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

December 4, 2017
10:00 - 3:00 PM

Ronald M. George State Office Complex
William C. Vickrey Judicial Council Conference Center, 3rd Floor
Malcolm M. Lucas Board Room
455 Golden Gate Avenue San Francisco, California 94102-3688

Advisory Body Members Present:	Hon. Sheila F. Hanson, Chair; Hon. Louis R. Mauro, Vice Chair; Hon. Marc Berman; Mr. Brian Cotta; Hon. Julie R. Culver; Hon. Tara Desautels; Ms. Alexandra Grimwade; Hon. Michael S. Groch; Mr. Paras Gupta; Hon. Samantha P. Jessner; Hon. Jackson Lucky; Hon. Kimberly Menninger; Hon. James Mize; Mr. Snorri Ogata; Mr. Darrel Parker; Hon. Alan G. Perkins; Ms. Heather Pettit; Hon. Peter Siggins; Hon. Bruce Smith; Ms. Jeannette Vannoy; Mr. Don Willenburg; Mr. David H. Yamasaki
Advisory Body Members Absent:	Mr. Terry McNally; Hon. Daniel J. Buckley; Hon. Joseph Wiseman
Others Present:	Mr. Harry Ermoian (Asm. Berman's office); Mr. Rob Oyung; Mr. Mark Dusman; Ms. Kathy Fink; Ms. Jamel Jones: Ms. Andrea Jaramillo; 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
The advisory body reviewed and approved the minutes of the October 27, 2017, Information Technology Advisory Committee meeting.

No public comments received.

DISCUSSION AND ACTION ITEMS (ITEMS 1–9)

Item 1

Opening Remarks and Chair Report
Presenter: Hon. Sheila F. Hanson, Chair

Update: Judge Hanson welcomed everyone to the meeting. She also welcomed new members: Assemblymember Marc Berman, Judge Tara M. Desautels, Mr. Paras Gupta, Ms. Heather Pettit, and Justice M. Bruce Smith to their first in-person ITAC meeting. Judge Hanson also welcomed reappointed members: Justice Peter Siggins, Judge Julie Culver, and Judge Samantha Jessner.

The Judge thanked members for their participation and response to the member survey and she shared some results. There were high remarks that ITAC's mission and direction is clear and in alignment with the branch technology strategy; appropriately serving its purpose; and the updates from the subcommittees and workstreams are timely and informative. Also received was valuable feedback about how to improve the work ITAC does, including looking at meeting enhancements such as using video, updating the presentation format, holding more in person sessions, and providing or promoting technology education.

The chairs and staff began addressing the suggestions and there will be 3 in person meetings in 2018. Staff will also help to rebrand the presentations style, and during the annual agenda discussion today, there will be additional initiatives that address the remaining comments.

There was also feedback that members are generally supportive of the written reports from subcommittees and workstreams, but are interested in hearing more of the key debates being considered and discussed within the workstream teams. As a reminder, all ITAC members are welcome to participate in any subcommittee and workstream calls. Members are also welcome to reserve time on upcoming ITAC meeting agendas to highlight substance of their deliberations.

Lastly, many compliments were received for the work of the council staff supporting each workstream and subcommittee, their commitment and involvement is essential. Judge Hanson thanked council staff for their service.

Judge Hanson announced Mr. Robert Oyung, JC IT CIO has been appointed as the new Judicial Council Chief Operating Officer (COO). Mr. Oyung will continue oversight of JC IT and involvement in IT initiatives. Judge Hanson thanked him for his consistently positive outlook and strategic leadership.

Item 2

Judicial Council Technology Committee Update (Report)

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

Presenter: Hon. Marsha Slough, Chair, JCTC

Update: Justice Slough provided ITAC with a JCTC update. Since the October ITAC meeting, a joint orientation was held for the new JCTC and ITAC members on November 6. The

JCTC held an educational session on November 16 to review the Strategic Plan for Technology. This is in preparation for the committee's kick-off of the update to the Strategic Plan. The goal will be to have the Strategic Plan for Technology updated so it may be presented to the Judicial Council at the end of next year. This will be the first update to the Strategic Plan since it was approved by the Council in 2014 - and the updated plan will be for 2019 - 2022. The Strategic Plan and Tactical Plan for Technology are complementary documents. The work to update the Tactical Plan will be led by ITAC and that work will begin in 2018. A communication was sent last month to all courts requesting volunteers to assist with these efforts.

