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 2, 2020
10:00 AM to 12:00 PM
Videoconference

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; Hon. Michael S. Groch; Mr. Paras Gupta; Hon. Samantha P. Jessner; Hon. Kimberly Menninger; Hon. James Mize; Mr. Snorri Ogata; Mr. Darrel Parker; Hon. Donald Segerstrom; Hon. Bruce Smith; Ms. Jeannette Vannoy; Mr. Don Willenburg; Mr. David H. Yamasaki; Hon. Theodore Zayner
Advisory Body Members Absent:	Assemblymember Marc Berman; Ms. Alexandra Grimwade; Senator Robert Hertzberg; Hon. Peter Siggins; Hon. Joseph Wiseman
Others Present:	Hon. Kyle Brodie; Mr. Kevin Lane; Ms. Heather Pettit; Mr. Mark Dusman; Ms. Jamel Jones; Mr. Alex Barnett (Sen. Hertzberg office); Ms. Camilla Kieliger; Ms. Andrea Jaramillo; Ms. Nicole Rosa; 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
The advisory body reviewed and approved the minutes of the August 3, 2020 and September 17, 2020, Information Technology Advisory Committee meetings.

There were no public comments for this meeting.

DISCUSSION AND ACTION ITEMS (ITEMS 1–4)

Item 1

Chairs Report

Presenter: Hon. Sheila Hanson, Chair, Information Technology Advisory Committee

Report: Judge Hanson welcomed members and provided the following updates.,

The Tactical Plan Workstream has completed review of the initiatives and members are drafting updates from session feedback. The workstream will review updates at the next meeting.

At the September 25 Judicial Council meeting, Judge Jessner, Mr. Jake Chatters, Ms. Heather Pettit, and Judge Hanson presented the final report for the Remote Video Appearances Workstream. The Council approved the report. They also approved the proposal to amend rule 2.255 of the California Rules of Court to require an electronic filing service provider to allow an electronic filer to proceed with an electronic filing even if the filer does not consent to receive electronic service. The proposal also clarifies procedures for consent to electronic service as permitted by Code of Civil Procedure section 1010.6. Lastly, Judge Brody and Ms. Pettit presented the Judicial Council Technology Committee's recommendation to fund 13 separate technology projects.

Item 2

Judicial Council Technology Committee Update

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

Presenter: Hon. Kyle Brodie, Chair, Judicial Council Technology Committee

Report: Judge Brodie provided an update on his committee's work. They met on August 25 and September 14 and Judge Hanson provided updates at both meetings. Received an update on the Language Access Signage and Grant Program. On the $25M modernization of court operations, reviewed a governance process and list of 13 potential -projects.

These are the projects approved by the Judicial Council to be funded with the $25M:

- Remote Appearance Technology
- Digital Evidence
- Automated Messaging (notifications and reminders)
- Data Driven Forms
- Digitizing Documents
- Virtual Customer Service Center
- Trial Court Digital Services
- Statewide Case Index
- Judicial Branch Office of Information Security
- Next Generation Data Center and Cloud Solutions
- California Courts Protective Order Registry (CCPOR) Mobile Access and Modernization
- Building a Digital Ecosystem
- Data Governance

The next meeting will be on October 9.

Item 3

Data Analytics Workstream – Preview of Findings

Receive an update on this Workstream's recent progress, including an overview of proposed governance principles and policies. The Workstream leads will also discuss the timeline for

finalizing its work and for soliciting feedback on the proposed principles and policies from judicial branch entities and the public.

Presenters: Hon. Tara Desautels, Workstream Co-Executive Sponsor
Mr. David Yamasaki, Workstream Co-Executive Sponsor

Discussion: Judge Desautels and Mr. Yamasaki presented the Data Analytics draft policy and concepts, slides are in the member materials. The workstream's next steps include presenting at several branch meetings with various audiences and incorporating their suggestions and ideas. They will then bring updated concepts back to this committee in January 2021 and would like to request Judicial Council approval in March 2021.

Item 4

Futures Commission Directive: Voice to Text Language Services Outside the Courtroom – Status and Final Report (Action Requested)

Review and discuss the draft report to the Judicial Council on the potential of a pilot project using real-time voice-to-text language services at court filing and service counters and in self-help centers. Decide the report's readiness to recommend to the Judicial Council Technology Committee for acceptance and submission of the report to the Judicial Council.

