of record

There are some important restrictions on the records that may be made available remotely that do not apply to records at the courthouse. By rule of court, the following types of court records may not be made available remotely to the public:

(1) Records in a proceeding under the Family Code, including proceedings for dissolution, legal separation, and nullity of marriage; child and spousal support proceedings; child custody proceedings; and domestic violence prevention proceedings;
(2) Records in a juvenile court proceeding;
(3) Records in a guardianship or conservatorship proceeding;

(4) Records in a mental health proceeding;
(5) Records in a criminal proceeding;
(6) Records in a civil harassment proceeding under Code of Civil Procedure section 527.6;
(7) Records in a workplace violence prevention proceeding under Code of Civil Procedure section 527.8;
(8) Records in a private postsecondary school violence prevention proceeding under Code of Civil Procedure section 527.85;
(9) Records in an elder or dependent adult abuse prevention proceeding under Welfare and Institutions Code section 15657.03; and
(10) Records in proceedings to compromise the claims of a minor or a person with a disability.

(See Cal. Rules of Court, rule 2.503(c).) As this list indicates, many of the types of cases whose records that are by deliberate policy not made readily available remotely to the public involve sensitive private personal and financial information about children, elderly and disabled persons, and victims of crime and violence.

3.1.5 Remote access in high-profile criminal cases

Notwithstanding the general restriction against providing criminal records remotely in rule 2.503(c), under rule 2.503(e), the presiding judge or a designated judge may order the records of a high-profile criminal case to be posted on the court's website to enable faster and easier access to these records by the media and public. This rule specifies several factors that judges must consider before taking such action. One of the factors to be considered is: "The privacy interests of parties, victims, witnesses, and court personnel, and the ability of the court to redact sensitive personal information." (Cal. Rules of Court, rule 2.503(e)(1)(A).) Prior to posting, staff should, to the extent feasible, redact any confidential information contained in the court documents in accord with California Rules of Court, rule 2.503(e)(2). In addition, five days' notice must be provided to the parties and the public before the court makes a determination to provide electronic access under the rule. (Cal. Rules of Court, rule 2.503(e)(3).)

3.1.6 Case-by-case access

The court may only grant electronic access to an electronic record when the record is identified by the number of the case, the caption of the case, or the name of party, and only on a case-by-case basis. (Cal. Rules of Court, rule 2.503(f).)

3.1.7 Bulk data

The court may provide bulk distribution of only its electronic records of a calendar, index, or register of actions. "Bulk distribution" means distribution of all, or a significant subset, of the court's electronic records. (Cal. Rules of Court, rule 2.503(g).)

3.1.8 Access to calendars, indexes, and registers of action

Courts that maintain records in electronic form must, to the extent feasible, provide—both at the courthouse and remotely—access to registers of action, calendars, and indexes. (Cal. Rules of

Court, rule 2.503(b).) The minimum contents for electronically accessible court calendars, indexes, and registers of action are prescribed by rule. (See Cal. Rules of Court, rule 2.507(b).) This enables the public to obtain access to court records in an effective, meaningful way.

There is also a rule on what information must be *excluded* from court calendars, indexes, and registers of action; the information to be excluded includes social security numbers, financial information, arrest and search warrant information, victim and witness information, ethnicity, age, gender, government (i.e., military) identification numbers, driver's license numbers, and dates of birth. (See Cal. Rules of Court, rule 2.507(c).) Thus, the rule on court calendars, indexes, and registers of action explicitly recognizes the parties to lawsuits have important privacy rights that should not be compromised by easily and unnecessarily providing large amounts of private information.

3.2 Public Access to Records in the Courts of Appeal

Appellate court records are assumed to be open unless they are confidential as a matter of law or are sealed by court order. Confidential and sealed records on appeal are described in section 2.2 of this resource guide on rules 8.46 (sealed records) and 8.47 (confidential records). This section addresses other rules on access to appellate court records that are intended to protect persons' privacy interests.

3.2.1 The transition to electronic court records in the Courts of Appeal

Historically, paper records that are not confidential or sealed have been available at the appellate court for public inspection and copying. However, like the trial courts, the appellate courts are increasingly relying on records created and maintained in electronic rather than paper form. These electronic records can be made available remotely to the extent feasible and permitted by law.

The paper records used in the past were costly to locate, inspect, and copy. The difficulties and expense involved in obtaining these paper records impeded public access but also provided an added level of privacy. This important practical effect of older business practices was reflected in the doctrine of "practical obscurity," which recognized that obscurity could serve positive purposes with respect to protecting privacy interests. But as the appellate courts are shifting to electronic records, protecting privacy interests is no longer a by-product of paper-based business practices, but rather is the result of deliberate policy choices to provide differential access to electronic records. These policy choices are reflected in the rules of court on remote access to records.

3.2.2 Public access to electronic appellate court records

Public access to electronic appellate court records are governed by rules 8.80–8.85:

- Rule 8.80. Statement of purpose
- Rule 8.81. Application and scope
- Rule 8.82. Definitions

- Rule 8.83. Public access
- Rule 8.84. Limitations and conditions
- Rule 8.85. Fees for copies of electronic records

These rules, adopted effective January 1, 2016, are intended to provide the public with reasonable access to appellate records that are maintained in electronic form while protecting privacy interests. (Cal. Rules of Court, rule 8.80(a).)

The rules on remote access to electronic appellate court records are not intended to give the public a right of access to any electronic record that they are not otherwise entitled to access in paper form, and do not create any right of access to records sealed by court order or confidential as a matter of law. (Cal. Rules of Court, rule 8.80(c).) These rules apply only to records of the Supreme Court and the Courts of Appeal and only to access to records by the public. They do not prescribe the access to court records by a party to an action or proceeding, by the attorney for a party, or by other persons or entities that may be entitled to such access by statute or rule. (Cal. Rules of Court, rules 8.81(a)–(b).)

3.2.3 General right of access; remote access to the extent feasible

Rule 8.83 provides that all electronic records must be made reasonably available to the public in some form, whether in electronic or paper form, except sealed or confidential records. (Cal. Rules of Court, rule 8.83(a).)

Under rule 8.83(b) to the extent feasible, appellate courts will provide, both remotely and at the courthouse, the following records provided they are not sealed or confidential:

- Dockets or registers of actions
- Calendars
- Opinions
- The following Supreme Court records:
    - Results from the most recent Supreme Court conference
    - Party briefs in cases argued in the Supreme Court in the preceding three years
    - Supreme Court minutes from at least the preceding three years

(Cal. Rules of Court, rule 8.83(b)(1).)

If an appellate court maintains records in electronic form in civil cases in addition to the records just listed, electronic access to these records must be provided both at the courthouse and remotely, to the extent feasible, except those records listed in section 3.2.4 of this resource guide. (Cal. Rules of Court, rule 8.83(b)(2).)

3.2.4 Access by type of record

By rule, access to the electronic records listed below must be provided at the courthouse to the extent it is feasible to do so, but remote electronic access may not be provided to the following records:

- Any reporter's transcript for which the reporter is entitled to receive a fee; and
- Records other than those listed in rule 8.83(b)(1) in the following proceedings:
    - Proceedings under the Family Code, including proceedings for dissolution, legal separation, and nullity of marriage; child and spousal support proceedings; child custody proceedings; and domestic violence prevention proceedings;
    - Juvenile court proceedings;
    - Guardianship or conservatorship proceedings;
    - Mental health proceedings;
    - Criminal proceedings;
    - Civil harassment proceedings under Code of Civil Procedure section 527.6;
    - Workplace violence prevention proceedings under Code of Civil Procedure section 527.8;
    - Private postsecondary school violence prevention proceedings under Code of Civil Procedure section 527.85;
    - Elder or dependent adult abuse prevention proceedings under Welfare and Institutions Code section 15657.03; and
    - Proceedings to compromise the claims of a minor or a person with a disability.

(Cal. Rules of Court, rule 8.83(c).)

3.2.5 Remote electronic access permitted in extraordinary cases

The appellate rules on remote access include a provision that allows the presiding justice, or a justice assigned by the presiding justice, to exercise discretion to permit remote access by the public to all or a portion of the public court records in an individual case if (1) the number of requests for access to documents is extraordinarily high and (2) responding to those requests would significantly burden the operations of the court. Unlike the comparable trial court records rule (see Cal. Rules of Court, rule 2.503(c)) that is limited to extraordinary *criminal* cases, the appellate rule has no restriction on the type or types of cases to which it applies. (See Cal. Rules of Court, rule 8.83(d).)

The appellate rule does provide: "An individual determination must be made in each case in which such remote access is provided." (*Id.* at p. ____.) It also provides guidance on the relevant factors to be considered in exercising the court's discretion to provide remote access, including "[t]he *privacy interests* of parties, victims, witnesses, and court personnel, and the ability of the court to redact *sensitive personal information*." (Cal. Rules of Court, rule 8.83(d)(1) (emphasis added).)

In addition, the rule provides a specific list of the information that must be redacted from the records to which the court allows remote access in extraordinary cases, including driver's license numbers; dates of birth; social security numbers; criminal identification and information and national crime information numbers; addresses, e-mail addresses, and phone numbers of parties, victims, witnesses, and court personnel; medical or psychiatric information; financial information; account numbers; and other personal identifying information. (Cal. Rules of Court, rule 8.83(d)(2).)

3.2.6 Other limitations on remote access

Like the trial court rules, the appellate rules on remote access have certain additional safeguards that prevent remote access to court records from being used to thwart the privacy interests of individuals whose names appear in those records. Except for calendars, registers of action, and certain Supreme Court records, electronic access to records may be granted only if the record is identified by the number of the case, the caption of the case, the name of a party, the name of the attorney, or the date of oral argument, and only on a case-by-case basis. (Cal. Rules of Court, rule 8.83(e).) Also, bulk distribution is not permitted for most court records. (Cal. Rules of Court, rule 8.83(f).)

3.3 Remote Access to Trial Court Records by a Party, Party's Attorney, Court-Appointed Person, or Authorized Person Working in a Legal Organization or Qualified Legal Services Project

As described in section 3.1.2 of this resource guide, the Judicial Council adopted rules relating to remote public access to electronic trial court records in 2002. However, those rules apply only to access to electronic records by the public; they do not prescribe the access to those records by a party to an action or proceeding, by the attorney for a party, or by other persons or entities that may be entitled to such access by statute or rule. This gap in the law on remote access was addressed, effective January 1, 2019, by the adoption of a new set of rules on remote access to trial court records by a party, a party's attorney, a court-appointed person, or an authorized person working in a legal organization or qualified legal services project.

- Rule 2.515. Application and scope
- Rule 2.516. Remote access to extent feasible
- Rule 2.517. Remote access by a party
- Rule 2.518. Remote access by a party's designee
- Rule 2.519. Remote access by a party's attorney
- Rule 2.520. Remote access to persons working in the same legal organization as a party's attorney
- Rule 2.521. Remote access by a court-appointed person
- Rule 2.522. Remote access by persons working in a qualified legal services project providing brief legal services
- Rule 2.523. Identity verification, identity management, and user access
- Rule 2.524. Security of confidential information

- Rule 2.525. Searches and access to electronic records in search results
- Rule 2.526. Audit trails
- Rule 2.527. Additional conditions of access
- Rule 2.528. Termination of remote access

These rules (collectively the "party access rules") have been carefully written to balance increased access to records while protecting the reasonable privacy interests of parties doing business with the courts.

The party access rules are different from the public access rules (Cal. Rules of Court, rules 2.503–2.507) in significant ways. The rules on public access include some important limitations on remote access to protect the privacy interests of persons doing business with the courts. In particular, those rules contain provisions allowing public access to records only at the courthouse in certain types of cases, including criminal, family law, and violence restraining order cases. (See Cal. Rules of Court, rule 2.503(c).) The public may not have remote access to these records even if they are in electronic form. This policy of creating "practical obscurity" of certain types of records that often contain sensitive personal or financial information helps protect the privacy of many litigants from undue public scrutiny.

On the other hand, there are no privacy reasons to prevent a party, a party's attorney, or another person legally assisting a party from having remote access to the party's records. Preventing easy access to parties' own records does not promote parties' privacy interests while it makes it more difficult for them to conduct their business with the court. Hence, the party access rules (Cal. Rules of Court, rules 2.515–2.528) have been adopted to provide greater remote access to parties than to the public at large.

While the party access rules facilitate parties' access to their own records, they also include provisions that further protect the privacy interests of persons doing business with the courts. First, they do not provide unfettered remote access to records. Like all the rules in the chapter on Access to Electronic Trial Court Records, the party access rules do not give parties, their attorneys, legal organizations, or court-appointed persons any greater right of access to records than they would otherwise be legally entitled if they went to the courthouse to inspect records.[4]

The party access rules also contain other safeguards to protect the privacy of parties. For instance, parties' attorneys and others authorized to have remote access to a party's records must access records only for the purposes of their representation, may not distribute any electronic records obtained remotely for sale, must comply with all laws governing confidentiality of records, and must comply with any other terms required by the court. (See Cal. Rules of Court,

[4] In some instances, for security or policy reasons, a lesser amount of remote access has been deemed appropriate. The party designee rule, rule 2.518, allows a party to designate other persons to have remote access to electronic records in actions or proceedings in which that person is a party. However, a party's designee is not permitted remote access to criminal electronic records, juvenile justice electronic records, or child welfare electronic records. (Cal. Rules of Court, rule 2.518(b).) Also, parties may limit the scope of their designees' access. (*Id.* at p. ____.)

rules 2.519(d), 2.520(d), 2.521(c), 2.522(d).) The identity of persons accessing a party's records must be verified. (Cal. Rules of Court, rule 2.523.) Remote access to any confidential or sealed records must be provided through a secure platform and any electronic transmission of the information must be encrypted. (Cal. Rules of Court, rule 2.524(a).) The rules encourage courts to have the ability to generate audit trails (Cal. Rules of Court, rule 2.526) and require courts to impose reasonable conditions on remote access, for among other reasons, to preserve the integrity of their records and prevent the unauthorized use of information (Cal. Rules of Court, rule 2.527). Finally, the rules provide that remote access to records is a privilege and not a right, and that a court may, at any time and for any reason, terminate the permission it granted to a person to remotely access records. (Cal. Rules of Court, rule 2.528.)

3.4 Remote Access to Trial Court Records by Government Entities

In addition to providing expanded remote access for parties, their attorneys, and legal aid organizations, the Judicial Council adopted rules effective January 1, 2019, that provide greater remote access to electronic trial court records to government entities. (Cal. Rules of Court, rules 2.540–2.545.)

- Rule 2.540. Application and scope
- Rule 2.541. Identity verification, identity management, and user access
- Rule 2.542. Security of confidential information
- Rule 2.543. Audit trails
- Rule 2.544. Additional conditions of access
- Rule 2.545. Termination of remote access

These rules (collectively the "government access rules")—like the public access rules and the party access rules—have been carefully written to balance increased access with protecting the reasonable privacy interests of persons doing business with the courts.

Government entities are not given unfettered access to electronic records. Each entity is given remote access only to those types of electronic records that are necessary for the entity to carry out its legal responsibilities. (Cal. Rules of Court, rule 2.540(a).) With respect to the records to which it is allowed access, a government entity may be given the same level of remote access to electronic records as the government entity would be legally entitled if a person working for the government entity were to appear at the courthouse to inspect court records in that case type. If a court record is confidential by law or sealed by court order and a person working for the government entity would not be legally entitled to inspect the court record at the courthouse, the court may not provide the government entity with remote access to the confidential or sealed electronic record. (Cal. Rules of Court, rule 2.540(b)(2).)

Like the party access rules, the government access rules contain other safeguards to protect the privacy of parties. For instance, a court that allows government entities to have remote access to electronic records must have an identity verification method that verifies the identity of, and the

unique credentials of, each person who is permitted remote access. (Cal. Rules of Court, rule 2.541(b).) The government entity must approve the granting of access to that person, verify the person's identity, and provide the court with all the information it needs to authorize that person to have access to electronic records. (*Id.*, subd. (d)(1).) Remote access to any confidential or sealed records must be provided through a secure platform and any electronic transmission of the information must be encrypted. (Cal. Rules of Court, rule 2.542(a).) The rules encourage courts to have the ability to generate audit trails (Cal. Rules of Court, rule 2.543) and require courts to impose reasonable conditions on remote access, for among other reasons, to preserve the integrity of their records and prevent the unauthorized use of information (Cal. Rules of Court, rule 2.544). Finally, the rules provide that remote access to records is a privilege and not a right, and that a court may, at any time and for any reason, terminate the permission it granted to a person to remotely access records. (Cal. Rules of Court, rule 2.545.)

4. Financial Privacy in Civil and Criminal Cases

The constitutional right to privacy extends to one's personal financial information. (*Valley Bank of Nevada v. Superior Court* (1975) 15 Cal.3d 652, 656.) In court proceedings, this right of financial privacy is often protected by a particular statute or rule, as illustrated by the examples below. However, the right of financial privacy is not unlimited in scope. As discussed in the example in section 4.4 of this resource guide, a court has concluded that Family Code section 2014.6, the statute relied on by a participant in a divorce proceeding to close the records in that proceeding, was constitutionally overbroad. (See *In re Marriage of Burkle* (2006) 135 Cal.App.4th 1045, 1048.) Also, the Legislature has not made the Financial Privacy Act of 1977 applicable to the courts.

4.1 Fee Waivers

In civil cases, an application for an initial fee waiver, which contains personal financial information, is confidential. (Cal. Rules of Court, rule 3.54.) Only the court and authorized court personnel, persons authorized by the applicant, and persons authorized by order of the court may have access to the application. No person may reveal any information contained in the application except as authorized by law or order of the court. However, the order granting a fee waiver is not confidential.

4.2 Requests for Funds

In criminal cases, an indigent defendant's requests for funds for payment of investigators, experts, and others to aid in presenting or preparing the defense in certain murder cases is confidential. This exemption applies to defendants in capital and life-without-parole murder cases under Penal Code section 190.05(a). (Pen. Code, § 987.9.)

4.3 Criminal Defendant's Statement of Assets

Defendant's Statement of Assets (form CR-115) is a mandatory Judicial Council form. It is confidential in the same manner as probation reports. (See Pen. Code, § 1202.4.)

4.4 Information about the Financial Assets and Liabilities of Parties to a Divorce Proceeding

In *In re Marriage of Burkle* (2006) 135 Cal.App.4th 1045, the court considered the constitutionality of Family Code section 2014.6 that requires a court, on the request of a party to a divorce proceeding, to seal any pleading that lists and provides the location or identifying information about the financial assets of the parties. The court concluded that section 2024.6 is unconstitutional on its face. The court stated: "While the privacy interests protected by section 2014.6 may override the First Amendment right of access in an appropriate case, the statute is not narrowly tailored to serve overriding privacy interests. Because less restrictive means exist to achieve the statutory objective, section 2014.6 operates as an undue burden on the First Amendment right of public access to court records." (*Id*. at p. 1048.)