The JCTC also sent out two other requests for participation. One regarding the Digitizing Paper Pilot Program for Fiscal Year 18/19 to the Courts of Appeal and trial courts. Judicial Council IT is preparing a Budget Change Proposal or BCP for a pilot program enabling approximately five courts to digitize their paper and filmed case files. The second communication was an invitation to participate in this fiscal year's Jury Management System Grant Program. This was distributed to the trial courts and the accompanying completed form is due by January 12, 2018.

The JCTC will continue to meet regularly and work efficiently to address the judicial branch's needs and also build relationships with other state agencies and the legislature around technology, as well as partnerships to be certain that the needs of the judicial branch are heard in terms of technology.

Finally, Justice Slough congratulated Mr. Oyung on his promotion to COO and thanked Judge Hanson and ITAC for their excellent updates on the work of the workstreams.

Item 3

Next Generation Hosting Strategy Workstream (Action Requested)

Review final deliverables and decide whether to recommend for acceptance by the Judicial Council Technology Committee. The deliverables include a next-generation hosting framework guide, recommendations, and spreadsheet tools.

Presenters: Hon. Jackson Lucky, Workstream Executive Co-Sponsor
Mr. Brian Cotta, Workstream Executive Co-Sponsor
Ms. Heather Pettit, Workstream Project Manager/Court Lead
Ms. Jamel Jones, Supervisor, Judicial Council Information Technology

Update: Judge Lucky, Mr. Cotta and Ms. Pettit presented final deliverables for this workstream. The deliverables can be found in the meeting materials. The Next Generation Hosting Framework Guide references data center options, service-level definitions and timeframes, technology assets and service levels, recommended solutions, and branchwide recommendations. Deliverables were circulated to the branch for comment in October and November and the response was generally supportive. Non-substantive revisions for clarity were incorporated. A full comment matrix is provided in meeting materials. They asked ITAC for additional feedback and to approve and recommend

deliverables to the JCTC for adoption. Next steps include establishing master agreements for cloud service providers, identify and implement a pilot program and report findings, establish a judicial branch support model for IT services, and determine funding mechanism to transition courts to new hosting models.

Motion to Approve the final deliverables and recommendations of the Next-Generation Hosting Workstream.

Approved.

Item 4

Annual Agenda Discussion (Action Requested)

Review of proposals for the ITAC 2018 annual agenda. The committee will discuss and assess proposals in the following order:

(1) Existing Subcommittees
(2) Existing Workstreams
(3) Newly Expected Workstreams (directives, phase 2, tactical plan additions)
(4) Potential Ideas

The committee will be requested to vote to approve the contents of the final agenda.

Presenters: Mr. Robert Oyung, Chief information Officer, Judicial Council Information Technology

Ms. Jamel Jones, Supervisor, Judicial Council Information Technology

Update: Mr. Rob Oyung and Ms. Jamel Jones facilitated discussion on the current and proposed 2018 ITAC Annual Agenda projects. Handouts were provided to members for a Gartner graph exercise and informal voting determined the priority of items.

Final approved list of projects:

- Futures Commission Directive: Voice-to-Text Language Services Outside the Courtroom Phase 1 (New Project)
- Futures Commission Directive: Remote Video Appearances for Most Non-Criminal Hearings Phase 1 (New Project)
- Tactical Plan for Technology Update (New Workstream)
- Video Remote Interpreting (VRI) Pilot (Existing Workstream)
- E-Filing Strategy (Existing Workstream)
- Identity and Access Management Strategy (New Workstream)
- Self-Represented Litigants (SRL) E-Services (Existing Workstream)
- IT Community Development (New Workstream)
- Intelligent Forms Strategy: Research & Scope Phase 1 (Existing Workstream)
- Digital Evidence: Assessment Phase 1 (Existing Workstream)
- Data Analytics: Assess and Report Phase 1 (New Workstream)