Presenters: Hon. James Mize, Workstream Executive Sponsor
Mr. Rick Walery, Workstream Court Lead

Action: Judge Mize and Mr. Walery presented findings of the workstream that included three recommendations. They are that the Judicial Council sponsor a pilot project with the highest scoring vendor; courts should consider enterprise solutions with proven high-level of accuracy and responsiveness while ensuring data privacy and confidentiality; and this committee should collaborate with other advisory bodies to monitor advances in voice-to-text language technology and advise how to expand its use to the branch. Next steps include approving findings, developing end-to-end solution, and piloting solution to capture findings and determine future steps.

Motion to recommend the Voice-to-Text Workstream report for acceptance by the Technology Committee and the Judicial Council.

Approved.

ADJOURNMENT

There being no further business, the meeting was adjourned at enter time.

Approved by the advisory body on enter date.

Digital Evidence Workstream Rules and Statutes Subcommittee Report

SUBCOMMITTEE REPORT RECOMMENDING RULES AND STATUTES TO BE ADOPTED OR CHANGED TO ALLOW COURTS TO IMPLEMENT AND RECEIVE ELECTRONIC EVIDENCE

JUDICIAL COUNCIL OF CALIFORNIA
INFORMATION TECHNOLOGY ADVISORY COMMITTEE

TABLE OF CONTENTS

A. EXECUTIVE SUMMARY AND INTRODUCTION

The Rules and Statutes Track of the Digital Evidence Workstream was assigned to identify rules and statutes that need to change to allow courts to implement and receive electronic evidence and to identify and create new rules and/or statutes where appropriate. The Subcommittee developed this draft report to recommend changes to rules and statutes. Because the rules and statutes should be implemented to enable the other tracks to proceed, and based on the Judicial Council legislative and rule proposal timelines, the Subcommittee's work was spun off from the rest of the Workstream. Consequently, this Report is submitted as a stand-alone document.

Recommendations:

1. Use the descriptive term "electronic evidence" rather than "digital evidence."
2. Revise statutes requiring the clerk to maintain custody of exhibits to permit a third party vendor to maintain exhibits.
3. Address destruction and return of electronic evidence.
4. Create rules addressing access to electronic exhibit and electronic evidence.
    a. Litigant access
    b. Public access
    c. Electronic evidence submitted during remote video proceedings
    d. Status of lodged electronic exhibits
    e. Access rules should apply only while court has possession
5. Address confidential records, sealed records, and harmful matter.
6. Maintain the security, integrity, and chain of custody.
7. Modify various other statutes and rules addressing exhibits.
8. Other recommended guidelines for lodged electronic exhibits and evidence.

B. OBJECTIVES

The Rules & Forms Subcommittee of the Digital Evidence Workstream was tasked with:

1. Identifying any and all rules and statutes that need to change to allow courts to implement and receive electronic evidence; and

2. Identifying and creating new rules and/or statutes where appropriate.

C. ACTIVITIES

The Subcommittee identified numerous issues to be addressed concerning the courts' receipt of electronic evidence.

Standards Governing Court Held Electronic Evidence

The Branch should have appropriate standards governing court held electronic evidence and its:
- identification
- organization
- timing and methods of receipt, return and destruction
- security protocols
- preservation in original form
- handling and confidentiality of sealed and confidential electronic evidence

During discussion it was noted that these standards should address all stages of the courts' holding of electronic evidence, including the transmission, introduction, retention, return, and destruction of electronic evidence.

Methods and Locations for Holding Electronic Evidence

Current statutes require the court clerk to hold all evidence received by the court. The Subcommittee discussed that electronic evidence may be held by outside third-party vendors. Statutes addressing evidence retention must provide for evidence submission and retention with a third-party vendor.

Public Access Standards

Although rules and statutes treat public access to exhibits that are *filed* in court as court records[1], no statutes or rules clearly address public access to exhibits that are offered or received into evidence.[2] Public access to electronic evidence will need to be considered and addressed. Appropriate (but limited) access should be allowed. Public access to an electronic exhibit that has been provided to the court before it is offered or received into evidence should be restricted. As a general rule, the public has a right of access to exhibits used as a basis for adjudication while they are in the possession or control of the court. (*Mercury Interactive Corp. v. Klein* (2007) 158 Cal.App.4th 60, 91.)