4.5 Information Privacy Act Not Applicable to the Courts

A general protection for individuals' privacy rights is contained in the Information Practices Act of 1977. However, recognizing the special role that courts play in conducting the people's business and the need for openness in conducting that business, the Legislature has expressly exempted the courts from the application of that act. (See Civ. Code, §1798.3(b)(1) [excluding from the definition of "agency" covered by the Information Privacy Act of 1977 "[a]ny agency established under Article VI of the California Constitution"—that is, the courts]).

4.6 Taxpayer Information

4.6.1 Confidential statements of taxpayer's social security numbers

Confidential Statements of Taxpayer's Social Security Number on mandatory Judicial Council forms (forms WG-021 and WG-025) for use in connection with wage garnishments are confidential.

4.6.2 Income tax returns in child support cases

In a proceeding involving child, family, or spousal support, if a judge finds that a tax return is relevant to disposition of the case, the tax return must be sealed and maintained as a confidential record of the court. (Fam. Code, § 3552.)

5. Privacy in Judicial Administrative Records

5.1 Public Access to Judicial Administrative Records (Cal. Rules of Court, rule 10.500)

Rule 10.500 provides for public access to "judicial administrative records" (Cal. Rules of Court, rule 10.500(c)(2)), which includes records of budget and management information related to the administration of the courts.

5.1.1 Policy

The rule is based on the California Public Records Act (Gov. Code, § 6250 et seq.) and is intended to be broadly construed to further the public's right of access. Unless otherwise

indicated, the terms used in this rule have the same meaning as under the Legislative Open Records Act (Gov. Code, § 9070 et seq.) and the California Public Records Act (Gov. Code, § 6250 et seq.) and must be interpreted consistently with the interpretation applied to the terms under those acts.

5.1.2 Scope of access

Rule 10.500 covers only judicial administrative records and does not govern the public's right to access "adjudicative records," which are "writings" prepared, used, or filed in a court proceeding, relate to judicial deliberation, or the assignment or reassignment of cases of justices, judges, subordinate judicial officers, and the assignment or appointment of counsel by the court. (Cal. Rules of Court, rule 10.500(c)(1).) As discussed above, adjudicative records, or court records, are presumptively public, subject to exceptions as discussed in sections 2 and 3 of this resource guide.

Disclosable judicial administrative records include any nonadjudicative records (writings) containing information that relates to "the conduct of the people's business that is prepared, owned, used, or retained by a court, regardless of the writing's physical form or characteristics." (Cal. Rules of Court, rule 10.500(c)(2).) However, personal information that is not related to the conduct of the people's business—or material falling under a statutory exemption (see below)—is not disclosable and can be redacted from the public records that are produced or presented for review. (See *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608.) This limitation on disclosure protects the privacy rights of government employees involved in creating public records.

Even if electronic communications are conducted on an agency employee or official's personal device or personal e-mail account, they are disclosable if they pertain to the people's business and are prepared, owned, used, or retained by a court or its personnel. (See Cal. Rules of Court, rule 10.500(b)(5); *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608.) On the other hand, if the documents relate to purely personal information, that content is not disclosable. Pursuant to a 10.500 request, courts may ask their employees to search their own files, segregate public records from personal records, and submit an affidavit with sufficient factual basis for determining whether the contested items are public records or personal materials. (*Id.* at p. _____.)

5.1.3 Exemptions and waiver of exemptions

Rule 10.500(f) provides 12 categories of records that a court may exempt from disclosure. For the purpose of this resource guide, the most important of these categories is the exemption for personnel, medical, or similar files, or other personal information whose disclosure would constitute an unwarranted invasion of personal privacy. (Cal. Rules of Court, rule 10.500(f)(3).) Some of the other exempt categories include records that relate to pending or anticipated claims or litigation to which a judicial branch entity or its personnel are parties (Cal. Rules of Court, rule 10.500(f)(2)); disclosure that is exempt or prohibited under state or federal law, including under the California Evidence Code relating to privilege or by court order in a court proceeding

(Cal. Rules of Court, rule 10.500(f)(5); records that would reveal or compromise court security or safety of court personnel (Cal. Rules of Court, rule 10.500(f)(6)); trade secrets, or confidential commercial or financial information (Cal. Rules of Court, rule 10.500(f)(10) and the catch-all exemption where, on the facts of a specific request, the public interest in withholding the record clearly outweighs the public interest in disclosure. (Cal. Rules of Court, rule 10.500(f)(12).)

Records relating to evaluations of complaints or investigations of judicial officers may be exempt under rule 10.500(f)(7). However, this exemption does not apply to settlement agreements entered into on or after January 1, 2010, for which public funds were spent in the settlement. Privacy concerns may justify redaction of names of complainants or witnesses and information that would identify such individuals. (Cal. Rules of Court, rule 10.500(f)(7).)

A judicial branch entity's or judicial branch personnel's disclosure of a judicial administrative record that is exempt from disclosure pursuant to rule 10.500(f) or law waives the exemptions as to that specific record. (Cal. Rules of Court, rule 10.500(h).) However, waiver does not apply to disclosures made in certain contexts as discussed in rule 10.500(h).

5.2 Criminal History Information

Summaries of criminal history information (also known as "rap sheets") are confidential. (*Westbrook v. Los Angeles* (1994) 27 Cal.App.4th 157, 164; Pen. Code, §§ 11105 and 13300–13326.) Public officials have a duty to preserve the confidentiality of a defendant's criminal history. (*Craig v. Municipal Court* (1979) 100 Cal.App.3d 69, 76.) Unauthorized disclosure of criminal history violates a defendant's privacy rights under the California Constitution. *(Ibid.)* Courts have upheld the confidentiality assigned to criminal history records. (See, e.g., *Westbrook, supra*, 27 Cal.App.4th 157 [unauthorized private company was denied access to municipal court information computer system].)

6. Privacy of Witnesses, Jurors, and Other Nonparties

6.1 Witness and Victim Information

6.1.1 Confidential information about witnesses and victims in police, arrest, and investigative reports

The court and the district attorney shall establish a mutually agreeable procedure to protect the confidential information of any witness or victim contained in police reports submitted to the court in support of a complaint, indictment, information, search warrant or arrest warrant. (Pen. Code, § 964.)

6.1.2 Victim impact statements

Victim impact statements filed with the court must remain under seal until imposition of judgment and sentence, except that the court, the probation officer, and counsel for the parties may review such statements up to two days before the date set for imposition of judgment and

sentence. (Pen. Code, § 1191.15(b).) Victim impact statements shall not be otherwise reproduced in any manner. (Pen. Code, § 1191.15(c).)

6.1.3 Information about victims, witnesses, and others

Law enforcement agencies are prohibited from disclosing the address and phone number of a witness or victim, to an arrestee or potential defendant. (Pen. Code, § 841.5.) Similarly, defense counsel may not disclose the address or phone number of a victim or witness to the defendant or his or her family. (Pen. Code, § 1054.2.) If this information is contained in documents filed with the courts, it should be redacted before the documents are filed.

6.1.4 Identity of sex offense victims

At the request of a victim of an alleged sexual offense, the court may order that the victim be treated anonymously. Upon a proper showing, the judge may order the identity of the victim in all records and during all proceedings to be either "Jane Doe" or "John Doe" if the judge finds that such an order is reasonably necessary to protect the alleged victim's privacy and that such measures will not unduly prejudice the prosecution or defense. (Pen. Code, § 293.5.)

6.2 Juror Information

6.2.1 Juror questionnaires of those jurors not called

The questionnaires of jurors not called to the jury box for voir dire are not open to the public. (*Copley Press, Inc. v. Superior Court* (1991) 228 Cal.App.3d 77, 87–88); but cf. *Bellas v. Superior Court of Alameda County* (2000) 85 Cal.App.4th 636, 645, fn. 6 [suggesting a contrary rule].)

6.2.2 Juror questionnaires answered under advisement of confidentiality

These records are not open to the public. (*Pantos v. City and County of San Francisco* (1984) 151 Cal.App.3d 258, 493–494 [jurors were told their answers on questionnaire were confidential].)

6.2.3 Confidentiality of requests for permanent medical excuse from jury service

Rule 2.1009, adopted effective January 1, 2019, provides a process for a person with a disability to request a permanent medical excuse from jury service in cases where the individual, with or without accommodations, including the provision of auxiliary aids or services, is incapable of performing jury service. The rule provides that the jury commissioner must keep confidential all information concerning the request for permanent medical excuse, including any accompanying request for disability-related accommodation, unless the applicant waives confidentiality in writing or the law requires disclosure. The applicant's identity and confidential information may not be disclosed to the public but may be disclosed to court officials and personnel involved in the permanent medical excuse process. (Cal. Rules of Court, rule 2.1009(c)(4).)

6.2.4 Sealed juror records in criminal courts

After the jury reaches a verdict in a criminal case, the court's record of personal juror identifying information (including names, addresses, and phone numbers) must be sealed. (Code Civ. Proc., § 237(a)(2).) This is often accomplished by replacing juror names with numbers. Indeed, that is how appellate court records contain the relevant information while conforming to the requirements of Code of Civil Procedure section 237. The defendant or his or her counsel can petition the court for access to this information to aid in developing a motion for a new trial or for any other lawful purpose. (Code Civ. Proc., § 206(f).)

6.2.5 Records of grand jury proceedings

Records of criminal grand jury proceedings are not open to the public unless an indictment is returned. If an indictment is returned, records of the grand jury proceeding are not open to the public until 10 days after a copy of the indictment has been delivered to the defendant or his or her attorney. (Pen. Code, § 938.1(b); *Daily Journal Corp. v. Superior Court* (1999) 20 Cal.4th 1117, 1124–1135.) If there is a "reasonable likelihood" that release of all or part of the transcript would prejudice the accused's right to a fair trial, a judge may seal the records. (Pen. Code, §§ 938.1, 929; see *Rosato v. Superior Court* (1975) 51 Cal.App.3d 190.) Notwithstanding the confidential status of a record, in civil grand juries, a judge may order disclosure of certain evidentiary materials, as long as information identifying any person who provided information to the grand jury is removed. (Pen. Code, § 929.) Also, after an indictment is returned, the judge may order disclosure of nontestimonial portions of the grand jury proceedings to aid preparation of a motion to dismiss the indictment. (*People v. Superior Court (Mouchaourab)* (2000) 78 Cal.App.4th 403, 434–436.)

6.2.6 Courts' inherent power to protect jurors

Courts may exercise their discretion to seal juror records where a "compelling interest" exists, such as protecting jurors' safety or privacy, protecting litigants' rights, or protecting the public from injury. (*Pantos v. City and County of San Francisco* (1984) 151 Cal.App.3d 258, 262; Code Civ. Proc., § 237; see *Townsel v. Superior Court* (1999) 20 Cal.4th 1084, 1091.) Thus, any juror information that a judge orders sealed is not open to the public.

7. Privacy Protection for Judicial Officers

7.1 Privacy Protection Guidance for Judicial Officers

Government Code section 6254.21 prohibits persons or businesses from publicly posting or displaying on the Internet the home address and phone number of a judicial officer, if he or she has made a written demand of that person or business not to disclose that information. Upon request of a California trial court judge, commissioner, or referee, the Judicial Privacy Protection Program of the Judicial Council's Security Operations unit will make such written demand to a predetermined list of major online data vendors. For further information, contact *securityoperations@jud.ca.gov*.

8. Court Websites: Best Practices

California courts use public websites extensively to conduct their business. All the trial and appellate courts have websites. These websites perform essential services. For example, they provide the public with key information about the courts. They provide access to local rules and forms needed for cases. They provide litigants with information about hearing dates and other calendar information. And they provide information to jurors about when and where to appear at court. Recently, websites have also become an increasingly important means for transacting business, such as paying for traffic tickets or scheduling hearings.

8.1 Privacy Statements

Like other institutions employing websites, courts need to advise the public and other users of the court's privacy policies with regard to the use of their websites. Courts need to inform users about the information that is collected. A privacy statement on the website will explain how the court gathers information, how it uses it, and how the court will protect users' privacy.

Each court will develop its own privacy statement relating to its website. For courts to consider as they develop or revise their statements, a sample privacy statement is attached as appendix 2 to this resource guide. In addition, a sample terms of use is attached as appendix 3 to this resource guide.

8.2 Retention and Tracking of User Information and Data

8.2.1 Use of cookies on court websites

To the extent that courts use cookies on their websites, it is advisable that they disclose such use in their privacy statements.

9. Video and Surveillance: Best Practices

9.1 Photographing, Recording, and Broadcasting in Court

California Rules of Court, rule 1.150 permits photographing, recording, and broadcasting of courtroom proceedings pursuant to a judge's ruling on media requests and sets forth factors to be considered by a judge in determining whether to grant media requests for such activity. A judge may not permit media coverage of: proceedings held in chambers; proceedings closed to the public; jury selection; jurors or spectators; or conferences between an attorney and a client, witness, or aide; between attorneys; or between counsel and the judge at the bench. (Cal. Rules of Court, rule 1.150(e)(6).)

9.2 Security Cameras in Public Areas

The Judicial Council has recommended best practices and policies for security camera recordings in the courthouse, covering the retention schedule, downloading, disclosures to the public or other parties; and retention schedules for downloaded recordings. (See Fact Sheet: Recommendations on Security Camera Recordings Policy and Best Practices (Oct. 2015).) Further questions may be directed to the Supervisor of the Judicial Council's Security Operations unit.

10. Privacy and Information Security: Best Practices

10.1 Information Systems Controls Framework Template

The Judicial Council has developed an Information Systems Control Framework. This document provides guidance for the courts in developing best practices regarding information system security. It is available to authorized court personnel through the Judicial Resources Network.

10.2 How to Use the Information Systems Control Framework

The Information Systems Control Framework sets forth principles for developing best practices for privacy and information security but is not intended to establish specific procedures. For further guidance on how to use the Information Systems Control Network, courts should contact the Judicial Council's Information Technology office.

Appendices

Appendix 1: Court records designated confidential by statute or rule
Appendix 2: Sample privacy statement for court websites
Appendix 3: Sample terms of use for court websites

APPENDIX 1—COURT RECORDS DESIGNATED CONFIDENTIAL BY STATUTE OR RULE

	GENERAL		
1	Information that must be excluded from court calendars, indexes, and registers of actions	Cal. Rules of Court, rule 2.507(c) Code Civ. Proc., § 527.6(v); Cal. Rules of Court, rule 3.1161	"The following information must be excluded from a court's electronic calendar, index, and register of actions: (1) Social security number; (2) Any financial information; (3) Arrest warrant information; (4) Search warrant information; (5) Victim information; (6) Witness information; (7) Ethnicity; (8) Age; (9) Gender; (10) Government-issued identification card numbers (i.e., military); (11) Driver's license number; and (12) Date of birth." Minor's name in protective order cases where a request for minor's information to be kept confidential has been granted.
2	Subpoenaed Records (Section 1560(d) of the Evidence Code)	Evid. Code, § 1560(d).	Unless the parties to the proceeding otherwise agree, or unless the sealed envelope or wrapper is returned to a witness who is to appear personally, the copy of the records shall remain sealed and shall be opened only at the time of trial, deposition, or upon direction of the judge.
3	Special Immigrant Juvenile Findings	Code Civ. Proc, § 155(c)	If not otherwise protected by state confidentiality laws, information regarding the child's immigration status must remain confidential and must be available for inspection only by the court, the child who is the subject of the proceeding, the parties, the attorneys for the parties, the child's counsel, and the child's guardian.
	CIVIL LAW		
1	Request for accommodations by persons with disabilities	Cal. Rules of Court, rule 1.100(c)(4)	"The court must keep confidential all information of the applicant concerning the request for accommodation"; this includes the identity of the applicant, all medical information, and all communications from the applicant.
2	Application to proceed *in forma pauperis* (i.e.,	Cal. Rules of Court, rule 3.54	Access to the application and to the information in the application is limited to court and authorized persons only.

	application for waiver of fees and costs)		
3	Documents filed under seal (per court order)	Cal. Rules of Court, rule 2.550	A sealed record is a record that by court order is not open to inspection by the public.
4	Documents that are the subject of a motion to seal	Cal. Rules of Court, rule 2.551(b)	A party requesting that a record be filed under seal must lodge it with the court. Pending the court's ruling, the lodged record will be conditionally under seal. In addition, unredacted memoranda and other documents filed in support of and opposition to the motion must be lodged, conditionally under seal, with redacted versions filed publicly.
5	Confidential documents that may be the subject of a motion to seal	Cal. Rules of Court, rule 2.551(b)	A party that intends to file documents that are subject to a confidentiality agreement or protective order, but does not intend to request that they be filed under seal, must lodge the records, as well as any pleadings or other documents that disclose the contents of the records, with the court. Redacted versions of those documents are filed publicly. Unredacted records are lodged, with notice to parties that the records will be placed in the court file unless a motion to seal is filed and granted. The documents are conditionally under seal for 10 days. If a party moves to seal the documents within that period, or longer if extended by the court, the documents remain conditionally under seal pending the court's ruling on the motion.
6	Records examined by the court in confidence during a confidential *in camera* proceeding in which a party is excluded	Cal. Rules of Court, rule 2.585	Such records must be filed under seal and must not be disclosed without court order.
7	Records in unlawful detainer actions	Code Civ. Proc., § 1161.2 (a)	For 60 days after the complaint has been filed, access is limited to specific enumerated persons set forth in the statute, including parties and residents of the property. If the defendant prevails in the action within 60 days of the filing of the complaint, access is permanently limited to those specific enumerated persons. An exception excludes records of mobile home park tenancies from this code section; those records are not confidential. In addition, effective January 1, 2011, access to court records is permanently limited to those specified enumerated persons in unlawful detainer cases involving residential property based on section 1161a (holding over after sale under execution, mortgage, or trust deed [foreclosures]) as indicated in the caption of the complaint, unless judgment has been entered, after a trial, for the plaintiff and against all defendants.
8	Records of actions brought under False Claims Act (i.e., *qui tam* actions)	Gov. Code, § 12652(c)(2); Cal. Rules of Court, rule 2.570	A complaint that is filed by a private person is automatically filed under seal (no sealing order required) for 60 days, longer if extended by the court. During that period, all records in the action are filed under seal and are confidential until the seal is lifted. Access to sealed records is limited to specifically enumerated parties.
9	All information regarding complaints about the conduct of mediators in court-connected mediation programs	Cal. Rules of Court, rule 3.867	All communications, inquiries, complaints, investigations, procedures, deliberations, and decisions about the conduct of a mediator under rule 3.865 must occur in private and must be kept confidential. The presiding judge or a person designated by the presiding judge for this purpose may, at his or her discretion, authorize the disclosure of information or records concerning rule 3.865 complaint procedures that do not reveal any mediation communications.