- Disaster Recovery (DR) Framework Phase 1 (Existing Workstream)
- Disaster Recovery (DR) Framework Phase 2 (New Workstream)
- Next Generation Hosting Strategy Phase 1 (Existing Workstream)
- Next-Generation Hosting Strategy Phase 2 (New Workstream)
- Modernize Trial Court Rules (Ongoing Project)
- Standards for E-Signatures (One-Time Project)
- Remote Access Rules for Government Entities, Parties, Attorneys (One-Time Project)
- Standards for Electronic Court Records as Data (One-Time Project)
- Privacy Resource Guide (One-Time Project)
- Modernize Appellate Court Rules (Ongoing Project)
- Rules Regarding Certification of Electronic Records, E-Signature, and Paper Copies (One-Time Project)
- Input on Appellate Document Management System (One-Time Project)
- Liaison Collaboration (Ongoing Project)

Staff will circulate a final draft to members before it's sent to the JCTC for review and approval.

Motion to Approve the final content of the annual agenda.

Approved.

Item 5

Branch Budget Update (Report)

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, Judicial Council Budget Services

Update: Mr. Theodorovic provided a branch budget update to ITAC. Budget staff is in preparation of the budget process for meetings with the Legislature over the summer. They spent two days explaining trial court budgets and visited five courts. IT was a focus of the CMS BCP revenue collecting. The BCP was submitted in September to the Legislature and they seemed generally supportive. State revenues are 2% over the forecasted amount, but this is not final. The branch IMP & MOD funds are still low due to the decline of traffic revenues.

Item 6

Budget Change Proposal (BCP) Discussion

Review in progress BCPs for FY18-19. Gather committee input on BCPs for FY19-20.

Presenter: Mr. Robert Oyung, Chief Information Officer, Judicial Council Information Technology

Update: Mr. Oyung provided an update on the BCPs process and which BCPs are being submitted. Initial funding requests (IFR) are developed January – March, then approved by the appropriate committees between Mach – May, they are sent to the Judicial Council for approval in July. The regular cycle begins with drafting the BCP June – July, then submitting the BCP to Budget Services for review and refinement in August, finally submitting to the Department of Finance (DOF) in September. The spring cycle is to draft June – November, submit to Budget Services in December, and finally to the DOF in January-February.

BCPs in progress for FY 18-19:

Regular Cycle

- Upgrade the Phoenix System
- California Courts Protective Order Registry (CCPOR)
- Single Sign-On Solution

Spring Cycle

- CMS Replacement
- Digitizing Paper and Filmed Case Files pilot
- Self-Represented Litigants Statewide e-Services Solutions

The top FY 19/20 CITMF Priorities include disaster recover, data analytics, digital evidence, collaboration platform, next generation hosting, and case management next wave. Additional suggestions are included in the materials.

Item 7

Update on IT Security Framework (Report)

An update on the implementation of the IT security framework that was previously adopted by the Judicial Council.

Presenters: Mr. Michael Derr, Principal Manager, Judicial Council Information Technology

Update: Mr. Derr updated the progress and next steps in disaster recovery. The current structure is designed to adhere to NIST standards. The Judicial Council released a generic template to be localized by individual courts. The framework will be revised so that it applies universally to the branch, which allows courts to shift focus from localizing the framework and reallocate time towards implementation tasks. There must also be additional privacy controls incorporated as outlined in NIST. ITAC endorsed the proposed revision strategy and asked Mr. Derr to bring the updated document back to ITAC.

Item 8

Judicial Council Information Technology—Statewide Initiative Update (Report)

Present update on the status of various branch/enterprise technology initiatives.

Presenters: Ms. Virginia Sanders-Hinds, Principal Manager, Judicial Council Information Technology

Mr. Mark Gelade, Supervisor, Judicial Council Information Technology

Update: Ms. Sanders-Hinds updated the case management RFP collaboration across eight courts. There will be vendor demos December 4 – 6 and they are targeting December for the intent to award. The appellate e-filing project now has all appellate courts accepting electronic filings. Next steps are application upgrades and enhancements. The document management system (DMS) contract completion is targeted for December and deployments will begin at that time. Finally, the electronic signature initiative RFP responses evaluation begins on December 4 with intent to award in January 2018.