D. RECOMMENDATIONS

1. **Use the descriptive term "electronic evidence" instead of "digital evidence."**

The Subcommittee recommends using the term "electronic evidence" rather than "digital evidence" to refer to evidence that has been sent to, communicated with, received by, or presented to the court in an electronic format. "Electronic evidence" fits within the scope of a "writing" as that term is used in the Evidence Code.[3] Specifically:

> "Writing" means handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing, any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored. (Evid. Code, § 250, emphasis added.)

An exhibit does not become evidence until it is admitted by the court. Accordingly, an exhibit not yet marked or admitted into evidence, but sent to, communicated with, or received by the court in an electronic format is a "lodged electronic exhibit." The use of the term "electronic" rather than "digital" is consistent with the use of "electronic" in other court contexts, including electronic records, electronic filing, and electronic service.

[1] See e.g., Gov. Code, § 68151, subd. (a)(1); Cal. Rules of Court, rules 2.3(2), 2.502(3), 2.551, 3.1112(b).

[2] The statutes addressing retention and return or destruction of evidence differ from the statute addressing retention of court records. (Compare Pen. Code, § 1417 et seq. and Code Civ. Proc., § 1952, et seq. with Gov. Code, § 68152.)

[3] The language "recording upon any tangible thing" as used in Evidence Code section 250 encompasses electronic evidence stored in the cloud, because the evidence is actually stored on an electronic storage device.

2. Revise statutes requiring the clerk to maintain custody of exhibits to permit a third party vendor to maintain exhibits

To the extent Penal Code section 1417, Code of Civil Procedure section 1952, and Government Code section 69846 require the clerk to maintain custody of exhibits, the Subcommittee recommends the statutes be amended to expressly permit, but not require, a third party vendor to handle and maintain custody of electronic exhibits on behalf of the court clerk.[4] If a third party vendor is permitted to store and manage a court's electronic evidence, the Subcommittee recommends that there be an exception for or special provisions governing the confidential nature of a "harmful matter" described in Penal Code section 1417.8.

3. Address the Destruction and Return of Electronic Evidence

The Subcommittee recommends addressing statutes concerning the return and destruction of exhibits, and determine whether electronic exhibits need to be "returned" to the party submitting them.[5]

4. Create rules addressing access to electronic exhibit and electronic evidence.

Exhibits that are "filed" in connection with motions or petitions are part of the court record. The Subcommittee recommends development of rules of court to define types of exhibits, who has access, when, and where.

a. Litigant Access

The Subcommittee recommends rules address whether, when, and to what extent remote access to lodged electronic exhibits and electronic evidence is authorized for parties, attorneys, and other specified individuals. California Rules of Court, rules 2.515 to 2.528, could serve as a model, allowing remote access to electronic court records by a party, a party's attorney, a court-appointed person, or authorized person working in a legal organization or qualified legal services project. (See also Cal. Rules of Court, rule 2.540 to 2.545 [similar rules for government entities].) Access should also require identity verification similar to California Rules of Court, rules 2.523 and 2.541.

b. Public Access

The Subcommittee recommends that rules address whether and when electronic evidence becomes a record subject to public access. As a general rule, the public has a right of access to exhibits used as a basis for adjudication while they are in the possession or control of the court. (*Mercury Interactive Corp. v. Klein* (2007) 158 Cal.App.4th 60, 91.) The Judicial Council should determine whether remote public access should be granted to electronic exhibits and electronic evidence, to the extent it is feasible to do so, except for exhibits or evidence that is sealed or confidential. The rules should provide a

[4] The Court could use the language of Government Code section 69955 as a guide. (See appendix C.)