10	Confidential name change because of domestic violence, stalking, or sexual assault	Code Civ. Proc., § 1277; Gov. Code, § 6205 et seq.	The Secretary of State shall keep confidential name changes because of domestic violence, stalking, sexual assault, or human trafficking. Petitions for change of name because of domestic violence, stalking, or sexual assault shall, in lieu of reciting the proposed name, state that the proposed name is confidential and will be on file with the Secretary of State.
11	All certificates of corroborative fact filed in a civil action based on childhood sexual abuse	Code Civ. Proc., § 340.1(p)	Confidential from the public *and all parties* (except the plaintiff).
12	Social security numbers (SSNs)	Cal. Rules of Court, rule 2.507(c)(1); see Gov. Code, § 68107	California Rules of Court, rule 2.507(c) requires that SSNs, along with other personal data, be excluded from any electronic court calendar, index, or register of action. (See the criminal law section below for list of all categories of data to be excluded.) Section 68107 of the Government Code specifically addresses court collection efforts in criminal cases but does state that an SSN obtained for that purpose "is not a public record and shall not be disclosed except for collection purposes."
13	Records in an action in which prejudgment attachment is sought	Code Civ. Proc., § 482.050; Cal. Rules of Court, rule 2.580	Upon request by the plaintiff at the time the complaint is filed, the clerk of the court shall not make the records in the action or the fact of the filing of the action available to the public for as long as 30 days, or sooner upon the filing of the return of service of the notice of hearing and any temporary protective order or writ of attachment. Notwithstanding the above, the clerk shall make the entire file available to any named party or his or her attorney.
14	Information about minors in protective orders	Code Civ. Proc., § 527.6(v); Cal. Rules of Court, rule 3.1161	Upon request, a minor or minor's legal guardian can ask the court to make information relating to a minor confidential when issuing a civil harassment restraining order. If the court orders information to be made confidential, the version of the document in the public file must be redacted, and an unredacted version must be maintained in a confidential file. Any documents filed in the case after the court has made an order for confidentiality must be filed with a cover sheet (form CH-175) to indicate that the case involves confidential information.
15	Information, including name, of party in an action for distribution of sexually explicit material under Civil Code §1708.85	Code Civ. Proc., § 1708.85	California Civil Code Section 1708.85 provides an individual with the right to bring a private cause of action against any person who, without consent, intentionally distributes nude or sexual imagery of that individual where the person should have known that there was a reasonable expectation that the imagery would remain private and the individual suffers damages (including, for example, loss of reputation, shame, hurt feelings and damage to profession or occupation). The action may be brought using a pseudonym, plaintiff shall file with the court a confidential information form and the court shall keep the plaintiff's name and excluded or redacted characteristics confidential. All court decisions, orders, petitions, and other documents, including motions and papers filed by the parties, shall be worded so as to protect the name or other identifying characteristics of the plaintiff from public revelation so these documents are not confidential.
16	Capacity Declarations (forms GC-335 and GC-335A)	Civ. Code, § 56.13	If these forms are filed with or as attachments to form GC-312, they are confidential under section 1821(a). If filed separately, they are confidential under section 56.13 of the Civil Code.

	CRIMINAL		
1	Sealed juror identification information	Pen. Code, § 95.2	This section makes it a misdemeanor for any person, without court authorization and juror consent, to intentionally provide a defendant juror identification information sealed by the court under Code of Civil Procedure section 237, where that information is in turn used to commit certain crimes.
2	Criminal juror identifying information	Code Civ. Proc., § 237	Upon the recording of a jury's verdict in a criminal jury proceeding, the court's record of personal juror identifying information of trial jurors shall be sealed until further order of the court. Please see criminal section (below) for further details.
3	Sex offense victim address information	Pen. Code, § 293	Allows victims of sex offenses to request that their names remain private and prohibits disclosure of their address information (with enumerated exceptions).
4	All records containing the identity of an alleged sex offense victim	Pen. Code, § 293.5	The court, at the request of the alleged victim, may order the identity of the alleged victim in all records and during all proceedings to be either Jane Doe or John Doe, if the court finds that such an order is reasonably necessary to protect the privacy of the person and will not unduly prejudice the prosecution or the defense.
5	Obscene matter	Pen. Code, § 312	When a conviction becomes final, the court may order any obscene matter or advertisement in its possession or under its control to be destroyed.
6	Two specific records involving victims of identity theft: (1) The police report generated on behalf of the victim under Pen. Code, § 530.6; and (2) The victim's written request for records regarding the unauthorized use of the victim's identity made upon the person or entity in possession of the records	Pen. Code, § 530.8(d)(1)	The aforementioned documents "shall be kept confidential by the court" pending the victim's petition to receive information pertaining to the unauthorized use of his or her identity.
7	Applications and orders regarding wiretaps	Pen. Code, § 629.66	Applications and orders for wiretaps "shall be sealed by the judge" and "shall be disclosed only upon a showing of good cause before a judge."
8	Peace or custodial officer personnel records	Pen. Code, § 832.7	Peace officer and/or custodial officer personnel records, and records maintained by any state or local agency, or information obtained from these records, are confidential and shall not be disclosed in any criminal or civil proceeding except by discovery pursuant to Evidence Code sections 1043 and 1046.
9	Records of juvenile arrests for misdemeanors	Pen. Code, § 851.7	Any person previously arrested for a misdemeanor while a minor may petition the court for an order sealing the records in the case, including any records of arrest and detention.
10	Records of arrest	Pen. Code, § 851.8	This section sets forth various provisions for sealing and destroying the arrest records of persons subsequently deemed "factually innocent."

11	Criminal case records following acquittal	Pen. Code, § 851.85	A judge presiding at a trial resulting in an acquittal may order that the records in the case be sealed, including any record of arrest or detention, whenever it appears to the judge that the defendant was "factually innocent."
12	Records of arrest following finding of factual innocence	Pen. Code, § 851.86	Where defendant's conviction is set aside based on a determination that he or she was factually innocent of the charge, the judge shall order that the records in the case be sealed, including any record of arrest or detention, upon the written or oral motion of any party in the case or the court, and with notice to all parties to the case.
13	Records of arrest and court files after completion of diversion program	Pen. Code, § 851.87	A person who successfully completes a prefiling diversion program may petition the court to seal records pertaining to an arrest after successful completion of the diversion program, and the court may order those records sealed as described in Penal Code section 851.92. The sealing order has specified limitations.
14	Arrest records and related court files and records, including court indexes and registers of actions	Pen. Code, § 851.90	Whenever a case is dismissed following a defendant's successful completion of drug diversion under Penal Code section 1000 et seq., the court may order those records pertaining to the arrest to be sealed as described in Section 851.92, upon either the written or oral motion of any party in the case or upon the court's own motion, with notice to all parties. The sealing order has specified limitations.
15	Records of arrest that did not result in conviction	Pen. Code, § 851.91	A person who suffered an arrest that did not result in a conviction may petition the court to have the arrest and related records sealed, as described in Penal Code section 851.92. The arrest and person must meet specified eligibility requirements. A court may grant relief as a matter of right or in the interests of justice if the arrest involves domestic violence, child abuse, or elder abuse. The sealing order has specified limitations.
16	Sealed arrest records under Pen. Code, §§ 851.87, 851.91, 1000.4, and 1001.9	Pen. Code, § 851.92	When a court issues an order to seal an arrest, the court shall provide copies to the person whose arrest was sealed, the prosecuting attorney, and relevant law enforcement agencies. The court shall furnish a disposition report to the Department of Justice. Any court records related to the sealed arrest shall be stamped "ARREST SEALED: DO NOT RELEASE OUTSIDE OF THE CRIMINAL JUSTICE SECTOR" with the date of the sealing and the relevant section pursuant to which the arrest was sealed. This stamp and note shall be on all master court dockets, digital or otherwise, relating to the arrest.
17	Grand jury reports containing unprivileged materials and findings	Pen. Code, § 929	This section sets forth the circumstances under which a grand jury may make available to the public certain information relied on for its "final report" and provides that a judge may require redaction or "masking" of any part of the evidentiary material, findings, or other information to be released, including "the identity of witnesses and any testimony or materials of a defamatory or libelous nature."
18	Personal information regarding witnesses or victims	Pen. Code, § 964	The court and district attorney shall establish a mutually agreeable procedure to protect the confidential personal information of any witness or victim contained in police reports submitted to a court in support of a complaint, indictment, information, search warrant and/or arrest warrant.
19	Financial statements and/or other financial information of criminal defendants	Pen. Code, § 987(c)	To determine if a defendant qualifies for a public defender, the court may require the defendant to file a financial statement with the court under penalty of perjury, which must remain "confidential and privileged" unless certain, enumerated exceptions apply.

20	Applications by indigent defendants for funds for investigators and/or experts	Pen. Code, § 987.9	"The fact that an application has been made shall be confidential and the contents of the application shall be confidential." (See subd. (d) for exception(s).)
21	Records in substance abuse cases	Pen. Code, § 1000.4	Upon successful completion of a pretrial diversion program, the arrest upon which defendant was diverted shall be deemed never to have occurred and the court may issue an order to seal the records pertaining to the arrest as described in Section 851.92. The sealing order has specified limitations.
22	Arrest records in mental disorder diversion cases	Pen. Code, § 1001.36	Upon successful completion of a pretrial diversion program, the court shall order access to the record of arrest restricted in accordance with Penal Code section 1001.9 (see below).
23	Records in misdemeanor diversion	Pen. Code, § 1001.9	A person who successfully completes a prefiling diversion program may petition the court to seal records pertaining to an arrest after successful completion of the prefiling diversion program, and the court may order those records sealed as described in Penal Code section 851.92. The sealing order has specified limitations.
24	Records of arrest and court records following dismissal pursuant to Pen. Code, § 1170.9	Pen. Code, § 1170.9(h)(4)(D)	When a dismissal pursuant to Penal Code section 1170.9 is granted (criminal offenses related to trauma, injury, substance abuse, or mental health problems stemming from military service), the court has the discretion to order the sealing of police records of the arrest and court records of the dismissed action, thereafter viewable by the public only in accordance with a court order.
25	Specified victim statements, including statements in lieu of personal appearance	Pen. Code, § 1191.15	With certain, enumerated exceptions, "[w]henever a written, audio, or video statement or statement stored on a CD-ROM, DVD, or other medium is filed with the court, it shall remain sealed until the time set for imposition of judgment and sentence … ."
26	Results of mandatory AIDS testing pursuant to Pen. Code, §§ 1202.1, 1524.1	Pen. Code, §§ 1202.1,1524.1	HIV test results ordered of defendants charged with certain crimes enumerated in Penal Code sections 1202.1 and 1524.1 shall be treated as confidential by the local health officer and victim.
27	Results of mandatory AIDS testing under former Pen. Code, § 1202.6(f)	Former Pen. Code, § 1202.6(f)*	With certain, specified exceptions, the results of mandatory AIDS testing for defendants convicted of violating Penal Code section 647(b) "shall be confidential." (*Former Penal Code section 1202.6 was repealed and replaced by a new Penal Code section 1202.6 that no longer requires mandatory AIDS testing, as of January 1, 2018 (Stats. 2017, ch. 537, § 16).)
28	Diagnostic reports from the Director of the Department of Corrections	Pen. Code, § 1203.03	The reports from the Director of the Department of Corrections concerning defendants considered for "treatment services as can be provided at a diagnostic facility" shall "be served only upon the defendant or his counsel, the probation officer, and the prosecuting attorney by the court receiving such report … [and] … the information contained therein shall not be disclosed to anyone else without the consent of the defendant. After disposition of the case, all copies of the report, except the one delivered to the defendant or his counsel, shall be filed in a sealed file … ."
29	Probation reports filed with the court	Pen. Code, § 1203.05	This section sets forth limitations on who may inspect probation reports filed with the court, and when those reports may be inspected.
30	Records of misdemeanor convictions of minors	Pen. Code, § 1203.45	With a few stated exceptions and/or limitations, this section allows for the sealing of "the record of conviction and other official records in the case, including records of arrests resulting in the

			criminal proceeding and records relating to other offenses charged in the accusatory pleading, whether defendant was acquitted or charges were dismissed."
31	Records in grant of petition under Welf.& Inst. Code, § 781	Pen. Code, § 1203.47	If a petition is granted under Welfare and Institutions Code section 781, all records relating to the violation or violations of subdivision (b) of Section 647 or of Section 653.22, or both, shall be sealed pursuant to Section 781 of the Welfare and Institutions Code.
32	Three specific sets of records: (1) Any written report of any law enforcement officer or witness to any offense; (2) Any information reflecting the arrest or conviction record of a defendant; and (3) Any affidavit or representation of any kind, verbal or written	Pen. Code, § 1204.5	With certain, specified exceptions, this section prohibits a judge from reading or considering the above records without the defendant's consent given in open court.
33	State summary criminal history information (i.e., rap sheets)	Pen. Code, § 11142	Makes it a misdemeanor for a person authorized to receive state criminal history information to furnish it to an unauthorized person.
34	State summary criminal history information (i.e., rap sheets)	Pen. Code, § 11143	Generally makes it a misdemeanor for any person to improperly buy, receive, or possess criminal history information.
35	State summary criminal history information (i.e., rap sheets)	Pen. Code, § 11144	Prescribes when information from criminal histories may be disseminated without violation.
36	Local summary criminal history information (i.e., rap sheets)	Pen. Code, § 13300	Prescribes who may have access to local summary criminal history information.
37	Local summary criminal history information (i.e., rap sheets)	Pen. Code, § 13302	Makes it a misdemeanor for a criminal justice agency employee to improperly furnish a person's criminal history to an unauthorized recipient.
38	Local summary criminal history information (i.e., rap sheets)	Pen. Code, § 13303	Makes it a misdemeanor for an authorized recipient of criminal history information to improperly furnish it to an unauthorized recipient.
39	Local summary criminal history information (i.e., rap sheets)	Pen. Code, § 13304	Generally makes it a misdemeanor for any person to improperly buy, receive, or possess criminal history information.

40	Local summary criminal history information (i.e., rap sheets)	Pen. Code, § 13305	Prescribes when information from criminal histories may be disseminated without violation.
41	Court records and documents relating to search warrants	Pen. Code, § 1534	"The documents and records of the court relating to the warrant need not be open to the public until the execution and return of the warrant or the expiration of the 10-day period after issuance. Thereafter, if the warrant has been executed, the documents and records shall be open to the public as a judicial record."
42	Peace and custodial officer personnel records	Evid. Code, §§ 1043, 1045–1047	In conjunction with Penal Code section 832.5, these sections restrict how the court may review and disclose peace officer personnel records.
43	Records of specified marijuana convictions	Health & Saf. Code, § 11361.8(e), (f)	Upon application by the defendant, specified marijuana convictions meeting the requirements of Section 11361.8(e) shall be redesignated by the court as a misdemeanor or infraction or dismissed and the conviction sealed as legally invalid under the Control, Regulate and Tax Adult Use of Marijuana Act.
44	Automatic reduction or dismissal of specified marijuana convictions	Health & Saf. Code, § 11361.9	On or before July 1, 2020, the prosecution shall inform the court if they are or are not challenging a particular recall or dismissal of sentence; if the prosecution does not challenge the recall or dismissal of sentence, the court shall reduce or dismiss and seal the conviction pursuant to Section 11361.8.
45	HIV test results under Health & Saf. Code, §§ 121055, 121056, and 121060	Health & Saf. Code, § 121065	If a court orders HIV tests under Health and Safety Code sections 121055, 121056, and 121060, the court shall order that all persons receiving the results maintain the confidentiality of personal identifying data related to the test results, except as necessary for medical or psychological care or advice.
46	Exhibits	Cal. Rules of Court, rule 2.400(c)(1)	"The clerk must not release any exhibit except on order of the court."
47	Reporters' transcripts of *Marsden* hearings	Cal. Rules of Court, rule 8.328	"The reporter's transcript of any hearing held under *People v. Marsden* (1970) 2 Cal.3d 118 must be kept confidential."
48	Records on appeal	Cal. Rules of Court, rule 8.610	This rule provides for confidentiality of certain records on appeal.
49	Juvenile court records	Welf. & Inst. Code, § 781	This section sets forth the procedure for—and consequences of—petitions for sealing juvenile records.
50	Determination of an ability to pay traffic and other infractions	TR-320/CR-320	This form is confidential.
	PROBATE		
1	Confidential Guardian Screening Form (form GC-212	Cal. Rules of Court, rule 7.1001(c)	This mandatory Judicial Council form regarding the proposed guardian is confidential. It is used by the court and by persons or agencies designated by the court to assist in determining whether a proposed guardian should be appointed. (Cal. Rules of Court, rule 7.1001(c).)
2	Confidential Supplemental Information (form GC-312)	Prob. Code, § 1821(a)	This form regarding the proposed conservatee is confidential. It shall be separate and distinct from the form for the petition. The form shall be made available only to parties, persons given notice of the petition who have requested this supplemental information, or who have appeared in the

			proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, § 1821(a).)
3	Confidential Conservator Screening Form (form GC-314)	Cal. Rules of Court, rule 7.1050(c)	This mandatory Judicial Council form is confidential. (Cal. Rules of Court, rule 7.1050(c).)
4	Reports regarding proposed guardianship or conservators	Prob. Code, §§ 1513, 1826	An investigative report created pursuant to Probate Code section 1513 concerning a proposed guardianship is confidential and available only to parties served in the action or their attorneys (generally, parents, legal custodian of child). An investigative report created pursuant to Probate Code section 1826 regarding the proposed conservatee is confidential and available only to those persons specified by statute. Under the statute, the reports on proposed conservatees shall be made available only to parties, persons given notice of the petition who have requested the report, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the reports on guardianships and conservatorships exclusively to persons entitled thereto. (Prob. Code, §§ 1513(d) & 1826(n).)
5	Investigator's review reports in conservatorships	Prob. Code, § 1851	These reports are confidential. The information in the reports may be made available only to parties, persons identified in section 1851(b), persons given notice who have requested the report or appeared in the proceeding, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interests of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, §§ 1851(b) & (e).) Subdivision (b) provides for special restricted treatment of attachments containing medical information and confidential criminal information from CLETS. Although the attachments are not mentioned in (e), it is recommended, to be consistent with (b), that they be treated as confidential except to the conservator, conservatee, and their attorneys.
6	Certification of counsel of their qualifications (form GC-010) and certification of completion of continuing education (form GC-011)	Cal. Rules of Court, rule 7.1101	The forms state that they are "confidential for court use only." They are governed by rule 7.1101, which states only that the certifications must be submitted to the court but not lodged or filed in a case file.
7	*Confidential Guardianship Status Report* (form GC-251)	Prob. Code, § 1513.2(c)	A report submitted by a court-appointed guardian is confidential and must be made available only to persons served in the proceedings or their attorneys.
8	Report of an investigation in response to an order provisionally granting a petition to transfer a	(Prob. Code, §§ 1851.1(d), 2002.)	The report of an investigation in response to an order provisionally granting a petition to transfer a conservatorship from another state is also confidential.

	conservatorship from another state		
	FAMILY		
1	Family conciliation court records	Fam. Code, § 1818	Records and proceedings in Family Conciliation Courts are confidential.
2	**Psychological evaluations of children and recommendations regarding custody and visitation; confidentiality; exceptions**	Fam. Code, § 3025.5	Any psychological evaluations of children or recommendations regarding custody and visitation proceedings that are submitted to the court shall remain confidential and may be disclosed only to certain people (parties, attorneys, law enforcement officers, judicial officers, family law facilitator).
3	Controlled substances or alcohol abuse testing of persons seeking custody or visitation; grounds for testing; confidentiality of results; penalties for unauthorized disclosure	Fam. Code, § 3041.5	Test results for controlled substances or alcohol abuse of persons seeking custody or visitation shall remain confidential and maintained in a sealed record in the court file. These results may not be released to anyone except the court, the parties, their attorneys, the Judicial Council, and any other person whom the court expressly grants access by written order made with prior notice to all parties.
4	Child custody evaluations; reports; confidentiality, and use	Fam. Code, § 3111	Child custody evaluation reports are available only to the court, the parties, and their attorneys.
5	Confidentiality of mediation proceedings	Fam. Code, § 3177	Mediation proceedings shall be held in private and shall be confidential. All communications, verbal or written, from the parties to the mediator made in the proceeding are official information within the meaning of Evidence Code section 1040.
6	Recommendations to court as to custody or visitation, investigation, restraining orders, and minor's counsel	Fam. Code, §§ 3183, 3184	Child custody recommending counselor may submit recommendations to the court as to the custody of or visitation with the child except as is provided in Family Code section 3188.
7	Confidential mediation program	Fam. Code, § 3188 (not operative pursuant to subd. (b) because of lack of budget allocation)	In a court that adopts a confidential mediation program, the mediator may not make a recommendation as to custody or visitation to anyone other than the disputing parties, exceptions noted in statute.
8	State and federal income tax returns; submission to court; examination and discovery	Fam. Code, § 3552	Tax returns are confidential court records.
9	Criminal history search; prior restraining orders	Fam. Code, § 6306	Information found in a search for person to restrained's prior criminal history must be kept confidential in certain circumstances (see subd. (a)); the information may be reviewed or disclosed to certain persons involved in the case.