Mr. Gelade presented on JC IT web services. Their goal is to support the branch technology goal by promoting the digital court, optimize branch resources, optimize infrastructure, and promote rule and legislative changes. The roadmap timeline: 2017 Mobile/Responsive Framework for the courts.ca.gov and JRN home page redesign; 2018-19 New Scalable Managed Web Hosing Platform and interactive Appellate Self-Help Center; 2019-21 Statewide e-Services Portal. Some additional initiatives include: online/web accessibility; socializing “service design”; trial court web template refresh; and online collaborative tools & workspaces for JRN. Near future may include cloud hosting; intelligent chat; self-help options; online collaboration; open source; and artificial intelligence.

Item 9

Liaison Reports

Reports from members appointed as liaisons to/from other advisory bodies.

Update: No liaison updates.

ADJOURNMENT

There being no further business, the meeting was adjourned at 3:00 PM.

Approved by the advisory body on enter date.

Judicial Council of California

455 Golden Gate Avenue · San Francisco, California 94102-3688
www.courts.ca.gov/policyadmin-invitationstocomment.htm

INVITATION TO COMMENT

[ItC prefix as assigned]-__

Title
Technology: Rules Modernization Project

Proposed Rules, Forms, Standards, or Statutes
Amend Cal. Rules of Court, 2.250, 2.251, 2.255, and 2.257

Proposed by
Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

Action Requested
Review and submit comments by June 8, 2018

Proposed Effective Date
January 1, 2019

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

Executive Summary and Origin

As part of the Rules Modernization Project, the Information Technology Advisory Committee recommends amending several rules related to electronic service and electronic filing. The purpose of the proposal is to conform the rules to the Code of Civil Procedure, clarify and remove redundancies in rule definitions, and ensure indigent filers are not required to have a payment mechanism to create an account with electronic filing service providers. The proposal includes amendments required by statute and suggested by the public.

Background

New provisions of Code of Civil Procedure section 1010.6 require express consent for electronic service, which will require rule amendments and adoption of a form for withdrawal of consent. In addition, new provisions of Code of Civil Procedure section 1010.6 require the Judicial Council to adopt rules of court related to disability access and electronic signatures for documents signed under penalty of perjury. Finally, the proposal includes amendments based on comments received from the public. These include amendments to the definitions and contract requirements between electronic filing service providers and courts.

The Proposal

The proposal would:

- Amend the definition of "document" in rule 2.250(b). The current wording can be read to mean that a document must be a filing. The proposed amendment removes this ambiguity by striking "filing" and replacing it with "writing" to clarify that a "document" is not necessarily a filing. The amendment was suggested by members of the public.

- Amend the definitions of "electronic service," "electronic transmission," and "electronic notification" in rule 2.250(b) to refer to the definitions in Code of Civil Procedure section 1010.6 rather than duplicate them. This is to avoid risk of the rules and Code of Civil Procedure differing in their definitions should the Legislature amend Code of Civil Procedure section 1010.6.

- Add a definition for "electronic filing manager." The proposal includes amendments to rule 2.255 to include electronic filings managers. Accordingly, a definition of electronic filing manager was also added. The proposed definition is based on descriptions the Judicial Council used of electronic filing managers in a request for proposals in 2017.

- Add a definition for "self-represented" to rule 2.250(b) and exclude attorneys from the definition. Rules applicable to self-represented persons were intended to add protections for those without an attorney. For example, self-represented persons are exempt from mandatory electronic filing. Attorneys acting for themselves are not acting without an attorney. Accordingly, attorneys are excluded from the definition of "self-represented" under the electronic filing and service rules. Because Code of Civil Procedure section 1010.6 uses the term "unrepresented" and the rules use the term "self-represented," the definition in the rules refers to self-represented parties or other persons as being those unrepresented by an attorney. This proposal was a suggestion from a member of the public.

- Amend rule 2.251(b) to require express consent for permissive electronic service. The current rules allows the act of electronic filing to serve as consent to electronic service. Effective January 1, 2019, Code of Civil Procedure section 1010.6 will no longer allow the act of electronic filing alone to serve as consent. (Code Civ. Proc, § 1010.6(a)(2)(A)(ii).) Under Code of Civil Procedure section 1010.6, parties may still consent through electronic means by "manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic service address with that consent for the purpose of receiving electronic service." The proposal amends the rules to remove the provision allowing the act of filing to serve as consent to electronic service and replace it with the language for manifesting affirmative consent by electronic means. Substantively, this is a technical amendment to ensure the rules comply with the statute. The proposal does not interpret the statute, however the committee seeks specific comments on whether there is a need for interpretation to provide more guidance to courts and electronic filing service providers.