[5] Code Civ. Proc., §§ 1952, subds. (c & d), 1952.2, and 1952.3; Pen. Code, §§ 1417.1, 1417.2, and 1417.3.

method to prevent public access to private information of witnesses and victims and harmful matter. (See section 5 below.) The rule should identify any proceedings in which remote access should be precluded or limited to a courthouse-only access rule. Rules governing public access to electronic court records could serve as a model. (See Cal. Rules of Court, rules 2.503(c) and 8.83.) The rules might address time, place, and manner restrictions on public access to lodged electronic exhibits and electronic evidence. (See *Courthouse News Service v. Planet* (9th Cir. 2020) 947 F.3d 581, 595.)

c. Electronic Evidence Submitted during Remote Video Proceedings

Electronic exhibits or electronic evidence that is not submitted in advance of a hearing, and is merely held up to the screen, or screen-shared by the litigant or attorney during a remote video proceeding poses unique issues. The Court does not receive a copy of the exhibit, only views it. It potentially could include information that should be redacted or sealed from public view, but may be viewed by the public watching remote proceedings. In that case, a screen capture could be taken of improper material and result in broad dissemination.

The Subcommittee recommends that the Judicial Council's Remote Video Workstream address the issue of electronic exhibits and electronic exhibits in remote video proceedings.

d. Lodged Electronic Exhibits

The court or rules may require that potential electronic exhibits be transmitted to the court in advance of the proceeding in which the material is anticipated to be used. With hard copy exhibits, the court never acquires access to the exhibit until it is offered into evidence. The Subcommittee recommends that during the time the court only serves as a bailee of a potential electronic exhibit, before the evidence is offered into evidence, the potential evidence be considered confidential to maintain the status it would have had prior to the promulgation of procedures addressing electronic evidence.

The Subcommittee recommends a rule defining a "lodged electronic exhibit" to be confidential prior to its use in any court proceeding, and it only becomes subject to public access if it is offered in court or used as a basis for adjudication, and it is not otherwise confidential or sealed. *(Mercury Interactive Corp. v. Klein* (2007) 158 Cal.App.4th 60, 94.) Once a lodged electronic exhibit is used as a basis for adjudication or offered as evidence, a rule should specify that it loses its character as a confidential lodged electronic exhibit.

The Subcommittee recommends rules to address who has access to lodged electronic exhibits. The Subcommittee recommends that only parties and attorneys for the side lodging the exhibit should have remote access to lodged electronic exhibits.

The Subcommittee recommends a rule or method to allow a court or third party vendor to destroy or permanently delete a lodged electronic exhibit that has been provided electronically but not used as a basis for adjudication or offered as evidence. The rule addressing destruction of conditionally lodged exhibits may provide guidance. (Cal. Rules of Court, rule 2.551(b)(6).) The rules should identify how the court should hold lodged electronic exhibits that are not used.

e. Access Rules Should Apply Only While Court Has Possession

Because the Court may not retain custody of exhibits after the case is completed, the Subcommittee recommends that litigant access or public access rules only apply while electronic evidence is in the possession or control of the court. Once the court no longer has possession of an exhibit or evidence, it should have no obligation to provide access to it.

5. Address Confidential Records, Sealed Records, and Harmful Matter

The Subcommittee recommends that the rules of court specifically address maintaining the confidentiality of any sealed or confidential electronic evidence. "Lodged electronic exhibits" may retain their confidential nature under other statutes or rules even after being used as a basis for adjudication or offered as evidence, for example a psychiatric report could be a lodged electronic exhibit, but may continue to be a confidential record after it has been offered as evidence. (See Evid. Code, § 1014.)

The Subcommittee recommends that the rules address redaction of sensitive personal information including social security numbers, financial information, arrest warrant and search warrant information, victim information, witness information, ethnicity, age, gender, government-issued identification card numbers, California Driver's license numbers, birth dates, confidential documents; sealed records; and harmful matter in electronic exhibits. (See e.g. Cal. Rules of Court, rule 8.83(d)(2).[6]) Redaction requirements may also be imposed to redact GPS metadata from the electronic files and/or blurring faces of bystanders and witnesses.

When redacted electronic evidence or an electronic exhibit is submitted to the court, the parties and/or their attorneys must submit both an original unredacted version and a redacted version for public access purposes.

The Subcommittee recommends amending California Rules of Court, rule 1.201(b) to require the parties and their attorneys to redact information not only from filed documents, but also from electronic evidence or electronic exhibits submitted to the court.