10	Hearing or trial in closed court; papers and records, inspection	Fam. Code, § 7643	With the exception of the final judgment, records in Uniform Parentage Act proceedings are closed to the public.
11	Inspection of petitions, reports, and court records and briefs	Fam. Code, § 7805	A petition to terminate parental rights or a report of the probation officer or county social services department may be inspected only by the following persons: (1) Court personnel. (2) The child who is the subject of the proceeding. (3) The parents or guardian of the child. (4) The attorneys for the parties. (5) Any other person designated by the judge. On appeal to the court of appeal or the Supreme Court, the court record and briefs filed by the parties may be inspected only by the following persons: (1) Court personnel. (2) A party to the proceeding. (3) The attorneys for the parties. (4) Any other person designated by the presiding judge of the court before which the matter is pending. The court and/or probation officer may provide information in a termination of parental rights case, if it is believed that the welfare of the child will be promoted, to any of the following: (1) The State Department of Social Services. (2) A county welfare department. (3) A public welfare agency. (4) A private welfare agency licensed by the State Department of Social Services.
12	Privacy rights; confidentiality of records	Fam. Code, § 17212	All child and spousal support enforcement records are confidential and shall not be released for any purpose not directly connected with the administration of the child and spousal support enforcement program. Information regarding the location of one party or the child shall not be disclosed to another party, or to the attorney of any other party, if a protective order has been issued by a court or administrative agency with respect to the party, a good cause claim under Section 11477.04 of the Welfare and Institutions Code has been approved or is pending, or the public agency responsible for establishing paternity or enforcing support has reason to believe that the release of the information may result in physical or emotional harm to the party or the child. The information shall be omitted from any pleading or document to be submitted to the court. A proof of service filed by the local child support agency shall not disclose the address where service of process was accomplished. Instead, the local child support agency shall keep the address in its own records. Authorized disclosures are described in the statute.
13	Inspection of documents; authorization; fee; deletion of	Fam. Code, § 9200	Documents relating to adoption proceedings are confidential and may be seen only by the parties, their attorneys, and the child welfare agency. The name and identifying information regarding the

	identification of birth parents; certificate of adoption		child's birth parents shall not be disclosed to anyone receiving the documents unless the adoption is by a stepparent or second-parent.
14	Confidentiality	Cal. Rules of Court, rule 3.854	This covers guidelines for mediators with respect to confidentiality.
15	Court-connected child custody mediation	Cal. Rules of Court, rule 5.210(d)(1)(F) & (G), (h)(3)	Mediators must protect the confidentiality of the parties and the child by not releasing information about the case except as is authorized.
16	Domestic violence protocol for Family Court Services	Cal. Rules of Court, rule 5.215(e), (f)(2), (g)(3)	Family Court Services (FCS) staff must make reasonable efforts to keep contact/identifying information confidential on FCS documents when dealing with domestic violence cases.
17	Information about minors in Domestic Violence Prevention Act matters	Family Code § 6301.5; Cal. Rules of Court, rule 5.382	Upon request, a minor or minor's legal guardian can ask the court to make information relating to a minor confidential when issuing a domestic violence protective order. If the court orders information to be made confidential, the version of the document in the public file must be redacted, and an unredacted version must be maintained in a confidential file. Any documents filed in the case after the court has made an order for confidentiality must be filed with a cover sheet (form DV-175) to indicate that the case involves confidential information.
	JUVENILE		
1	Information available for juvenile court proceedings regarding best interest of child; confidentiality	Welf. & Inst. Code, § 204	Any information provided to the court under this section to make a determination regarding the best interest of the child may be released to authorized persons; however, if the information is confidential, it shall remain confidential and not be released to others except as is necessary.
2	Admission of public and persons having interest in case; confidentiality of name; disclosure of court documents	Welf. & Inst. Code, § 676	Unless requested by the minor, the public shall not be admitted to a juvenile court hearing; the name of a minor found who has committed one of the juvenile offenses listed in Welfare and Institutions Code section 676 shall not be confidential unless the court, for good cause, so orders; when a petition is sustained for any of these offenses, the charging petition, the minutes of the proceeding, and the orders of adjudication and disposition of the court contained in the court file may be available for public inspection; the probation officer or any party may petition the juvenile court to prohibit disclosure to the public of any file or record.
3	Records related to any petition dismissed under Welf. & Inst. Code, § 786	Welf. & Inst. Code, § 786	The court must order sealed all records related to any petition dismissed under Welfare and Institutions Code section 786 that are in the custody of the juvenile court, law enforcement agencies, the probation department, and the Department of Justice. The procedures for sealing these records are stated in Welfare and Institutions Code section 786.
4	Juvenile court record	Welf. & Inst. Code, § 825	The order and findings of the superior court in each case under the provisions of this chapter shall be entered in a suitable book or other form of written record that shall be kept for that purpose and known as the "juvenile court record."
5	Release or destruction of court record; reproduction	Welf. & Inst. Code, § 826 et seq.	The juvenile court records include all records and papers, any minute book entries, dockets, and judgment dockets. These records may be destroyed after five years from the date on which

			jurisdiction of the juvenile court is terminated; they must be destroyed by order of the court under various circumstances, outlined below; records may also be released to the juvenile who is the subject of the proceeding.
6	Juvenile case file inspection; confidentiality; release; probation reports; destruction of records; liability	Welf. & Inst. Code, § 827	Only certain persons may inspect juvenile case files; special rules apply when a deceased child is involved; further description of protocol for access/release of information in the files.
7	Computerized database system; authorized access; security procedures	Welf. & Inst. Code, § 827.1	A city/county may establish a computerized database system for intercounty/city exchange of information regarding minors under the jurisdiction of the juvenile court and may be accessed by authorized personnel under certain circumstances; this system must have security procedures to block unauthorized personnel from accessing the data.
8	Commission of felony; notice; disclosure of information	Welf. & Inst. Code, § 827.2	Information received regarding a juvenile's commission of a felony shall be held in confidence, with limited exceptions.
9	Commission of serious felony; minor in custody; hearing commenced; disclosure of name	Welf. & Inst. Code, § 827.5	Notwithstanding any other provision of law except sections 389 and 781 of Welfare and Institutions Code and section 1203.45 of the Penal Code, a law enforcement agency may disclose the name of any minor 14 years of age or older taken into custody for the commission of any serious felony, as defined in subdivision (c) of section 1192.7 of the Penal Code, and the offenses allegedly committed, upon the request of interested persons, following the minor's arrest for that offense.
10	Commission for violent offense; release of information	Welf. & Inst. Code, § 827.6	A law enforcement agency may release the name, description, and the alleged offense of any minor alleged to have committed a violent offense, as defined in subdivision (c) of section 667.5 of the Penal Code, and against whom an arrest warrant is outstanding, if the release of this information would assist in apprehending the minor or protecting public safety. Neither the agency nor the city, county, or city and county in which the agency is located, shall be liable for civil damages resulting from release of this information.
11	Disclosure of juvenile police records	Welf. & Inst. Code, § 827.9	Records or information gathered by law enforcement agencies relating to the taking of a minor into custody, temporary custody, or detention (juvenile police records) should be confidential. See subdivision (b) of the Welfare and Institutions Code for list of persons or entities that law enforcement may release a copy of a juvenile police record to.
12	Disclosure of information gathered by law enforcement agency; release of descriptive information about minor escapees	Welf. & Inst. Code, § 828	With exceptions, information gathered by a law enforcement agency relating to taking the minor into custody can be disclosed to another law enforcement agency; the law enforcement agency may release the name of, and any descriptive information about, the minor.
13	Confidentiality of records	Cal. Rules of Court, rule 5.552	In conjunction with Welfare and Institutions Code sections 827 and 828, this rule sets forth the procedure for review of otherwise confidential juvenile court records.
14	School district police or security department; disclosure of juvenile	Welf. & Inst. Code, § 828.1	There is a limitation to the confidentiality of juvenile criminal records in cases involving serious acts of violence—although any dissemination should be as limited as possible and take into consideration school-related issues.

	criminal records; protection of vulnerable school staff and other students		
15	Crimes against property, students, or personnel of school; juvenile custody or commission; information sharing	Welf. & Inst. Code, § 828.3	Notwithstanding any other provision of law, information relating to the taking of a minor into custody on the basis that he or she has committed a crime against the property, students, or personnel of a school district or a finding by the juvenile court that the minor has committed such a crime may be exchanged between law enforcement personnel, the school district superintendent, and the principal of a public school in which the minor is enrolled as a student if the offense was against the property, students, or personnel of that school.
16	Review of juvenile court records; suitability for release	Welf. & Inst. Code, § 829	Notwithstanding any other provision of law, the Board of Prison Terms, in order to evaluate the suitability for release of a person before the board, shall be entitled to review juvenile court records that have not been sealed, concerning the person before the board, if those records relate to a case in which the person was found to have committed an offense that brought the person within the jurisdiction of the juvenile court pursuant to Section 602.
17	Nonprivileged information and writings; disclosure among members of juvenile justice multidisciplinary team	Welf. & Inst. Code, § 830.1	Notwithstanding any other provision of law, members of a juvenile justice multidisciplinary team engaged in the prevention, identification, and control of crime, including, but not limited to, criminal street gang activity, may disclose and exchange nonprivileged information and writings to and with one another relating to any incidents of juvenile crime, including criminal street gang activity, that may also be part of a juvenile court record or otherwise designated as confidential under state law if the member of the team having that information or writing reasonably believes it is generally relevant to the prevention, identification, or control of juvenile crime or criminal street gang activity. Every member of a juvenile justice multidisciplinary team who receives such information or writings shall be under the same privacy and confidentiality obligations and subject to the same penalties for violating those obligations as the person disclosing or providing the information or writings. The information obtained shall be maintained in a manner that ensures the protection of confidentiality. As used in this section, “nonprivileged information” means any information not subject to a privilege pursuant to Division 8 (commencing with Section 900) of the Evidence Code. As used in this section, “multidisciplinary team” means any team of three or more persons, the members of which are trained in the prevention, identification, and control of juvenile crime, including, but not limited to, criminal street gang activity, and are qualified to provide a broad range of services related to the problems posed by juvenile crime and criminal street gangs. The team may include, but is not limited to, (a) Police officers or other law enforcement agents (b) Prosecutors (c) Probation officers (d) School district personnel with experience or training in juvenile crime or criminal street gang control

			(e) Counseling personnel with experience or training in juvenile crime or criminal street gang control (f) State, county, city, or special district recreation specialists with experience or training in juvenile crime or criminal street gang control.
18	Immigration status	Welf. & Inst. Code, § 831	Juvenile court records should remain confidential regardless of a juvenile's immigration status. (Welf. & Inst. Code, § 831(a).) Juvenile information may not be disclosed or disseminated to federal officials absent a court order upon filing a petition under Welfare and Institutions Code section 827(a). (Welf. & Inst. Code, § 831(b) & (c).) Juvenile information may not be attached to any documents given to or provided by federal officials absent prior approval of the presiding judge of the juvenile court under Welfare and Institutions Code section 827(a)(4). (Welf. & Inst. Code, § 831(d).) "Juvenile information" includes the "juvenile case file" as defined in Welfare and Institutions Code section 827(e), as well as information regarding the juvenile such as the juvenile's name, date or place of birth, and immigration status. (Welf. & Inst. Code, § 831(e).)
19	Records of mental health treatment or services	Welf. & Inst. Code, § 5328 et seq.	Records of mental health treatment, services, or confinement are confidential as described in the Welfare and Institutions Code section 5328 et seq.
20	Confidentiality; rules and regulations; violations; disclosure of confidential information regarding criminal act	Welf. & Inst. Code, § 10850 et seq.	All records and information regarding the identity of applicants for or recipients of public social services grants are confidential and not open to examination for any purpose not directly involved with the administration of the grant program or any investigation, prosecution, or criminal or civil proceeding conducted regarding the administration of the program. Exceptions and authorizations of disclosure are listed in the codes.

Appendix 2

Sample Privacy Statement[5]

Thank you for visiting the website of the Superior Court of California, County of _____ ("Court"). This policy explains how the Court treats information that this website collects and receives, including information related to your use of the website and information about you that is personally identifiable.

Information Collected and How It Is Used

Non-personal Information. Non-personal information is automatically collected by this website to make the site more useful, to diagnose problems with the website or servers, to learn about the number of visitors to the site, the types of technology they use, and to improve the site content and performance. None of this information contains personal identifiers (such as name, address, telephone number, etc.). Information that is automatically collected includes:

- If you linked to this website from another site, the address of the site you linked from;
- Your IP address (an IP address is a numerical identifier automatically assigned either to your Internet service provider or directly to your computer when you are surfing the Internet);
- Environmental variables including, among other things, the:
  - Internet domain from which you access the Internet;
  - Date and time you accessed this website;
  - Type of device, browser, operating system or platform, screen resolution, JavaScript status, and media player versions used;
  - The pages you accessed at this website; and
  - Internet address of the site you visit after leaving this website.
- Invisible tags placed on this website's pages, not on your computer or device, to compile aggregate statistics about site usage. When you visit a page with a tag, a generic notice of your visit to that page is generated. We sometimes track the keywords that are entered into our search engine to measure interest in specific topics.

Statistical, aggregated, and anonymous information collected by this website may be shared with third parties or the public. This information is not linked to any personal information that can identify any individual person.

Personally Identifiable Information. If you send comments or questions through the website, the information you provide, including your contact information, will normally be used to respond to

[5] This Sample Privacy Statement is meant to be user-friendly and easily understandable. It is only a starting point for your website. Each court should carefully review this document to confirm that it's acceptable from a court operations and court information technology standpoint.

you to address issues you identify, to improve our services, or in some cases, to refer you to another public entity that may be better able to assist you.

In order to access certain areas or services of this website, you may be asked to provide additional information or to register as a user and provide personal information. Personal information collected on this website may be used or shared in order to provide you with access to services and transactions offered by the Court including [case search, online payment of fines, text reminders, access to restricted information and documents]. Once you provide personal information, you are no longer an anonymous user of this website.

Unless otherwise required by law, the Court will not transfer, sell or otherwise make available to third parties personal information about, related to, or provided by users of this website, including e-mail and mailing addresses.

Cookies

Cookies are simple text files stored on your computer by your web browser. Cookies created on your computer by using this website do not contain personally identifiable information. The cookie feature may also be used to store a randomly generated identifying temporary tag on your computer. You may refuse the cookie or delete it through any of the widely available methods. However, if you turn your cookie option off, you may not be able to access some portions or services of this website.

Links to Other Sites

This website includes links to other sites we think you might be interested in or to assist with completing transactions or payments. The Court is not responsible for the privacy practices or the content of such sites.

Site Security

We have put in place physical, electronic and procedural safeguards to protect your personal information and to identify unauthorized attempts to access, upload or change information or to otherwise cause damage to the site. Anyone using this website expressly consents to such monitoring. As effective as any security measure implemented by this website may be, no security system is impenetrable.

General Disclaimer

This website and its content are provided on an “as is” “as available” basis, and may be subject to errors, inaccuracies, or omissions. The Court makes no representations or warranties regarding this website or its content. This website and its content do **not** constitute the official record of the Court.

Changes to Our Privacy Policy

Please note this privacy statement may change from time to time. We will post those changes as they occur.

Contacting Us

If you have questions about this privacy statement, you may contact us at: **[insert contact info].**

APPENDIX 3

SAMPLE TERMS OF USE

This website is operated by the Superior Court of California, County of _____ [***to be added***] ("court"). These Terms of Use govern public access to and use of this website ("website"), as well as the information and materials available on or through this website, including any court-related or case-related information (collectively, the "content").

By accessing or using this website, you agree that you have read, understood, and accept these Terms of Use. If you do not accept these Terms of Use, you may not access or use this website or the content.

The website and the content do **not** constitute the official record of the court. To obtain a certified copy of an official record of the court and information on certification fees, contact _____ [***contact info to be added***].

Disclaimers and Limitation of Liability

This website and the content are provided on an "as is," "as available" basis, and may be subject to errors, inaccuracies or omissions. The court and its officers, officials, employees, contractors and agents make no representations or warranties regarding this website or the content, including but not limited to their completeness, accuracy, timeliness, non-infringement of third-party rights, or freedom from computer viruses.