- Amend rule 2.255 to add electronic filing managers within the scope of the rule. Code of Civil Procedure section 1010.6(g)(2) requires that "[a]ny system for the electronic filing and service of documents, including any information technology applications, Internet Web sites, and Web-based applications, used by an electronic service provider or any

other vendor or contractor that provides an electronic filing and service system to a trial court" be accessible by persons with disabilities and comply with certain access standards. Vendors and contractors must comply as soon as practicable, but no later than June 30, 2019. (Code Civ. Proc., § 1010.6(g)(3). Likewise, the statute requires the Judicial Council to adopt rules to implement the requirements as soon as practicable, but no later than June 30, 2019. (Code Civ. Proc., § 1010.6(g)(1). Code of Civil Procedure section 1010.6 includes specific requirements that courts and contractors must meet. Rule 2.255 already requires courts contracting with electronic filing service providers to comply with Code of Civil Procedure section 1010.6. However, because the rules do not account for contracts with electronic filing managers, the proposal amends rule 2.255 is amended to include them.

- Amend rule 2.255 to add subdivision (f) requiring require electronic filing service providers to allow filers to create an account without having to provide a credit card, debit card, or bank account information. The amendment is based on a suggestion from the State Bar Standing Committee on the Delivery of Legal Services. According to the standing committee, some electronic service providers require such payment information even if the filer is never charged. According to the standing committee, this "creates an insurmountable barrier to those without access to credit or banking services." Subdivision (f) provides that it only applies to the creation of an account, but not to the provision of services unless the filer has a fee waiver.

- Amend rule 2.257 to create a procedure for electronically filed documents signed under penalty of perjury. Code of Civil Procedure section 1010.6(b)(2)(B)(ii) provides that when a document to be filed requires a signature made under penalty of perjury, the document is considered signed by the person if, in relevant part, "The person has signed the document using a computer or other technology pursuant to the procedure set forth in a rule of court adopted by the Judicial Council by January 1, 2019." Accordingly, the proposal creates a procedure where the document is deemed signed when the "declarant has signed the document using an electronic signature, and declares under penalty of perjury that the information submitted is true and correct." The language is modeled after the requirements in the Uniform Electronic Transactions Act for electronic signatures made under penalty of perjury. (Civ. Code, § 1633.11(b).) In addition, a definition of "electronic signature" is added to the rule modeled after the definitions used in UETA and the Code of Civil Procedure.

Alternatives Considered

The committee considered retaining the definitions of "electronic service," "electronic transmission," and "electronic notification" in rule 2.250(b) rather than referencing Code of Civil Procedure section 1010.6 for the definitions. The committee considered that referencing the Code of Civil Procedure will create an extra step in looking up the definitions. However, the committee opted for the proposed language to remove the risk of having differing definitions should the Legislature amend Code of Civil Procedure section 1010.6.

Implementation Requirements, Costs, and Operational Impacts

It is expected that the new express consent requirements will result in one-time costs to electronic filing service providers and courts to create a mechanism to capture affirmative consent by electronic means to electronic service. It is unknown whether or how these costs will impact fees electronic filing service providers charge filers for their services.

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?
- The technical amendments to rule 2.251(b) bring the rule into compliance with Code of Civil Procedure section 1010.6's express consent requirements. The rule does not interpret the express consent requirements. Is there a need for interpretation of the statute to provide guidance to the courts and electronic filing service providers? If so, what specific guidance is needed?

Attachments and Links

1. Proposed amendments to rules 2.250, 2.251, 2.255, and 2.257 of the California Rules of Court.
2. Code of Civil Procedure section 1010.6, *http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1010.6&lawCode=CCP*.

Rules 2.250, 2.251, 2.253, 2.255, and 2.257 of the California Rules of Court are amended, effective January 1, 2019, to read:

Title 2. Trial Court Rules

Division 3. Filing and Service

Chapter 2. Filing and Service by Electronic Means

Rule 2.250. Construction and definitions

(a) * * *

(b) Definitions

As used in this chapter, unless the context otherwise requires:

(1) A "document" is a pleading, ~~a paper,~~ a declaration, an exhibit, or another writing submitted by a party or other person, or by an agent of a party or other person on the party's or other person's behalf. A document is also a notice, order, judgment, or other issuance by the court. A document may be in paper or electronic form.