[6] California Rules of Court, rule 8.83(d)(2) provides:
The following information must be redacted from records to which the court allows remote access under (d): 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. The court may order any party who files a document containing such information to provide the court with both an original unredacted version of the document for filing in the court file and a redacted version of the document for remote electronic access. No juror names or other juror identifying information may be provided by remote electronic access. Subdivision (d)(2) does not apply to any document in the original court file; it applies only to documents that are made available by remote electronic access.

Proposal: It may also be appropriate to permit the Court to redact information that should not be in the public record.

The court has discretion to seal or redact personal identifying information in electronic evidence that are part of the public court record if the court makes findings that it would protect constitutionally-protected privacy interests of parties, victims, and witnesses.

The Subcommittee recommends special provisions protecting the confidential nature of Harmful Matter described in Penal Code section 1417.8.

The Subcommittee recommends that confidential and sealed lodged electronic evidence must be provided through a secure platform, and transmission of the information must be encrypted. (See Cal. Rule of Court, rule 2.542 as it relates to confidential or sealed electronic records, and Cal. Rules of Court, rule 2.256 regarding responsibilities of an electronic filer.)

6. Maintain security, integrity, and chain of custody of electronic evidence

The Subcommittee recommends that the holder of electronic evidence or electronic exhibits, whether it is the court or a third party vendor, be required to maintain the records in a secure manner that preserves confidentiality, and to strictly limit public access either by having separate repositories or digital rights management that limits access based on security levels.

The Subcommittee recommends the Judicial Council develop technical guidance or best practices to establish roles, digital rights management, and security levels to determine who can submit, access, retrieve lodged electronic exhibits and electronic evidence. Third party vendors must be required to comply with Judicial Council guidelines, and be subject to identify verification, identity management and user access provisions such as California Rules of Court, rules 2.523 and 2.541.

Safeguards will be required to protect the confidentiality and integrity of electronic evidence at all points where it is received, processed, stored, and maintained. This requires a broad set of management, operations, and technology specific security controls that must be in place to protect the data and ensure that privacy rights, safety and security protocols, chain-of-custody, and confidentiality requirements are maintained.

This will also require cloud security controls to protect the full lifecycle of data and ensure appropriate background screening of personnel with potential access to personal identifying information and criminal justice information (CJI).

The FBI's Criminal Justice Information Services (CJIS) requires all private contractors who process CJI to sign the CJIS Security Addendum, a uniform agreement that helps ensure the security and confidentiality of CJI in compliance with the CJIS Security Policy. It also commits the contractor to maintaining a security program consistent with federal and state laws, regulations, and standards, and limits the use of CJI to the purposes for which a government agency provided it.

7. Modify various other statutes and rules addressing exhibits.

The Subcommittee recommends amending Evidence Code section 1560 subdivisions (c) and (d) to permit electronic submission of subpoenaed business records from nonparty entities under seal and treating as confidential until they are introduced as evidence or entered into the record. Currently, Evidence Code section 1560 requires such evidence to be enclosed in a sealed "envelope or wrapper."

Adopting a comprehensive set of rules addressing electronic exhibits may render subdivisions (c) and (d) of rule 2.400 of the California Rules of Court moot. Those rules address the clerk's return of exhibits, and access to exhibits in the possession of temporary judges. The Subcommittee recommends that subdivisions (c) and (d) of California Rules of Court, rule 2.400 either be moved to the new rules addressing access to exhibits or cross-referenced in such rules.

Several rules of court require exhibits to be submitted to higher courts for writ and appeal purposes. If electronic evidence or electronic exhibits are maintained on the server of a court third party vendor, the Judicial Council should consider revising the rules to permit hyperlinks to the stored exhibits rather than actual submission of the exhibits. (See Cal. Rules of Court, rules 8.122, 8.204, 8.224, 8.320, 8.407, 8.483, 8.486, 8.504, 8.610, 8.622, 8.634, 8.832, and 8.931.)

8. Other Recommended Guidelines for Lodged Electronic Exhibits and Evidence

The Subcommittee recommends that statutes, rules and standards be flexible to address local court needs and capacities.

The Subcommittee recommends that electronic exhibits and electronic evidence file formats should be universally playable regardless of native format.

Guidelines or best practices should be established for the timing of submission of lodged electronic exhibits that precedes the date of any hearing or trial in which they will be offered.