Your access to and use of this website and the content of the website are at your sole risk. The court is not responsible for any damages (including but not limited to any direct, indirect, incidental, special, consequential or exemplary damages), losses, claims or liability, known or unknown (including but not limited to loss of profits, goodwill, use or data), arising out of the use of (or inability to use) this website, the content, any third-party site linked to this website, or any error, omission, interruption, defect, delay, computer virus, theft, destruction, damage to computer systems, or unauthorized access.

Restrictions on Access and Use

In accessing or using this website and the content, you agree to comply with these Terms of Use as well as all applicable laws, rules (including the California Rules of Court and local court rules), regulations, and court orders.

You may download publicly-available content on this website, provided that: (1) you access court records only as instructed by the court, and (2) you comply with these Terms of Use and all applicable laws.

You are responsible for all content that you transmit or otherwise make available to this website. Any person who willfully destroys or alters any court record maintained in electronic form is subject to penalties, including but not limited to those imposed by California Government Code section 6201.

You may not do any of the following:

i. Interfere with or disrupt this website or any related court operations, or attempt to circumvent this website's security features;
ii. Cause an unacceptable level of congestion to the functioning of this website or any related court operations.
iii. [Engage in any data mining, web mining, web harvesting, use of "bots," or similar data gathering and extraction methods or tools in connection with the website or its content.][6]

[6] Included for discussion purposes.

iv. Misrepresent or alter the content or this website, or misinform others about the origin or ownership of the content or this website.

v. Decompile, reverse engineer, disassemble, lease, sell, distribute, or reproduce this website;

vi. Transmit, post, or otherwise make available:(a) content that is unlawful, false, inaccurate, harmful, obscene, or otherwise objectionable, including but not limited to any content that infringes on any intellectual property right or proprietary right; (b) viruses, Trojan horses or other harmful programs or material; or (c) advertising or promotional materials, "spam," or any other form of solicitation;

vii. Violate any copyrights, and other proprietary or intellectual property rights in this Website or the content; or

viii. Remove or modify any copyright notices, other proprietary notices, or references to these Terms of Use in the content or on this website.

[Additional restrictions and limitations apply to persons and entities accessing and using the website for high-volume commercial or bulk data collection purposes.][7]

No Legal Advice

This website and the content do not constitute legal advice, and no attorney-client relationship is formed.

Linking and Third Parties

This website may include links to third-party sites. When you access these sites, you are subject to third-party terms of use and privacy/security policies, which you should review. The court is not responsible for the accuracy, completeness, legality, practices, or availability of linked sites (including any related services, content, software applications, and other technologies).

References or links in this Website to any commercial products or services, or the use of any trade, firm or corporation name do not constitute endorsement by the court.

Copyrighted Materials

This website and the content are protected by applicable copyrights, and other proprietary and intellectual property rights. You do not acquire any ownership rights in the content or this website. If your copying or use of any copyrighted materials on this website is other than "fair use" under federal copyright laws, you must seek permission directly from the copyright holder. Copyrights and other proprietary rights may apply to information in a case file. Use of such information in a case file is permissible only to the extent permitted by law or court order, and any use inconsistent with proprietary rights is prohibited.

General

The court may change these Terms of Use from time to time by posting a new version on this website. Your continued use of or access to this website after such changes constitutes acceptance of such changes.

Your access to and use of this website and the content may be terminated at any time without notice. The failure of the court to enforce any provision in these Terms of Use will not constitute or be construed as a waiver of such provision or of the right to enforce it at a later time.

Your access to and use of this website may be monitored, including but not limited to, for the purpose of identifying illegal or unauthorized activities.

[7] Included for discussion purposes.

California law, without regard to conflict of laws provisions, will govern these Terms of Use and any matter or dispute arising out of this website or the content. The state and federal courts located in [***location to be added***], California will have exclusive jurisdiction over any dispute relating to these Terms of Use, this website, or the content.

These Terms of Use constitute the entire agreement with respect to public access to and use of this website and the content. Additional terms of use may be applicable to the special access available to parties and others, as described below. If any provision of these Terms of Use is unlawful, void or unenforceable, then that provision will be deemed severable from the remaining provisions and will not affect their validity and enforceability.

Additional Terms of Use

Portions of this website [may] provide means for the public to access documents filed in civil cases or [may] permit parties or other individual or entities special access to review documents or to transact business. Those portions of the website [may] contain additional terms of use applicable to the persons accessing and using them.

[Also, additional restrictions and limitations apply to persons and entities accessing and using the website for high-volume commercial or bulk data collection purposes. For more information concerning these restrictions and limitations, see *[provide link]*][8]

[***Add the following language for courts that allow public users to establish accounts on the website***]: If you establish an account on this website, you are responsible for maintaining the confidentiality of your user ID and password, and you are responsible for all activities that occur under your password or user ID. You agree to: (i) log out from your account at the end of each session; and (ii) immediately notify _____ [***appropriate court contact info to be added***] of any unauthorized use of your password or user ID or any other breach of security.]

Remedies for violations of terms

The court has the right to suspend or reduce service to, or otherwise restrict, access to this website and its contents to any user that causes an unacceptable level of congestion or disruption to the operation of the website or otherwise violates the Terms of Use. Furthermore, the court reserves the right to seek all legal and equitable remedies available for violations of these Terms of Use.

Contact information

If you have any questions about these Terms of Use, please contact: _____ ***[NOTE: email address TBD, e.g., webmaster?]***. Please do not, however, ask for legal advice or specific information about a case.

[8] Included for discussion purposes.

Tactical Plan 2019-2020 Proposed Initiatives

Strategic Plan 2019-2022 Goals	2019-20 Initiatives	Description
Promote the Digital Court	**Case Management System (CMS) Migration and Deployment**	Assist courts in selecting, funding, and deploying modern case management systems
	Expansion of Electronic Court Record Management	Digitizing paper documents and managing electronic court records
	Language Access Technology	Emphasis on technology enabling non-English speakers access to the courts
	Video Remote Appearance	Includes uses inside and outside the courthouse
	Self Help e-Services	New vision for digital services for the public
	Statewide E-Filing Program Development & Deployment	Deploy enterprise e-filing
	Digital Evidence: Acceptance, Storage, and Retention	Best practices, standards, guidelines, and technology services
	Branchwide Identity Management	Enable the public and justice partners to more effectively interact with the courts (e.g., "Single sign-on")
	Data Analytics and Business Intelligence	Recognized need for accessible branchwide information
	Enterprise Resource Management	Phoenix, CAFM (for facilities management): upgrades and new services to enable the courts to manage their staff, financial, and facilities resources.
	Consideration of Online Dispute Resolution	Explore policies, techniques, and technology to enable online resolution for disputes
Innovate Through IT Community	***Expand Collaboration within the Branch IT Community***	Technology collaboration and education within the branch
Advance IT Security and Infrastructure	**LAN/WAN Infrastructure**	Optimize court connectivity for upcoming court needs.
	Transition to Next-Generation Branchwide Hosting Model Phase II	Pilot guidelines and framework delivered in phase 1
	Disaster Recovery Phase II	
	Branchwide Information Security Roadmap	Advance branchwide IT security
Promote Rule and Legislative Changes	**Identify New Policy, Rule, and Legislative Changes**	Policy, rule, and legislative changes to enable appropriate use of technology

December 2018 Progress Report Estimated Completion Date: April 2019

1.1. Futures Commission Directive: Intelligent Chat (Phase 1)

Highlight: **Ongoing meetings with the core team and full workstream** are occurring 3-4 times per month and the workstream model is proving quite effective. FY19-20 BCP funding requested.

Key Objectives	Status	Description
Identify core team (sponsor and leads); form group membership; hold kickoff meeting(s).	Completed	**The core team has been formed.** It includes: Executive Sponsor, Judge Michael Groch (San Diego); Technical Lead, John Yee, Judicial Council Information Technology (JCIT); Project Manager, Fati Farmanfarmaian, JCIT, along with JCIT technical resources. **The full workstream team/membership has been formed.** Executive Sponsor, Judge Groch, distributed a branch memorandum inviting nominations for workstream membership. The request called for those individuals with an interest and experience in intelligent chat and the technology to deliver court services. The request also set membership expectations and defined next steps. A final membership list was approved by the ITAC and JCTC Chairs. **A workstream kickoff meeting was held on August 28** and included a full team orientation and educational demos of the intelligent chat technology. **Ongoing meetings with the core team and full workstream** are occurring 3-4 times per month and the workstream model is proving quite effective. The SharePoint site is robust and well populated with tools and data. An example is the collaborative user story sheet which forms the basis of the POC project selected by the team. Note that the original **estimated completion date** was based on a start date of January 2018; however, given that the workstream began later, this initial target date is being reassessed and will be updated for the next report. Additionally, staff has prepared and the Judicial Council approved the submission of a **budget change proposal requesting FY19-20 funding** to support more formalized piloting.
(a) Identify and monitor a series of court proofs of concepts (POCs) to assess technology readiness for various cases (e.g., Court of Appeal, E-Filing, Self-Help).	In Progress	The Business/Court Operations Track has started identifying user stories. The Technical Track has started researching different vendor technologies. Discovery will continue into the next quarter to help further identify and monitor court proofs of concepts.

December 2018 Progress Report Estimated Completion Date: April 2019

1.1. Futures Commission Directive: Intelligent Chat (Phase 1) (cont'd)

Highlight: **Ongoing meetings with the core team and full workstream** are occurring 3-4 times per month and the workstream model is proving quite effective. FY19-20 BCP funding requested.

Key Objectives	Status	Description
(b) Identify key performance indicators and benchmark before/after success.	Not Started	
(c) Capture learnings and report findings.	Not Started	
(d) Update Phase 2 of workplan based on results.	Not Started	
(e) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; annual agenda accordingly.	Not Started	

December 2018 Progress Report

Estimated Completion Date: June 2019

1.2. Futures Commission Directive: Voice-To-Text Language Services Outside the Courtroom (Phase 1)

Highlight: Project team kick-off meeting held. FY19-20 BCP funding requested.

	Status	Description
Identify core team (sponsor and leads); form group membership; hold kickoff meeting(s).	Completed	**The core team has been formed.** It includes: Executive Sponsor, Judge James Mize, (Sacramento); Business Lead, Heather Pettit, Judicial Council Information Technology (JCIT); and Project Manager, Rick Walery, (IT Director, San Mateo). In late August, a memorandum will be distributed to the branch (appellate and trial court presiding judges, CEOs, and CIOs) seeking nominations for members, and including expectations and next steps. Final membership is expected to be approved in September, after which a kickoff meeting will be scheduled. The target timeframe for completion of Phase 1 of this effort is 6-9 months from the workstream kickoff. After that time, it will be determined if a Phase 2 workstream will need to be established. **The project team has been formed.** The team includes members from a diverse set of courts and the Judicial Council. Expertise on the team ranges from multiple members with IT-related experience, a member who previously was a translator, and multiple members with first-hand knowledge or working with LEP customers at a court. Additionally, staff has prepared and the Judicial Council approved the submission of a **budget change proposal requesting FY19-20 funding** to support more formalized piloting.
Define the standard of success and how to measure it as well as define the difference between translation and interpretation.	Not Started	Define what the standard of success is for voice-to-text language services. Part of the comparator for success will be the current level of accuracy for non-machine language services. Part of the definition of success will also need to include definitions of the terms translation and interpretation since the differences may be somewhat nuanced.
Determine how, or if, the work for this initiative aligns with existing work of the Language Access Plan Implementation Task Force (LAPITF) and the work of The Legal Design Lab at the Stanford University Law School.	Not Started	It will be important to align the efforts of this initiative with other on-going work that is related to language access services. Additionally, this initiative will need to be aware of other Branch initiatives that may utilize similar machine learning or AI technology as there may be economies of scale by using the same technology platform as other branch-wide initiatives.

Estimated Completion Date: June 2019

1.2. Futures Commission Directive: Voice-To-Text Language Services Outside the Courtroom (Phase 1) (cont'd)

Highlight: Project team kick-off meeting held. FY19-20 BCP funding requested.

	Status	Description
(a) Setup a technical lab environment at the Judicial Council or a local court to test the technical recommendations of the Futures Commission for this initiative.	Not Started	
(b) Pilot various voice-to-text language services in a lab environment, will allow for exposure to more technologies and shorter learning cycles than if a specific technology is deployed at a court for piloting.	Not Started	
(c) Capture learnings and draft a white paper report on the lessons learned, findings, and recommendations for next steps.	Not Started	
(d) Update Phase 2 of workplan based on results.	Not Started	
(e) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; amend the Annual Agenda accordingly.	Not Started	

Estimated Completion Date: March 2019

1.3. Futures Commission Directive: Remote Video Appearances for Most Non-Criminal Hearings (Phase 1)

Highlight: Workstream members are progressing through an issue and topic log to address any challenges revealed through various studies.

Key Objectives	Status	Description
Identify core team (sponsor and leads); form group membership; hold kickoff meeting(s).	Completed	**The core team has been formed.** It includes: Executive Sponsor, Judge Samantha Jessner (Los Angeles); Court Lead, Jake Chatters (CEO, Placer); Project Manager, Alan Crouse (Deputy CEO, San Bernardino), along with support from the Judicial Council Information Technology Office (JCIT), Language Access Plan and VRI programs. **The full initiative team/membership has been formed and approved.** Eight courts, representing a diversity of size; participants from the VRI Workstream and remote video innovation grant, are a part of the team for this directive—specifically, the Superior Courts of Fresno, Los Angeles, Merced, Mono, Orange, Placer, Sacramento, and San Bernardino. **The workstream held its kickoff and meets monthly.** It has formed 4 subgroups/subcommittees and assigned a Chair/lead to each - Procedures, Evidence, Rules, and Technology. The subcommittees will develop initial recommendations on topics including but not limited to user technical requirements, evidence exchange, and presentation rules. Note that the **estimated completion date** was based on a start date of January 2018; however, given that the workstream began later, this initial target date is being reassessed and will be updated for the next report. Additionally, staff has prepared and the Judicial Council approved the submission of a **budget change proposal requesting FY19-20 funding** to support pilot deployments to the courts.
(a) Identify and conduct a mock remote video hearing using a web conferencing system for a specific hearing type (e.g., Civil – Small Claims) as a Proof of Concept (POC) in a court. Include one or more mock hearings of the selected hearing type.	In Progress	The Core Team identified a number of recent studies by the Center for Legal and Court Technology, the National Association for Presiding Judges and Court Executive Officers, the State Justice Institute, and the Self-Represented Litigation Network. Thus, an initial set of challenges to be explored has been developed for further refinement and investigation by the team. (continued on next page)

December 2018 Progress Report Estimated Completion Date: March 2019

1.3. Futures Commission Directive: Remote Video Appearances for Most Non-Criminal Hearings (Phase 1)

Highlight: Workstream members are progressing through an issue and topic log to address any challenges revealed through various studies.

Key Objectives	Status	Description
(a) Identify and conduct a mock remote video hearing using a web conferencing system for a specific hearing type (e.g., Civil – Small Claims) as a Proof of Concept (POC) in a court. Include one or more mock hearings of the selected hearing type.	In Progress	The team had progressed through an issue and topic log created from the results of the studies and has crafted initial recommendations. These recommendations will be used during mock proceedings to be scheduled in December 2018. The team is currently preparing scripts for these proceedings and finalizing the location and dates for the mock run.
(b) Capture learnings and report findings.	Not Started	
(c) Update Phase 2 of workplan based on results.	Not Started	
(d) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; annual agenda accordingly.	Not Started	

December 2018 Progress Report Estimated Completion Date: April 2019

2. Tactical Plan for Technology Update

Highlight: Draft plan finalized and submitted to Editing and Graphics Group.

Key Objectives	Status	Description
(a) Initiate workstream, including formation of membership and conduct orientation/kickoff meeting.	Completed	Kickoff meeting held.
(b) Review, gather input, and update the Tactical Plan for Technology.	In Progress	Several working meetings held, initiatives drafted and reviewed by workstream members. Remaining sections drafted, reviewed and finalized. Initiative drafts finalized by workstream leads. Full plan submitted to Editing and Graphics Group.
(c) Circulate the draft plan for branch and public comment; revise as needed.	Not Started	
(d) Finalize, and seek approval by the JCTC and the Judicial Council; thereafter, formally sunset the workstream.	Not Started	

December 2018 Progress Report Estimated Completion Date: March 2019

3. Video Remote Interpreting (VRI) Pilot

Highlight: The six-month VRI Pilot concluded on July 31, 2018. Pilot findings and recommended minimum technical standards for VRI are currently in development.

.

Key Objectives	Status	Description
(a) Support implementation of the Assessment Period of the VRI pilot program (including kickoff, court preparations, site visits, and deployment), as requested.	Completed	• **January 2018:** Onsite training was conducted at the three VRI pilot courts: Sacramento, Merced and Ventura Superior Courts. The pilot courts went live with VRI events. • **February 2018:** SDSU Research Foundation (the independent evaluator) began collecting data. • **March-April 2018:** SDSU conducted onsite observation in Sacramento to gather additional data. • **July 2018:** The pilot courts successfully shared interpreters from county to county (inter-court). The VRI pilot was completed on July 31, 2018. • **August 2018:** SDSU conducted an online survey with pilot stakeholders to gather feedback and additional data. • **September 2018:** Equipment removal began at the pilot courts.
(b) Review pilot findings; validate, refine, and amend, if necessary, the technical standards.	In Progress	• SDSU is working on their final evaluation report, and the National Center for State Courts (NCSC) is also helping the council to develop minimum technical standards for VRI. A December 14, 2018 Workstream meeting has been scheduled to review pilot findings and the draft standards. A report on the VRI Pilot is being targeted for the March 2019 Judicial Council meeting (TBD).
(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 collaborate with 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	

December 2018 Progress Report

Estimated Completion Date: June 2019

4. E-Filing Strategy

Highlight: Continued progress on EFM negotiations; and report on progress of EFSP accessibility.