(2) "Electronic service" has the same meaning as defined in Code of Civil Procedure section 1010.6. ~~is service of a document on a party or other person by either electronic transmission or electronic notification. Electronic service may be performed directly by a party or other person, by an agent of a party or other person, including the party's or other person's attorney, through an electronic filing service provider, or by a court.~~

(3) "Electronic transmission" has the same meaning as defined in Code of Civil Procedure section 1010.6. ~~means the transmission of a document by electronic means to the electronic service address at or through which a party or other person has authorized electronic service.~~

(4) "Electronic notification" has the same meaning as defined in Code of Civil Procedure section 1010.6. ~~means the notification of a party or other person that a document is served by sending an electronic message to the electronic service address at or through which the party or other person has authorized electronic service, specifying the exact name of the document served and providing a hyperlink at which the served document can be viewed and downloaded.~~

(5) – (8) * * *

(9) An "electronic filing manager" is a service that acts as an intermediary between a court and various electronic filing service provider solutions certified for filing into California courts.

(10) "Self-represented" means a party or other person who is unrepresented in an action by an attorney and does not include an attorney appearing in an action who represents himself or herself.

Rule 2.251. Electronic service

(a) * * *

(b) Electronic service by express consent ~~of the parties~~

(1) ~~Electronic service may be established by consent.~~ A party or other person indicates that the party or other person agrees to accept electronic service by:

(A) Serving a notice on all parties and other persons that the party or other person accepts electronic service and filing the notice with the court. The notice must include the electronic service address at which the party or other person agrees to accept service; or

(B) ~~Electronically filing any document with the court. The act of electronic filing is evidence that the party or other person agrees to accept service at the electronic service address the party or other person has furnished to the court under rule 2.256(a)(4). This subparagraph (B) does not apply to self-represented parties or other self-represented persons; they must affirmatively consent to electronic service under subparagraph (A).~~ Manifesting affirmative consent through electronic means with the court or the court's electronic filing service provider, and concurrently providing the party's electronic service address with that consent for the purpose of receiving electronic service.

(2) A party or other person that has consented to electronic service under (1) and has used an electronic filing service provider to serve and file documents in a case consents to service on that electronic filing service provider as the designated agent for service for the party or other person in the case, until such time as the party or other person designates a different agent for service.

(c) - (k) * * *

Rule 2.255. Contracts with electronic filing service providers and electronic filing managers

(a) Right to contract

(1) A court may contract with one or more electronic filing service providers to furnish and maintain an electronic filing system for the court.

(2) If the court contracts with an electronic filing service provider, it may require electronic filers to transmit the documents to the provider.

(3) A court may contract with one or more electronic filing managers to act as an intermediary between the court and electronic filing service providers.

~~(3)~~(4) If the court contracts with an electronic service provider or the court has an in-house system, the provider or system must accept filing from other electronic filing service providers to the extent the provider or system is compatible with them.

(b) Provisions of contract

(1) The court's contract with an electronic filing service provider may:

(A) Allow the provider to charge electronic filers a reasonable fee in addition to the court's filing fee;

(B) Allow the provider to make other reasonable requirements for use of the electronic filing system.

(2) The court's contract with an electronic filing service provider must comply with requirements of Code of Civil Procedure section 1010.6.

(3) The court's contract with an electronic filing manager must comply with requirements of Code of Civil Procedure section 1010.6.

(c) Transmission of filing to court

(1) An electronic filing service provider must promptly transmit any electronic filing and any applicable filing fee to the court~~.~~ directly or through the court's electronic filing manager.

(2) An electronic filing manager must promptly transmit an electronic filing and any applicable filing fee to the court.

(d) Confirmation of receipt and filing of document

(1) An electronic filing service provider must promptly send to an electronic filer its confirmation of the receipt of any document that the filer has transmitted to the provider for filing with the court.

(2) The electronic filing service provider must send its confirmation to the filer's electronic service address and must indicate the date and time of receipt, in accordance with rule 2.259(a).