APPENDIX A - Subcommittee Roster

Judge Kimberly Menninger
Orange County Superior Court

Presiding Judge Julie R. Culver
Monterey County Superior Court

Andrea L. Jaramillo, Attorney
Legal Services | Leadership Services Division

Robin Brandes-Gibbs, Deputy General Counsel
Orange County Superior Court

Kelley Heffelfinger, IT Project Manager I
Los Angeles Superior Court

Fred Acosta, Court Operations Manager
Orange County Superior Court

APPENDIX B – Statutes and Rules Proposed To Be Modified

Rule	What it Does	What changes are necessary or issues should be resolved
Create definitions		Define lodged electronic exhibits that are potentially evidence, but have not been offered or admitted into evidence.
Define how lodged electronic exhibits are treated		Where are lodged electronic exhibits stored? Who has access? How do we address it once proceeding is over and we have not admitted it or used it for an offer of proof?
Code Civ. Proc., § 1952	In civil cases, the clerk must retain any exhibit introduced or filed in a civil action or proceeding for 60 days following the judgment or the final determination of any appeal.	Address the "custody of the clerk" language in the statutes. Can outside vendors retain the evidence? A model for this might be the TCRM - case management systems hosted by vendor.
Code Civ. Proc., § 1952.2	Procedure for ordering the return of trial exhibits.	
Code Civ. Proc., § 1952.3	Any exhibit contained in a sealed civil case must be retained for 2 years beyond the date they would have been destroyed if not sealed.	Address the "custody of the clerk" language in the statutes.
Pen. Code, § 1417	All exhibits that have been introduced or filed in any criminal action or proceeding shall be retained by the clerk of the court who shall establish a procedure to account for the exhibits properly until final determination of the action or proceedings.	Address "retention by the clerk" language. Need to call out exhibits that may be electronic. May want to have the Rules of Court amended to address what types of evidence is where, and give the Judicial Council authority to do so.
Pen. Code, § 1417.3	The clerk may recommend that the court order the return of exhibits that pose security, storage, or safety problems prior to the final determination of a criminal action or proceeding. But the clerk is supposed to substitute it with a photographic record. (Pen. Code, § 1417.3, subd. (a).)	For electronic evidence, because there can be multiple originals, laws addressing return of exhibits may be changed to reduce court workload. Statutes or rules should provide notice to parties that they should download their exhibits prior to destruction. This would make parties responsible for retaining/destroying their own evidence.

Rule	What it Does	What changes are necessary or issues should be resolved
Pen. Code, § 1417.8(a)	Addresses exhibits that are photographs of minors found to be harmful matter.	"Retained by the clerk of the court" and "any duplication of the photograph of the exhibit in the possession of the parties "shall be delivered to the clerk" (Pen. Code, § 1417.8, subd. (a)(2).) How do we address harmful matter? Should we prohibit this from going to a vendor if we use a vendor to store evidence? Should the court retain possession and control to protect privacy? If it does go to a third party, what type of controls should protect it?
Gov. Code, § 69846	"The clerk of the superior court shall safely keep or dispose of according to law all papers and records filed or deposited in any action or proceeding before the court."	This should permit a third party vendor to handle exhibits.
Evid. Code, § 1560	The rule addresses business records subpoenaed from a witness. Subdivisions (c) requires the records to be delivered to the court in a sealed envelope, and subdivision (d) addresses the return of the records to the party.	This statute should be amended to permit the subpoenaed records to be electronically filed conditionally under seal with the court.
CRC rule 1.201(b)	The parties and their attorneys are responsible for excluding or redacting personal identifiers, including social security numbers or financial account numbers from "filed" documents.	This applies to documents "filed" in the court's public file. There should be a similar requirement for redaction with respect to exhibits. But the original should be filed as a confidential document.
CRC rule 2.250	Defines terms for electronic service and electronic filing and transmission.	This does not address exhibits. We should have a process to electronically provide exhibits.
CRC rule 2.400(c)(1)	The clerk must not release any exhibit except on order of the court. The clerk must require a signed receipt for a released exhibit.	What does this mean with respect to electronic evidence?