Key Objectives	Status	Description
(a) Finalize master agreements with the three (3) E-Filing Managers (EFMs) selected to provide services.	In Progress	We continue to negotiate with 2 of the 3 chosen EFM Vendors Tyler, JTI and ImageSoft. We have an executed master agreement with JTI. We are close to agreement with ImageSoft who still must submit a SOW. Issues remain with Tyler that Snorri will discuss with the other courts using Tyler's Odyssey CMS.
(b) Develop the E-Filing Service Provider (EFSP) selection/certification process.	Not Started	Developing the certification process will require the JCIT staff positions, already identified, be filled. The initial position has been advertised with announcement of the selected candidate expected soon.
(c) Monitor the progress of EFSP accessibility compliance.	In Progress	In March 2018, the Judicial Council Information Technology Office conducted a survey of the 58 trial courts to determine compliance with AB 103. Based on survey results, currently 24 of the 58 trial courts provide electronic filing and electronic document service either directly, through vendor services, or a combination of vendor and in-house services. Preliminary feedback from the courts and vendors indicates a substantial level of compliance, with plans for achieving full compliance within the specified time frame of June 2019.
(d) Develop the roadmap for an e-filing deployment strategy, approach, and branch solutions/alternatives.	Not Started	
(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	
(f) Consult and report on the implementation of the court cost recovery fee that will support the statewide e-filing program.	In Progress	We have held a number of discussions with regard to the cost recovery fee. Currently the legal department are reviewing statutes to determine feasibility of implementing the cost recovery fee and distributing the funds collected.
(g) Coordinate and plan with JCIT regarding operational support of the ongoing e-filing program being funded through the court cost-recovery fee.	In Progress	The JCIT have identified the positions required for operational support of the statewide e-Filing program. The initial JCIT position has been advertised with announcement of the selected candidate expected soon.
(h) At the completion of these objectives and with the approval of the JCTC, formally sunset the workstream.	Not Started	

5. Identity and Access Management Strategy

Highlight: Phase 2 of the workstream, to identify policy and process recommendations as well as a strategy and roadmap, has started.

Key Objectives	Status	Description
(a) Develop and issue an RFP for a statewide identity management service/provider; identify and select.	Completed	Microsoft Azure AD Identity Service acquired under a Leveraged Procurement Agreement (LPA), County of Riverside RFQ #PUARC-1518, Microsoft Master Agreement Number 01E73970.
(b) Develop the roadmap for a branch identity management strategy and approach.	In Progress	Workstream membership approved. Two sub-streams formed. The Technical Roadmap team will be led by Michael Pugh (Yuba, IT Director) and comprised of mostly technical resources from around the state.
(c) Determine policies and processes for identity management (including proofing and access management).	In Progress	Workstream membership approved. Second sub-stream formed. The Policy team will be led by Rebecca Fleming (Santa Clara, CEO) and comprised largely of judges and court administrators from around the state. The first six policies for consideration have been identified.
(d) Ensure linkage and alignment with other branchwide initiatives such as E-Filing, SRL Portal, Next Generation Hosting, CMS Migration and Development.	In Progress	Sponsors or project managers for the aligned initiatives are members of the workstream.
(e) Coordinate and plan with JCIT regarding operational support, if appropriate.	In Progress	JCIT staff are participating in the pilot at Los Angeles Superior Court and are on the workstream.

Estimated Completion Date: April 2019

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

Highlight: BCP approved; began kickoff for pre-RFP planning.

Key Objectives	Status	Description
(a) Provide input for, and track, a SRL E-Services Budget Change Proposal (BCP) process for FY 18-19 funding.	Completed	• BCP was approved • $3.2 million in FY 2018–19 • $1.9 million in FY 2019–20 • $709,000 ongoing
(b) 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, and vendor resources.	In Progress	• This is being done in conjunction with the next line item (c) as part of the development of the RFP (or several if deemed advantageous).
(c) Develop and issue a request for proposal (RFP) or other solicitation, as needed, to support the implementation of the branchwide e-services portal.	In Progress	• In person kickoff meeting held on 7/12/18 • RFP scope and initial content outline completed • Follow-up meetings begin 7/30/18 • Target date for RFP(s) completion is January, 2019
(d) Determine implementation options for a branch-branded SRL E-Services website that takes optimal advantage of existing branch, local court, and vendor resources.	In Progress	• JCIT is funding a project (Digital Services Self-Help Pilot) as a pre-cursor to the SRL portal project which will pilot a small subset of features to get some experience and understanding in this area. • SRL E-Services workstream members participating on the Product Council for this Digital Services Pilot
(e) Coordinate and plan with JCIT regarding operational support, if appropriate. Note: In scope for 2018 is the submission and tracking of a budget change proposal (BCP) and development of an RFP; out of scope is the actual implementation.	In Progress	• Job Descriptions and PARS (Position Action Requests) are in progress for four new positions funded by the BCP. • Budget allocations and Project Team make-up are also in discussion • Target date to publish RFP(s) completion is January, 2019

December 2018 Progress Report

Estimated Completion Date: March 2019

7. IT Community Development

Highlight: Tools track conducted needs assessment on collaboration tools.

Key Objectives	Status	Description
Initiate new workstream: Identify sponsor and leads; form workstream membership; hold kickoff meeting(s).	Completed	Orientation and introduction meeting held on July 30, 2018 for members and workstream track leads to review the three workstream tracks (Resources, Education, Tools) and related key objectives. Next steps are for each track to solicit additional workstream participants as needed based on the area of focus and kick off the individual tracks. Workstream would like to amend its target end date from December 2018 to end of March 2019.
(a) Survey the courts to identify (i) their interest in exploring opportunities to share key technical resources and (ii) IT leadership and resource development needs and priorities; report findings.	In Progress	(i) Initial survey started for CEO input (ii) At the CITMF July 2018, there was a CIO development introductory session. Following the training, a survey was distributed to CIOs and participants on professional development opportunities for top 5 areas of focus for leadership development.
(b) Assess court CEO/CIO interest in an IT peer consulting program and develop recommendations.	In Progress	Initial survey started for CEO input.
(c) Partner with CJER to develop and implement an annual plan for keeping judicial officers, CEO's, and CIO's abreast of technology trends and tools.	In Progress	Work has begun on needs assessment strategies.
(d) Identify, prioritize, and report on collaboration needs and tools for use within the branch.	In Progress	Needs assessment conducted.
(e) Evaluate and prioritized possible technologies to improve advisory body and workstream meeting administration; pilot recommended solutions with the committee.	Not Started	
(f) Coordinate and plan with JCIT regarding operational support, as appropriate.	In Progress	Workstream Sponsor and Track Leads are working closely with JCIT to determine inclusive and appropriate workstream track membership and alignment with JC IT resources.

8. Intelligent Forms Strategy: Research & Scope (Phase 1)

Highlight: ITAC accepted workstream final report in April 2018 and sunset the workstream. JCIT assumed responsibility for investigating next steps and report back to ITAC.

Key Objectives	Status	Description
(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.	Completed	Final recommendation, Target Solutions Two and Five: Create and publish Application Programming Interface (API) that will merge data files with Judicial Council forms.
(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.	Completed	Final recommendation, Target Solutions One, Two and Five: Identify and deploy resources to certify all Judicial Council forms. Assign version numbering to all forms. Host all forms on a separate "Judicial Council forms server". Populate forms by merging data files with Judicial Council forms. Move away from filling out PDFs to completing web forms instead.
(c) Investigate options for redesigning forms to take advantages of new technologies, such as documents assembly technologies.	Completed	Final recommendation, Target Solutions Two, Six and Seven: The proposed solution will eventually separate the PDF from the data gathering tool, allowing a multitude of ways to populate forms, including third-party app developers. This proposal also recommends creating a clearinghouse for interview-based solutions so that best practices can be shared across platforms.
(d) Investigate options for developing standardized forms definitions and delivery methods that would enable forms to be efficiently electronically filed into the various modern CMSs across the state.	Completed	Final recommendation, Target Solutions Two, Four and Five: Standardize form field naming conventions by extending NIEM/ECF standards, preferably in collaboration with courts and vendors. Assign version numbering to all forms. Design form update governance standard to enable courts and vendors to easily identify changes.

December 2018 Progress Report

Estimated Completion Date: February 2018
Actual: April 2018

8. Intelligent Forms Strategy: Research & Scope (Phase 1) (cont'd)

Highlight: ITAC accepted workstream final report in April 2018 and sunset the workstream. JCIT assumed responsibility for investigating next steps and report back to ITAC.

Key Objectives	Status	Description
(e) Explore the creation and use of court generated text-based forms as an alternative to graphic forms.	Completed	Final recommendation, Target Solution Six: Develop pilot project to create truly dynamic forms. Such forms include only mandatory items and any optional items that contain data, but would not display empty fields.
(f) Investigate whether to recommend development of a forms repository by which courts, forms publishers, and partners may readily and reliably access forms in alternate formats.	Completed	Final recommendation, Target Solution Two: Host all Judicial Council forms on a separate "Judicial Council forms server".
(g) Develop recommendations for a potential BCP to support proposed solutions. (Note: Drafting a BCP would be a separate effort.)	Completed	An Initial Funding Request for three additional positions to support the recommendations in the workstream's report was drafted and submitted to the JCTC and JBBC for consideration.
(h) Initiate Phase 2 of the workstream, based on the recommendations.	Completed	At the April 30, 2018, ITAC meeting, ITAC asked JCIT to investigate the basis for any next steps. Suggestions included developing pilots, a Request for Information (RFI), and seeking funding for development and deployment. JCIT is expected to report back to ITAC on next steps, including if a Phase 2 workstream is needed. JCIT is considering initiating a pilot to test the workstream recommendations through the Appellate Self-Help Project. Given that JCIT is responsible for investigating and reporting back on next steps, including whether a phase 2 is appropriate, staff recommends this objective be removed from the annual agenda.

9. Digital Evidence: Assessment (Phase 1)

Highlight: Digital Evidence Survey Report drafted – presenting findings in ITAC educational session.

Key Objectives	Status	Description
(a) Review existing statutes and rules of court to identify impediments to use of digital evidence and opportunities for improved processes.	Completed	Existing statewide statutes and rules reviewed and documented. Findings summarized in the Digital Evidence Survey Report
(b) Survey courts for existing business practices and policies regarding acceptance and retention of digital evidence.	Completed	Survey completed and findings summarized in the Digital Evidence Survey Report
(c) Survey courts and justice system groups regrading possible technical standards and business practices for acceptance and storage of digital evidence.	Completed	Surveys completed and findings summarized in the Digital Evidence Survey Report
(d) Report findings to ITAC and provide recommendations on next steps.	In Progress	Digital Evidence Survey Report drafted
(e) Coordinate and plan with JCIT regarding operational support, if appropriate.	Not Started	Not applicable for Phase I. Recommend for Phase II.

10. Data Analytics : Access and Report (Phase 1)

Highlight: Workstream is drafting a proposed data governance policy for court data.

Key Objectives	Status	Description
(a) Research, scope, and recommend a data analytics strategy for the branch (e.g., this may include gaining case processing and resource data).	In Progress	Members are circulating a draft governance policy.
(b) Investigate possible policies, processes, and technologies to help the branch utilize data analytics to improve business effectiveness.	In Progress	The Judicial Council Legal Services Office has and will provide feedback about Rule 10.500 in the context of data analytics; members will also investigate policies and processes undertaken by other state agencies.
(c) Assess priorities for data collection and present findings to ITAC.	Not Started	This work will be undertaken in a second phase, once (a), (b), and (d) are complete.
(d) Identify possible data analytical tools and templates.	In Progress	Members are planning site visits and have previously viewed examples of products and output used by Orange County for their Innovations grant.

December 2018 Progress Report Estimated Completion Date: June 2019

11.2. Disaster Recovery (DR) Framework Phase 2

Highlight: Master agreements in process.

Key Objectives	Status	Description
Initiate new workstream: Identify sponsor and leads; form workstream membership; hold kickoff meeting(s).	In Progress	Sponsor has been identified. Through collaborative efforts initiated by the Innovation Grant-funded Cloud-Based Disaster Recovery project, members representing 26 JBEs crafted a branch-wide RFP to serve the majority of the courts. We plan to seek members of the workstream from the RFP strategy and review teams.
(a) Leverage the innovation grant awarded to the Superior Court of Monterey County for a Cloud DR Pilot Program.	In Progress	We expect to have master agreements completed by the end of December 2018. The next phase will include Monterey County Superior Court to select one for the award vendor solution, design and implement recovery for selected systems and programs.
(b) Recommend a list of critical technology services that make business sense for cloud-based recovery adoption.	Not Started	
(c) Establish a cloud DR master agreement wit h a short list of cloud service providers for judicial branch entities/courts to leverage.	In Progress	Master agreements with three vendors are expected to be completed by the end of December 2018. All three have been found to be capable of developing and implementing Cloud Based Disaster Recovery.
(d) Publish design solution templates using technologies and solutions from vendors selected in the cloud DR master agreement.	Not Started	
(e) Host knowledge sharing sessions for interested judicial branch entities/courts (including tools to estimate cost for deploying recovery solution using a particular cloud service provider; and Monterey solution case study).	In Progress	As part of the RFP for the Cloud-Based Disaster Recovery project, a proposal conference was held on May 31, 2018 to build knowledge on leveraging cloud technologies for disaster recovery. After the conclusion of the pilot phase, additional avenues for knowledge sharing will be made available to the judicial branch technology community.
(f) Provide input to JCIT that will be used in drafting a BCP to fund a pilot group of courts interested in implementing Cloud-based DR for critical technology services (see (b)).	Not Started	
(g) Coordinate and plan with JCIT regarding operational support, if appropriate.	Not Started	

12.1. Next-Generation Hosting Strategy Phase 1

Highlight: Completed Phase 1 workstream deliverables, including Judicial Council approval.

Key Objectives	Status	Description
(a) Coordinate with JCIT to define and plan the operational or ongoing support needed to maintain the *Next-Generation Hosting Framework Guide* and associated deliverables.	Completed	PM assigned for Next-Generation Hosting Workstream. PM assigned for future Next-Generation projects for CCTC.
(b) Seek approval of the proposed framework from the JCTC and adoption by the Judicial Council; thereafter, formally sunset this phase of the workstream.	Completed	Framework and toolkit was approved by the Judicial Council on March 2, 2018. Seeking formal approval from ITAC to sunset this phase of the workstream.

12.2. Next-Generation Hosting Strategy Phase 2

Highlight: Surveyed courts assessing hosting status; plan to formally solicit for membership.

Key Objectives	Status	Description
Initiate new workstream: Identify sponsor and leads; form workstream membership; hold kickoff meeting(s).	In Progress	Continue to work on workstream membership utilizing a survey to courts to gather data and feedback. No court workstream members identified to date.
(a) Identify and implement a pilot program to test the branch Next-Generation Hosting Framework and report findings. Pilot courts to include those with available funding; also, will include collaboration with courts already in progress of transitioning to next-generation hosting.	In Progress	Investigating current next generation hosting programs throughout the branch, including trial courts and judicial council technology projects. Axway Enterprise Managed File Transfer (EMFT) service at the California Courts Technology Center (CCTC) refresh used as pilot project, 9/18/2018, with Next-Generation Hosting Framework.
(b) Establish master agreements for cloud service providers. (Potential shared effort with DR Workstream initiative.)	In Progress	Monterey Court DR in cloud has concluded it's RFP and a Master Agreement with three vendors is in process.
(c) Establish the judicial branch support model for IT services.	Not Started	
(d) Determine funding mechanism to transition courts to new hosting models; this includes exploring a potential Budget Change Proposal (BCP)	Not Started	

13.1. Modernize Trial Court Rules

Highlight: Amendments to title 2, division 3, chapter 2 of the California Rules of Court were approved by the Judicial Council effective January 1, 2019.

Key Objectives	Status	Description
(a) **Proposals to create and amend rules to conform to legislation enacted in 2017.** For example, new provisions of Code of Civil Procedure section 1010.6 expressly require the Judicial council to adopt rules of court related to disability access and electronic signatures for documents signed under penalty of perjury. The new provisions also require express consent for electronic service, which will require a rule amendment, and creation of a form for withdrawal of consent.	Completed	• Amendments to title 2, division 3, chapter 2 of the California Rules of Court were approved by the Judicial Council effective January 1, 2019. The proposed amendments respond to new requirements in Code of Civil Procedure section 1010.6, amend definitions in the rules, and ensure indigent filers are not required to have a payment mechanism to create an account with electronic filing service providers. • Judicial Council form EFS-006, *Withdrawal of Consent to Electronic Service* was adopted by the Judicial Council effective January 1, 2019. The purpose of the form is to comply with Code of Civil Procedure section 1010.6(a)(6), which requires the Judicial Council to create such a form by January 1, 2019. This was a joint proposal with the Civil and Small Claims Advisory Committee. At its September 21, 2018 meeting, the Judicial Council voted to approve the rule amendments and adopt form EFS-006 effective January 1, 2019.
(b) **Proposals based on suggestions from the public** such as revising definitions and addressing a barrier to indigent users accessing services of electronic filing service providers.	Completed	See above.
(c) **Proposals for technical amendments** to amend rules language that is obsolete or otherwise unnecessary.	Completed	See above.

13.2 Standards for E-Signature

Highlight: E-signature rule approved by Judicial Council.

Key Objectives	Status	Description
(a) CEAC Records Management Subcommittee to develop standards governing electronic signatures for documents filed into the court with input from the Court Information Technology Managers Forum (CIOs). Rules & Policy Subcommittee to review.	In Progress Rule completed to comply with Code of Civil Procedure section 1010.6 CEAC Records Management Subcommittee no longer to develop standards.	AB 976 amended Code of Civil Procedure section 1010.6 to require the Judicial Council to develop a procedure for electronic signatures under penalty of perjury. Before the amendment to section 1010.6, rule 2.257 required standards for electronic signatures signed under penalty of perjury. AB 976 originally included standards, but the Legislature removed that and instead required only a procedure. ITAC proposed an e-signature rule to comply with section 1010.6's requirement for a procedure instead. The rule was presented to CEAC Records Management Subcommittee. The proposed rule defines electronic signature as it is defined in California's Uniform Electronic Transactions Act (UETA) and bases process for using an electronic signature under penalty of perjury on the process in UETA. The CEAC Records Management Subcommittee did not raise any concerns with this approach. At its September 21, 2018 meeting, the Judicial Council voted to approve the e-signature rule proposed by ITAC. The CEAC Records Management Subcommittee decided to remove standards from electronic signatures from its annual agenda because the law no longer requires the creation of standards. The annual agenda is pending approval by the full CEAC on Dec. 7 and the Executive and Planning Committee on Dec. 13.

13.3. Remote Access Rules for Government Entities, Parties, Attorneys

Highlight: The Judicial Council adopted the remote access rules effective January 1, 2019.

Key Objectives	Status	Description
(a) Lead the Joint Ad Hoc Subcommittee on Remote Access to amend trial court ruled to facilitate remote access to trial court records by state and local government entities, parties, parties' attorneys, and certain court-appointed persons.	Completed	At its September 20, 2018 meeting, Judge Hanson and Justice Siggins presented the remote access to electronic records to the Judicial Council. The council voted to adopt the remote access rules effective January 1, 2019.

13.4. Standards for Electronic Court Records as Data

Highlight: Members of CEAC Records Management Subcommittee have continued working on this project.

Key Objectives	Status	Description
(a) CEAC Records Management Subcommittee – in collaboration with the Data Exchange Workstream governance body – 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.	In Progress	The CEAC Records Management Subcommittee work is in progress. An initial draft is in progress and will be presented to the CEAC Records Management Subcommittee for review. A draft will also be presented to the ITAC Rules and Policy Subcommittee for feedback.
(b) Determine what statutory and rule changes may be required to authorize and implement the maintenance of record in the form of data; develop proposals to satisfy these changes.	In Progress	Same as above.

13.5. Privacy Resource Guide

Highlight: The Privacy Resource Guide (PRG) has been drafted and is ready for ITAC review.

Key Objectives	Status	Description
(a) Continue development of a comprehensive statewide privacy resource guide addressing, among other things, electronic access to court records and data, to align with both state and federal requirements.	In Progress	Finalized the Privacy Resource Guide that will assist the branch in addressing privacy issues; addressing among other things, confidential treatment of court records and data, and administrative records, consistent with statutes and case law. This final draft will be presented to ITAC at the Dec. 3 meeting.
(b) Continue development of court privacy resource guide, outlining the key requirements, contents, and provisions for courts to address within its specific privacy policy.	In Progress	The Privacy Resource Guide will include a section on best privacy practices for local courts to refer to regarding confidential treatment of court records and administrative records, and model templates for them to use. Legal staff has contacted various committees and divisions for assistance with this project.

Estimated Completion Date: Ongoing

14.1. Modernize Appellate Court Rules

Highlight: The Judicial Council approved JATS rules re: sealed and confidential materials and return of lodged e-records.

Key Objectives	Status	Description
(a) **Formatting of electronic reporters' transcripts:** Rule 8.144 was amended in the prior rules cycle to provide format requirements for electronic court reporter transcripts consistent with amendments to Code of Civil Procedure section 271. In this rules cycle JATS will consider whether additional amendments to Rule 8.144 are needed.	Completed	JATS monitored the implementation of this rule and received no reports of concern or problems with the rule amendment in practice. Since the implementation appears to be successful, the subcommittee will remove formal monitoring from the next annual agenda.
(b) **Sealed & Confidential Material:** Rules for the handling of sealed or confidential materials that are submitted electronically.	Completed	The Judicial Council approved and adopted JATS' recommended amendments on September 21, 2018. The amended rules become effective January 1, 2019.
(c) **Return of lodged electronic records:** The trial court rule modernization changes made in 2016 amend rules 2.551(b) and 2.577)d)(4) to give the moving party ten days after a motion to seal is denied, to notify the court if the party wants the record to be filed unsealed. If the clerk does not receive notification in then days, the clerk must return the record, if lodged in paper form, or permanently delete it if lodged in electronic form. JATS will consider whether equivalent appellate rules are desirable.	Completed	*See above. This proposal was consolidated with the above proposal (b) regarding sealed and confidential material.*
(d) **Rule amendments regarding access:** JATS will consider possible rule amendments to address online access to trial court records for parties, their attorneys, local justice partners, and other government agencies. The plan is for JATS to review what is ultimately proposed at the trial court level and use that as a basis for developing a companion proposal for access to appellate court records.	In Progress - Monitoring	The Judicial Council approved and adopted new rules on remote access for the trial courts, effective September 21, 2018. The rules become effective January 1, 2019. AAC/JATS will monitor the implementation of the trial court rules in the coming year to determine whether companion appellate rules are necessary.

Estimated Completion Date: Ongoing

14.1. Modernize Appellate Court Rules (cont'd)

Highlight: JATS developed its next set of recommended annual agenda projects; this includes the development of uniform format rules for e-documents submitted to the appellate courts.

Key Objectives	Status	Description
(e) **Bookmarking:** The 2016 trial court rules modernization changes include a new requirement, added to rule 3.1110(f), that electronic exhibits be electronically bookmarked. This issue was set aside by JATS for 2016, to permit those appellate courts new to e-filing at the time (or not yet on e-filing at the time) a chance to gain some experience with e-filing before participating in statewide decisions on this topic.	*Recommended for inclusion on next annual agenda.*	*This subject was consolidated with item (f) below.* JATS recommends inclusion of this project as part of its next annual agenda, anticipating an effective date of January 1, 2020. The project has expanded in scope to develop uniform format requirements for all electronic documents in the appellate courts. The Appellate Advisory Committee approved this project for the JATS annual agenda.
(f) **Exhibits:** Create a requirement that exhibits submitted in electronic form be submitted in electronic volumes, rather than individually.	*Consolidated with above.*	*See above. This proposal was consolidated with item (e) above, and is recommended for inclusion on the next annual agenda.*
(g) **Numbering of materials in requests for judicial notice:** Consider amending rule 8.252, which requires numbering materials to be judicially noticed consecutively , starting with page number one. The materials are attached to a motion and declaration(s) and are electronically filed as one document, making pagination and references to theses materials in the briefs confusing for litigants and the courts.	*Recommended for inclusion on next annual agenda.*	JATS recommends inclusion of this two-year project as part of its next annual agenda, anticipating an effective date of January 1, 2020. The Appellate Advisory Committee approved this project for the JATS annual agenda.

14.2. Rules Regarding Certification of Electronic Records, E-Signature, and Paper Copies

Highlight: The Judicial Council adopted trial court rules related to e-signatures; no other deliverables anticipated. ITAC to monitor implementation.

Key Objectives	Status	Description
(a) Provide input on proposed changes to the trial court rules of court governing certifications of electronic records, standards for electronic signatures, and requirements for paper copies of e-filed documents that will impact the appellate courts.	Completed	The Judicial Council approved and adopted the rule amendments applicable to the trial courts related to electronic signatures (rule 2.257). No other deliverables are anticipated.
(b) Consider whether to propose changes to the appellate court rules on this topic.	In Progress-Monitoring	Amended rule 2.257 takes effect January 1, 2019, and ITAC will monitor to assess how well it works and whether any amendments are needed. Following this process, JATS will consider whether to propose appellate court rules on electronic signatures. Until then, JATS will not take further action.

14.3. Input on Appellate Document Management System

Highlight: JATS continues to monitor and provide input.

Key Objectives	Status	Description
(a) Monitor and provide input on the implementation of a new document system (DMS) for the appellate courts.	In Progress-Monitoring	Phase 1 of this project has begun. The Third Appellate District and Fifth Appellate District will pilot initial implementation. JATS is monitoring and providing input through its Chair, Justice Mauro.

Information Technology Advisory Committee (ITAC)
Joint Appellate Technology Subcommittee
Annual Agenda—2019

One-Time Project (Ending 2020)

Rules Modernization: Uniform Formatting Rules for Electronic Documents — *Priority 1(e)*

Project Summary: Uniform Formatting Rules for Electronic Documents Filed or Submitted to the Appellate Courts

All appellate courts have implemented e-filing, but local rules for the format of electronic documents are often incomplete or inconsistent among the districts, resulting in burdens for litigants, attorneys, and appellate courts. This project originated with suggestions for rules regarding exhibits and bookmarking and was expanded in scope to include uniform formatting for all electronic documents.

Key Objective:

(a) The goal of this project is to develop uniform formatting rules for electronic documents filed or otherwise submitted to the appellate courts.

Origin of Project: Suggestions from advisory committee members, courts, the bar, and the public.

Status/Timeline: January 1, 2020

Resources:

- *ITAC:* Joint Appellate Advisory Subcommittee, Chair, Hon. Louis Mauro
- *Judicial Council Staffing:* Legal Services, Information Technology
- *Collaborations:* Appellate Advisory Committee

Information Technology Advisory Committee (ITAC)
Joint Appellate Technology Subcommittee
Annual Agenda—2019

Ongoing Project

Modernize Appellate Court Rules — *Priority 2(b)*

Project Summary: Modernize Appellate Court Rules to Support E-Filing and E-Business

Modernizing appellate court rules for e-filing and e-business is one of the main charges for JATS. Rules modernization includes projects such as (1) reviewing appellate rules to ensure they are consistent with e-filing practice and considering potential rule modifications where outdated provisions challenge or prevent e-business; (2) considering rule amendments to remove requirements for paper versions of documents; and (3) developing new rules to facilitate e-filing and e-business.

Specific projects:

(a) ***Numbering of materials in requests for judicial notice***. Consider amending rule 8.252, which requires that materials to be judicially noticed be numbered consecutively, starting with page number one. The problem is that such materials are attached to a motion and declaration(s) and are electronically filed as one document, making pagination and reference to those materials in the briefs confusing for litigants and the courts. This project may be addressed by the uniform format rules project. Source of the project: Dan Kolkey, committee member. Second year of a current priority 2 project/completion date of January 1, 2020.

(b) ***Method of notice to the court reporter***. Consider whether to amend rule 8.405, which governs the filing of an appeal in juvenile cases, to remove or modify the requirement in subdivision (b)(1)(B) that the clerk notify the court reporter "by telephone and in writing" to prepare a transcript. This language may be outdated or inconsistent with other rules requiring notification by the clerk. Source of the project: Tricia Penrose, Director of Juvenile Operations, Los Angeles Superior Court. New suggestion/completion date of January 1, 2021.

(c) ***Clarify the filing date of an e-filed document***. Amend rule 8.77 to clarify that an e-filed document received by the court before midnight that meets the filing requirements is deemed to have been filed that day. This project addresses an ambiguity in the rule that has resulted in inconsistent treatment of e-filed documents that are received after business hours. Source of the project: California Lawyers Association. New suggestion/completion date of January 1, 2021.

(continued next page)

(d) ***Court of Appeal service copy of a petition for review***. Amend rule 8.500(f)(1) to remove the requirement of a separate service copy of a petition for review. Once the Supreme Court accepts a petition for review for filing, the Court of Appeal automatically receives a filed/endorsed copy of the petition. The filing of the petition satisfies the service requirements for the Court of Appeal. This project is intended to eliminate an inefficiency. Source of the project: Colette Bruggman, Assistant Clerk/Administrator, Third District Court of Appeal. Second year of a current priority 2 project/completion date of January 1, 2020.

(e) ***Amend rule 8.70 to clarify content***. Consider amending rule 8.70 to clarify the subdivision (c)(2)(B) definition of a document and make subdivision (c)(2)(D) parallel with the rest of (c)(2). Source of the project: Justice Mauro, committee chair. New suggestion/completion date of January 1, 2021.

Origin of Project: Tactical Plan for Technology 2017-2018, and as specifically indicated above; standing item on annual agenda.

Status/Timeline: The rules modernization effort is ongoing. The completion date for each specific project is stated above.

Resources:

- *ITAC:* Joint Appellate Advisory Subcommittee, Chair, Hon. Louis Mauro
- *Judicial Council Staffing:* Legal Services, Information Technology
- *Collaborations, as needed:* Appellate Advisory Committee, Trial Court Presiding Judges Advisory Committee; Court Executives Advisory Committee.

Information Technology Advisory Committee (ITAC)
Joint Appellate Technology Subcommittee
Annual Agenda—2019

One-Time Project (Ending 2021)

E-Filing and E-Readers for Incarcerated Individuals — *Priority 2(b)*

Project Summary: E-Filing and E-Readers for Incarcerated Individuals to Access Electronic Reporter's Transcripts

Key Objective:

(a) This project involves exploring options with the California Department of Corrections and Rehabilitation (CDCR) and potentially recommending to the Judicial Council the development of a pilot program with one prison and one court to test promising options.

Origin of Project: Recent legislation (CCP § 271) allows a reporter's transcript to be produced electronically unless requested in paper. The defense bar supports providing access to electronic transcripts to incarcerated individuals. This project can be informed by other jurisdictions where e-filing and tablets have been made available to incarcerated individuals without providing general internet access.

Status/Timeline: January 1, 2021.

Resources:

- *ITAC:* Joint Appellate Advisory Subcommittee, Chair, Hon. Louis Mauro
- *Judicial Council Staffing:* Legal Services, Information Technology
- *Collaborations, as needed:* Appellate Advisory Committee, Court Executives Advisory Committee; California Department of Corrections and Rehabilitation (CDCR); any pilot court(s)

Information Technology Advisory Committee (ITAC)
Joint Appellate Technology Subcommittee
Annual Agenda—2019

	Ongoing Project	
	Appellate Document Management System	***Priority 1***

Project Summary: Liaise with Advisory Bodies for Collaboration and Information Exchange.

Key Objective:

(a) Receive status updates and provide feedback to Judicial Council Information Technology (JCIT) staff on implementation of a new document management system in the appellate courts. The Third Appellate District and the Fifth Appellate District are piloting the initial implementation.

Origin of Project: Part of JATS's ongoing charge to consult on technology matters impacting appellate court business.

Status/Timeline: This project is ongoing in that implementation across the appellate courts will take years. The timing of JATS's work will depend on the phases of implementation. Tentative completion date is 2021.

Resources:

- *ITAC:* Joint Appellate Advisory Subcommittee, Chair, Hon. Louis Mauro
- *Judicial Council Staffing:* Legal Services, Information Technology
- *Collaborations, as needed:* Appellate Advisory Committee; Administrative Presiding Justices; Appellate Court Clerk Executive Officers

Information Technology Advisory Committee (ITAC)
Rules and Policy Subcommittee
Annual Agenda—2019

	Ongoing Project	
	Trial Court Rules and Statutes Revisions	***Priority 1***

Project Summary: Revise Rules of Court and Statutes for the Trial Courts to Support E-Business

In collaboration with other advisory committees, as needed, review rules and statutes in a systematic manner and develop recommendations for amendments to align with modern business practices (e.g., eliminating paper dependencies).

Proposals within the scope of this item include:

(a) **Proposals to amend statutes to support e-business.** First, amend Code of Civil Procedure section 1010.6 to allow courts to recover actual costs of permissive electronic filing as they can with mandatory electronic filing, and clarify a provision for signatures made not under penalty of perjury. Second, amend Penal Code section 1203.01 to provide an alterative to mailing certain statements and reports.

(b) **Proposals to amend the electronic filing and service rules to provide greater clarity and remove paper dependancies.** First, amend rule 2.251 to clarify how notice of electronic service is to be given and provide standardized language for consent. Second, amend rule 2.257 to revise language on signatures of opposing parties, and make minor revisions consistent with Code of Civil Procedure section 1010.6.

(c) **Proposals to amend rules on remote access to electronic records.** Make minor amendments to rule 2.540 to add more clarity and additional local government entities.

In addition to proposals, the subcommittee will also monitor feedback on the new rules on remote access to electronic records to determine if more significant amendments may be needed as courts implement the rules. In particular, the subcommittee is interested in whether additional revisions to the government entity remote access rules are needed.

Origin of Project: Tactical Plan for Technology 2017-2018. Standing item on the agenda.

Status/Timeline: Ongoing

Resources:

- *ITAC:* Rules & Policy Subcommittee, Chair, Hon. Peter Siggins
- *Judicial Council Staffing:* Legal Services, Information Technology, Office of Governmental Affairs,

	• *Collaborations, as needed:* ITAC Joint Appellate Technology Subcommittee; Appellate Advisory Committee, Civil & Small Claims, Criminal Law, Traffic, Family and Juvenile Law, and Probate and Mental Health advisory committees; TCPJAC, CEAC and their Joint Technology, Rules, and Legislative Subcommittees

Information Technology Advisory Committee (ITAC)
Rules and Policy Subcommittee
Annual Agenda—2019

One-Time Project (Ending 2019)

Standards for Electronic Court Records as Data	***Priority 2***

Project Summary: Develop Standards for Electronic Court Records Maintained as Data

Key Objectives:

(a) CEAC Records Management Subcommittee – in collaboration with the Data Exchange Workstream governance body – to develop standards if needed 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.

(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.

Origin of Project: Carryover from 2016-2017 Annual Agenda. Court Executives Advisory Committee (CEAC); Government Code section 68150 provides that court records may be maintained in electronic form so long as they satisfy standards developed by the Judicial Council. These standards are contained in the Trial Court Records Manual. However, the current version of the manual addresses maintaining electronic court records only as documents, not data.

Status/Timeline: December 2019

Resources:

- *ITAC:* Rules & Policy Subcommittee, Chair: Hon. Peter Siggins
- *Judicial Council Staffing:* Information Technology, Legal Services
- *Collaborations, as needed:* Data Exchange governance body (TBD); CEAC, TCPJAC, and their Joint Technology Subcommittee

Information Technology Advisory Committee (ITAC)
Rules and Policy Subcommittee
Annual Agenda—2019

One-Time Project (Ending 2019)

13.3 Privacy Resource Guide — *Priority 2*

Project Summary: Monitor and maintain thePrivacy Resource Guide on Electronic Court Records and Access in Trial and Appellate Courts as needed

Key Objectives:

(a) Revise and update the Privacy Resource Guide with new privacy related laws, rules, forms, standards and best practices on an annual basis with a projected publication date after January 1, 2020 to allow for inclusion of published rules and law effective as of January 1, 2020.

(b) Monitor and analyze how the Privacy Resource Guide is being used for the calendar year 2019, and make recommendations for which Judicial Council entity will be responsible for maintaining and updating the Privacy Resource Guide beyond 2019.

Origin of Project: Tactical Plan for Technology 2017-2018; carryover from 2014-2017 Annual Agenda. Code Civ. Proc., § 1010.6 (enacted in 1999) required the Judicial Council to adopt uniform rules on access to public records; subsequently the rules have been amended in response to changes in the law and technology, requests from the courts, and suggestions from members of ITAC (formerly, CTAC), the bar, and the public.

Status/Timeline: December 2019

Resources:

- *ITAC:* Joint effort between the Rules & Policy and Joint Appellate Technology Subcommittees, Lead: Hon. Julie Culver
- *Judicial Council Staffing:* Legal Services, Information Technology
- *Collaborations, as needed:* Identity Management Working Group; Appellate Advisory Committee, CEAC, TCPJAC, and their Joint Technology Subcommittee; Criminal Law Advisory Committee, and the Department of Justice

Existing Project (Ending 2019)

Futures Commission Directive: Intelligent Chat for Self-Help Services (Phase 1)

Priority 1

Project Summary: The committee was directed by the Chief Justice to explore and make recommendations to the council on the potential for a pilot project using intelligent chat technology to provide information and self-help services.

Key Objectives:

Included in the Phase 1 of this project:

(a) Identify and monitor a series of court proofs of concepts (POCs) to assess technology readiness for various use cases (e.g., Court of Appeal, E-Filing, Self-Help).

(b) Identify key performance indicators and benchmark before/after success.

(c) Capture learnings and report findings.

(d) Update Phase 2 of workplan based on results.

(e) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; amend the annual agenda accordingly.

Origin of Project: Chief Justice directive from the Futures Commission recommendations report.