Rule	What it Does	What changes are necessary or issues should be resolved
CRC rule 2.400(c)(2) & (d)	These paragraphs address exhibits in the possession of temporary judges or referees.	Adoption of a comprehensive set of rules addressing electronic exhibits may render subdivisions (c) and (d) of rule 2.400 of the California Rules of Court moot. The Subcommittee recommends that California Rules of Court, rule 2.400(d) and (d) either be moved to the new rules addressing access to exhibits or cross-referenced in such rules.
CRC rule 2.502	Subdivision (c) defines "court record" for purposes of chapter to mean "any document, paper, **or exhibit filed** in an action or proceeding; any order or judgment of the court… "	Chapter 2 addresses public access to court records. Should the rule specifically exclude lodged electronic exhibits? Should we exclude "Exhibits that are not filed or admitted into evidence?" Do we need rules addressing public access to electronic exhibits? Do we want to permit remote access to such exhibits?
CRC rule 2.503(c)	Records in criminal proceedings, juvenile, guardianship, conservatorship, mental health proceedings, family law proceedings, civil harassment, workplace violence, elder abuse, and minor's compromises may not be made available remotely.	Should we preclude remote public access to electronic evidence in these case types?
CRC rules 2.515 to 2.528	Remote access is allowed for a party, a party's attorney, a court-appointed person, or authorized person working in a legal organization or qualified legal services project.	Does this apply to electronic evidence? When? We need rules to address lodged electronic exhibits and electronic evidence. Who has access to them, how it is handled, and how it is destroyed or removed. "After X days, we can destroy it."
CRC rule 2.516	To the extent feasible, a court that maintains records in electronic form must provide remote access to those records to the users described in rule 2.515 subject to the limitations of the law.	These rules are designed to provide access to specified people, create uniformity among trial courts.
CRC rules 2.540 to 2.545	Remote access for government entities. Confidential and sealed records must be provided through a secure platform, and transmission of the information must be encrypted.	Does this apply to electronic evidence? When?

APPENDIX C – Potential Digital Evidence Storage Vendor Rule

Using the language of Government Code section 69955 (which addresses electronic storage of official reporting notes) as a guide, the Judicial Council could create a rule addressing Digital Evidence Storage Vendors. Proposed language based on that rule follows:

(a) Electronic Evidence admitted into evidence shall be stored and maintained by the [Digital Evidence Storage Vendor] for the time periods specified for evidence preservation under California Penal Code, section 1417 et seq. and California Code of Civil Procedure, sections 1952 and 1952.2. The evidence shall be accessible to the court, court personnel, and authorized persons.

(b) Electronic Evidence accepted into evidence shall be kept by the [Digital Evidence Storage Vendor] in a place designated by the court, or, upon order of the court, delivered to the clerk of the court.

(c) The electronic evidence shall be maintained by the [Digital Evidence Storage Vendor].

(d) The electronic evidence shall be labeled with the case name, case number, the date admitted, the exhibit number. The electronic evidence shall be indexed for convenient retrieval and access. Instructions for access to electronic evidence shall be documented.

(e) At least one duplicate backup copy of the electronic evidence shall be stored in a manner and place that reasonably assures its preservation.

(f) Electronic transmissions that have not been marked for identification or admitted, but have been transmitted to the court through the Digital Evidence Storage Vendor shall be immediately deleted after the hearing, proceeding, or trial for which the transmissions were submitted, and email confirmation of such deletion shall be sent to the submitting party.

(g) Electronic transmissions that have not been offered, marked for identification, or admitted in evidence are not a court record and are not subject to public access rules.

(h) [Reserved for a section addressing evidence marked for identification, but not admitted.]

(i) Electronic evidence that is admitted may be destroyed by the Digital Evidence Storage Vendor after the periods established by California Penal Code, section 1417 et seq. and California Code of Civil Procedure, sections 1952 and 1952.2 upon notice to the Court and parties.

(j) A periodic review of the media on which the evidence is stored shall be conducted to assure that a storage medium is not obsolete and that current technology is capable of accessing and reproducing the evidence during the required retention period.

(k) If the agreement with the Digital Evidence Service Provider terminates, the evidence maintained by the Digital Evidence Service Provider shall be returned to the clerk of the court.

(l) The fees for the storage of evidence by the Digital Evidence Service Provider shall be paid by the court.