Status/Timeline: April 2019

Resources:

- *ITAC:* Sponsor: Hon. Michael Groch
- *Judicial Council Staffing:* Information Technology
- *Collaborations:* Court CIOs

Existing Project (Ending 2019)

Futures Commission Directive: Voice-to-Text Language Services Outside the Courtroom (Phase 1)

Priority 1

Project Summary: The committee was directed by the Chief Justice to explore available technologies and make recommendations to the Judicial Council on the potential for a pilot project using voice-to-text language interpretation services at court filing and service counters and in self-help centers. The goal of the lab pilot will be to determine next steps with this technology. Potential next step outcomes may be to continue to research the technology within a lab environment while it matures, to pilot at one court for a specific use case, or to pilot at multiple courts for multiple use cases.

Key Objectives:

Included in the Phase 1 of this project:

(a) Define the standard of success and how to measure it as well as define the difference between translation and interpretation.

(b) Determine how, or if, the work for this initiative aligns with existing work of the Language Access Plan Implementation Task Force (LAPITF) and the work of The Legal Design Lab at the Stanford University Law School.

(c) Setup a technical lab environment at the Judicial Council or a local court to test the technical recommendations of the Futures Commission for this initiative.

(d) Pilot various voice-to-text language services in a lab environment, which will allow for exposure to more technologies and shorter learning cycles than if a specific technology is deployed at a court for piloting.

(e) Capture learnings and draft a white paper report on the lessons learned, findings, and recommendations for next steps.

(f) Update Phase 2 of workplan based on results.

(g) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; amend the annual agenda accordingly.

Origin of Project: Chief Justice directive from the Futures Commission recommendations report.

Status/Timeline: June 2019

Resources:

- *ITAC:* Sponsors: Hon. James Mize
- *Judicial Council Staffing:* Information Technology
- *Collaborations:* Court CIOs, pilot courts, Innovation Grant awardees

Existing Project (Ending 2019)

Futures Commission Directive: Remote Video Appearances for Most Non-Criminal Hearings (Phase 1)

Priority 1

Project Summary: The committee was directed by the Chief Justice to consider, for presentation to the Judicial Council, the feasibility of and resource requirements for developing and implementing a pilot project to allow remote appearances by parties, counsel, and witnesses for most noncriminal court proceedings.

Key Objectives:

Included in the Phase 1 of this project:

(a) Capture learnings and report findings from Proof of Concept.

(b) Update Phase 2 of workplan based on results.

(c) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; amend the annual agenda accordingly.

Objectives resolved:

- *Identify and conduct a mock remote video hearing using a web conferencing system for a specific hearing type (e.g., Civil, Small Claims) as a Proof of Concept (POC) in a court. Include one or more mock hearings of selected case types. (Completed 2018. Workstream members proceeding through issue and topic log based on findings from POC)*

Origin of Project: Chief Justice directive from the Futures Commission recommendations report.

Status/Timeline: March 2019

Resources:

- *ITAC:* Sponsor: Hon. Samantha Jessner
- *Judicial Council Staffing:* Information Technology
- *Collaborations:* Court CIOs, pilot courts, and Innovation Award Grantees

Existing Workstream (Ending 2019)

Tactical Plan for Technology Update — *Priority 1*

Project Summary: Update *Tactical Plan for Technology* for Effective Date 2019-2020.

Key Objectives:

(a) Circulate the draft plan for branch and public comment; revise as needed.

(b) Finalize, and seek approval by the JCTC and the Judicial Council; thereafter, formally sunset the workstream.

Objectives resolved:

- *Initiate workstream, including formation of membership and conduct orientation/kickoff meeting. (Completed 2018)*
- *Review, gather input, and update the Tactical Plan for Technology (Workstream members collaborated to update the Tactical Plan for Technology, and is preparing to submit for branch and public comment).*

Origin of Project: Specific charge of ITAC per Rule 10.53 (b)(8).

Status/Timeline: April 2019

Resources:

- *ITAC:* Workstream, Sponsor: Hon. Sheila Hanson
- *Judicial Council Staffing:* Information Technology
- *Collaborations:* Broad input from the branch and the public.

Existing Workstream (End 2019)

Video Remote Interpreting (VRI) Pilot — *Priority 2*

Project Summary: Consult As Requested and Implement Video Remote Interpreting Pilot (VRI) Program

Key Objectives:

In cooperation and under the direction of the Language Access Plan Implementation Task Force (LAPITF) Technological Solutions Subccommittee (TSS):

(a) Review pilot findings; validate, refine, and amend, if necessary, the technical standards.

(b) Identify whether new or amended rules of court are needed (and advise the Rules & Policy Subcommittee for follow up).

(c) Consult and collaborate with LAPITF, as needed, in preparing recommendations to the Judicial Council on VRI implementations.

(d) Coordinate and plan with JCIT regarding operational support, if appropriate.

(e) At the completion of these objectives, seek approval of ITAC, JCTC and the Judicial Council and formally sunset the workstream.

Objectives Resolved

- *Support implementation of the Assessment Period of the VRI pilot program (including kickoff, court preparations, site visits, and deployment), as requested. (Completed 2018)*

Origin of Project: Tactical Plan for Technology 2017-2018; continuation of project from Annual Agenda 2015-2017.

Status/Timeline: March 2019

Resources:

- *Joint Workstream:*
  - *ITAC:* Sponsor: Hon. Samantha Jessner (ITAC)
  - *Language Access Plan Implementation Task Force (LAPITF):* Sponsor: Hon. Terence Bruiniers, Chair of LAPITF Technological Solutions Subcommittee (TSS)
- *Judicial Council Staffing:* Court Operations Special Services Office, Information Technology
- *Collaborations:* LAPITF TSS; CEAC, TCPJAC, and their Joint Technology Subcommittee; Court CIOs

Existing Workstream (Ending 2019)

E-Filing Strategy — *Priority 1*

Project Summary: Establish EFM Master Agreements, Develop EFSP Certification; Report on E-Filing Implementations, Standards, and Cost-Recovery

Key Objectives:

(a) Finalize master agreements with the three (3) E-Filing Managers (EFMs) selected to provide services (two of three completed in 2018).

(b) Consult and report on the implementation of the court cost recovery fee that will support the statewide e-filing program.

(c) At the completion of these objectives and with the approval of the JCTC, formally sunset the workstream.

Objectives resolved:

- *Develop the E-Filing Service Provider (EFSP) selection/certification process. (Task will be operationalized by JCIT. JCIT to provide oversight, with input from courts and EFMs.)*
- *Monitor the progress of EFSP accessibility compliance. (Completed 2018. JCIT will continue to report to the Legislature as required.)*
- *Develop the roadmap for an e-filing deployment strategy, approach, and branch solutions/alternatives.(Completed 2018. Projected roadmap for pilot phase included as part of BCP. JCIT to operationalize following initial pilot.)*
- *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. (NIEM/ECF standards have been developed for the pilot court. JCIT will operationalize and provide a report to the Judicial Council.)*
- *Coordinate and plan with JCIT regarding operational support of the ongoing e-fling program being funded through the court cost-recovery fee.(Completed 2018).*

Origin of Project: Tactical Plan for Technology 2017-2018; carryover project from 2015-2017 Annual Agenda with evolving objectives; also, directive from June 2016 Judicial Council meeting.

Status/Timeline: June 2019

Resources:

- *ITAC:* Workstream: Sponsor: Hon. Sheila Hanson
- *Judicial Council Staffing:* Information Technology, Legal Services
- *Collaborations:* Workstream members; CEAC, TCPJAC, and their Joint Technology Subcommittee

Existing Workstream (Ending 2019)

Identity and Access Management Phase II — *Priority 1*

Project Summary: Develop a Branch Identity Management Strategy

Key Objectives:

(a) Develop the roadmap for a branch identity management strategy and approach.

(b) Determine policies and processes for identity management (including proofing and access management).

(c) Ensure linkage and alignment with other branchwide initiatives such as E-Filing, SRL Portal, Next Generation Hosting, CMS Migration and Deployment.

(d) Coordinate and plan with JCIT regarding operational support, if appropriate.

Objectives resolved:

- *Develop and issue an RFP for a statewide identity management service/provider; identify and select. (Completed 2018)*

Origin of Project: Previously, this was a sub-task of the e-filing initiative. The item was promoted to its own annual agenda initiative given its many touchpoints with other workstreams (including Self-Represented Litigants E-Services, Next-Generation Hosting, E-filing Strategy, etc.). Tactical Plan for Technology 2017-2018.

Status/Timeline: July 2019

Resources:

- *ITAC:* Workstream: Sponsor: Mr. Snorri Ogata
- *Judicial Council Staffing:* Information Technology, Legal Services, Branch Accounting and Procurement
- *Collaborations:* Workstream members; CEAC, TCPJAC, and their Joint Technology Subcommittee

Existing Workstream (Ending 2019)

Self-Represented Litigants (SRL) E-Services — *Priority 1*

Project Summary: Develop Requirements and a Request for Proposal (RFP) for Establishing Online Branchwide Self-Represented Litigants (SRL) E-Services

Key Objectives:

(a) Develop and issue a request for proposal (RFP) or other solicitation, as needed, to support the implementation of the branchwide e-services portal. Anticipated time-to-completion: January 2019

(b) Coordinate and plan with JCIT regarding operational support, if appropriate.

Note: In scope for 2018 is the submission and tracking of a budget change proposal (BCP) and development of an RFP; out of scope is the actual implementation.

Objectives Resolved

- *Provide input for, and track, a SRL E-Services Budget Change Proposal (BCP) process for FY18-19 funding. (Awarded BCP funding for FY18-19 ($3.2 million) and FY19-20 ($1.3million))*
- *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. (Completed 2018)*
- *Determine implementation options for a branch-branded SRL E-Services website that takes optimal advantage of existing branch, local court, and vendor resources. (Completed 2018)*

Origin of Project: Tactical Plan for Technology 2017-2018; next phase of project following feasibility and desirability assessment (2015-2016).

Status/Timeline: January 2019

Resources:

- *ITAC:* Workstream, Sponsors: Hon. James Mize, Hon. Michael Groch
- *Judicial Council Staffing:* Information Technology, Center for Families, Children and the Courts (CFCC)
- *Collaborations:* Alternative Dispute Resolution (ADR) Subcommittee of the Civil and Small Claims Advisory Committee (C&SCAC) standing subcommittee; Advisory Committee Providing Access & Fairness; CEAC, TCPJAC, and their Joint Technology Subcommittee; CITMF, the Southern Regional SRL Network, and the California Tyler Users Group (CATUG)

Existing Workstream (Ending 2019)

IT Community Development — *Priority 1*

Project Summary: Expand Collaboration and Professional Development within the Branch IT Community

Key Objectives:

(a) Survey the courts to identify (i) their interest in exploring opportunities to share key technical resources and (ii) IT leadership and resource development needs and priorities; report findings.

(b) Assess court CEO/CIO interest in an IT peer consulting program and develop recommendations.

(c) Partner with CJER to ensure that technology related education and trends are incorporated within annual education plans for judicial officers, CEO's, CIO's, and court staff.

(d) Identify, prioritize, and report on collaboration needs and tools for use within the branch.

(e) Evaluate and prioritize possible technologies to improve advisory body and workstream meeting administration; pilot recommended solutions with the committee.

(f) Coordinate and plan with JCIT regarding operational support, as appropriate.

Origin of Project: Tactical Plan for Technology 2017-2018

Status/Timeline: March 2019

Resources:

- *ITAC:* Workstream, Sponsors: Hon. Alan Perkins, Ms. Jeannette Vannoy
- *Judicial Council Staffing:* Information Technology
- *Collaborations:* Workstream members; CEAC, TCPJAC, and their Joint Technology Subcommittee

New Workstream (Ending 2019)

Digital Evidence Workstream (Phase 2) — *Priority 2*

Project Summary: Investigate and draft technology best practices, standards, and policies, and propose changes to evidence-based rules and statutes.

Key Objectives:

(a) Investigate and draft proposed best practices, policies, and standards for transmitting, accepting, storing, and protecting digital evidence.

(b) Research and recommend existing technology and services that would support transmission, acceptance, storage, and protection of digital evidence.

(c) Based on findings from Phase 1, propose and process changes to evidence-based rules and statutes.

(d) Review the Trial Court Records Manual for any needed updates to reflect revisions of rules and statutes, and any proposed best practices, policies and standards.

(e) Report findings to ITAC and provide recommendations on next steps.

Origin of Project: Tactical Plan for Technology 2019-2020

Status/Timeline: December 2019

Resources

- *ITAC:* Workstream, Sponsor: Hon. Kimberly Menninger
- *Judicial Council Staffing:* Information Technology, Legal Services
- *Collaborations (Advisory Committees and External):* Workstream members; CEAC, TCPJAC

Existing Workstream (Ending 2019)

Data Analytics: Assess and Report (Phase 1) — *Priority 1*

Project Summary: Scope and Recommend a Data Analytics Strategy

Key Objectives:

(a) Scope and recommend a data analytics strategy for the branch.

- Identify, evaluate and prioritize possible policies, processes, and technologies to help the branch utilize data analytics to improve business effectiveness.
- Assess and report priorities for data collection.
- Identify and evaluate possible data analytical tools and templates.
- Identify whether new or amended rules of court and/or statutes are needed (and advise the Rules & Policy Subcommittee for follow up).
- Based on findings and recommendations, scope and initiate Phase 2 of the workstream.

(b) At the completion of these objectives, formally sunset this phase of the workstream.

Origin of Project: Topic resulted from a brainstorm of ideas conducted with ITAC and the court CIOs.

Status/Timeline: September 2019 [Judicial Council meeting is 9/24/19]

Resources:

ITAC: Workstream, Sponsors: Hon. Tara Desautels, Mr. David Yamasaki

Judicial Council Staffing: Information Technology, Criminal Justice Services, Judicial Branch Statistical Information System (JBSIS) Program, Center for Families, Children, and the Courts, Legal Services

Collaborations: CIOs, CEAC, TCPJAC, appellate group representation

Existing Workstream (Ending 2020)

Disaster Recovery (DR) Phase 2 — *Priority 1*

Project Summary: Implement Branch Disaster Recovery (DR) Pilot Program, Master Agreement, Knowledge-Sharing; Evaluate need for BCP

Key Objectives:

Leveraging the innovation grant awarded to the Superior Court of Monterey County for a Cloud DR Pilot Program, the workstream will:

(a) Recommend a list of critical technology services that make business sense for cloud-based recovery adoption.

(b) Establish a cloud DR master agreement with a short list of cloud service providers for judicial branch entities/courts to leverage.

(c) Publish design solution templates from JBEs that implement technologies and solutions from vendors selected in the cloud DR master agreement.

(d) Host knowledge sharing sessions for interested judicial branch entities/courts (including tools to estimate cost for deploying recovery solution using a particular cloud service provider; and Monterey solution case study).

(e) Evaluate the need for a BCP to fund a pilot group of courts interested in implementing Cloud-based DR for critical technology services (see (a)).

(f) Coordinate and plan with JCIT regarding operational support, if appropriate.

Origin of Project: Tactical Plan for Technology 2017-2018; next phase of project following framework adoption.

Status/Timeline: June 2020

Resources:

- *ITAC:* Workstream: Sponsor: Mr. Paras Gupta
- *Judicial Council Staffing:* Information Technology
- *Collaborations:* Workstream members; pilot courts; CEAC, CITMF

	Workstream (Ending 2019)	
	Next-Generation Hosting Strategy Phase 2	***Priority 1***

Project Summary: Pilot the Branch Next-Generation Hosting Strategy Framework, Establish Master Agreements, Establish Support and Funding Models

Key Objectives:

(a) Identify and implement a pilot program to test the branch Next-Generation Hosting Framework and report findings. Pilot courts to include those with available funding; also, will include collaboration with courts already in progress of transitioning to next-generation hosting.

(b) Establish master agreements for cloud service providers. (Potential shared effort with DR Workstream initiative.)

(c) Establish the judicial branch support model for IT services.

(d) Determine funding mechanism to transition courts to new hosting models; this includes exploring a potential Budget Change Proposal (BCP).

Origin of Project: Tactical Plan for Technology 2017-2018

Status/Timeline: July 2019

Resources:

- *ITAC:* Workstream, Sponsors: Mr. Brian Cotta
- *Judicial Council Staffing:* Information Technology
- *Collaborations:* CITMF

New Workstream (Ending 2019)

Electronic Court Record Management: Assessment — *Priority 1*

Project Summary: Identify and evaluate opportunities for migrating paper or microfiche case files to electronic case records with the use and integration of a DMS/ECMS with an existing CMS; identify efficient and cost-effective models for implementation

Key Objectives:

(a) Identify opportunities for migrating paper or microfiche case files through integration of a DMS/ECMS with existing branch and local case management systems
(b) Research and identify the most efficient and cost-effective models for electronic file conversion implementation.
(c) Develop and provide implementation guidelines, educational sessions and training materials for courts transitioning from paper/microfiche to electronic case files.
(d) Report findings to ITAC, including whether to recommend a Phase 2 of this workstream.

Origin of Project: Tactical Plan for Technology 2019-2020

Status/Timeline: December 2019

Resources:

(e) ITAC: Workstream, Sponsors:

(f) Judicial Council Staffing: Information Technology

(g) Collaborations:

New Workstream (Ending 2019)

Online Dispute Resolution (ODR): Assessment — *Priority 2*

Project Summary: Identify and evaluate available ODR technologies and potential scenarios in which ODR might benefit the judicial branch and its customers

Key Objectives:

(a) Identify and evaluate available ODR technologies.

(b) Review findings from existing court-offered ODR programs.

(c) Evaluate and describe scenarios where ODR might be beneficially deployed in the judicial branch.

(d) Review rules and statutes for possible amendments needed.

(e) Report findings to ITAC.

(f) At the completion of these objectives and with the approval of the JCTC, formally sunset the workstream.

Origin of Project: Tactical Plan for Technology 2019-2020.

Status/Timeline: December 2019

Resources:

- *ITAC:* Workstream: Sponsor: Hon. Sheila Hanson
- *Judicial Council Staffing:* Information Technology, Legal Services
- *Collaborations:* Workstream members; CEAC; TCPJAC; Civil and Small Claims Advisory Committee

	New Workstream (Ending 2019)	
	Branchwide Information Security Roadmap	***Priority 1***

Project Summary: This initiative will develop an implementation roadmap through the use of information security policies, standards, and guidelines.

Key Objectives:

(a) Update the strategy for expanding branch security capabilities.

(b) Update the strategy for educating courts on security best practices and mitigation strategies for security incidents.

(c) Identify resources to assist the courts in developing policies and procedures based on the Judicial Branch Information Systems Controls Framework.

Origin of Project: Tactical Plan for Technology 2019-2020

Status/Timeline: December 2019

Resources:

- *ITAC:* Workstream, Sponsors:
- *Judicial Council Staffing:* Heather Pettit, Matt Nicholls
- *Collaborations:*