(3) After reviewing the documents, the court must promptly transmit to the electronic filing service provider and the electronic filer the court's confirmation of filing or notice of rejection of filing, in accordance with rule 2.259.

(e) Ownership of information

All contracts between the court and electronic filing service providers or the court and electronic filing managers must acknowledge that the court is the owner of the contents of the filing system and has the exclusive right to control the system's use.

(f) Establishing a filer account with an electronic filing service provider

(1) An electronic filing service provider may not require a filer to provide a credit card, debit card, or bank account information to create an account with the electronic filing service provider.

(2) This provision applies only to the creation of an account and not to the use of an electronic filing service provider's services. An electronic filing services provider may require a filer to provide a credit card, debit card, or bank account information before rendering services unless the services are within the scope of a fee waiver granted by the court to the filer.

Rule 2.257. Requirements for signatures on documents

(a) Electronic signature

An electronic signature is an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign a document or record created, generated, sent, communicated, received, or stored by electronic means.

~~(a)~~(b) Documents signed under penalty of perjury

When a document to be filed electronically provides for a signature under penalty of perjury of any person, the document is deemed to have been signed by that person if filed electronically provided that either of the following conditions is satisfied:

(1) The declarant has signed the document using an electronic signature ~~a computer or other technology, in accordance with procedures, standards, and guidelines established by the Judicial Council~~ and declares under penalty of perjury under the laws of the state of California that the information submitted is true and correct; or

(2) The declarant, before filing, has physically signed a printed form of the document. By electronically filing the document, the electronic filer certifies that the original, signed document is available for inspection and copying at the request of the court or any other party. In the event this second method of submitting documents electronically under penalty of perjury is used, the following conditions apply:

(A) At any time after the electronic version of the document is filed, any party may serve a demand for production of the original signed document. The demand must be served on all other parties but need not be filed with the court.

(B) Within five days of service of the demand under (A), the party or other person on whom the demand is made must make the original signed document available for inspection and copying by all other parties.

(C) At any time after the electronic version of the document is filed, the court may order the filing party or other person to produce the original signed document in court for inspection and copying by the court. The order must specify the date, time, and place for the production and must be served on all parties.

(D) Notwithstanding (A)–(C), local child support agencies may maintain original, signed pleadings by way of an electronic copy in the statewide automated child support system and must maintain them only for the period of time stated in Government Code section 68152(a). If the local child support agency maintains an electronic copy of the original, signed pleading in the statewide automated child support system, it may destroy the paper original.

~~**(b)**~~**(c)** * * *

~~**(c)**~~**(d)** * * *

~~**(d)**~~**(e)** * * *

~~**(e)**~~**(f)** * * *

~~**Advisory Committee Comment**~~

~~**Subdivision (a)(1).** The standards and guidelines for electronic signatures that satisfy the requirements for an electronic signature under penalty of perjury are contained in the Trial Court Records Manual.~~

Judicial Council of California

455 Golden Gate Avenue · San Francisco, California 94102-3688
www.courts.ca.gov/policyadmin-invitationstocomment.htm

INVITATION TO COMMENT

[ItC prefix as assigned]-__

Title Technology: Rules Modernization Project	Action Requested Review and submit comments by June 8, 2018
Proposed Rules, Forms, Standards, or Statutes Adopt Judicial Council Form EFS-006-CV.	Proposed Effective Date January 1, 2019
Proposed by Information Technology Advisory Committee Hon. Sheila F. Hanson, Chair Civil and Small Claims Advisory Committee Hon. Ann I. Jones, Chair	Contact Andrea Jaramillo, 916-263-0991 andrea.jaramillo@jud.ca.gov Anne Ronan, 415-865-8933 anne.ronan@jud.ca.gov

Executive Summary and Origin

As part of the Rules Modernization Project, the Information Technology Advisory Committee and Civil and Small Claims Advisory Committee recommend adopting a new form for withdrawal of consent to electronic service. The purpose of the proposal 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.

The Proposal

The proposed form is Judicial Council form EFS-006-CV, *Withdrawal of Consent to Electronic Service*. Under Code of Civil Procedure section 1010.6(a)(6), "A party or other person who has provided express consent to accept service electronically may withdraw consent at any time by completing and filing with the court the appropriate Judicial Council form. The Judicial Council shall create the form by January 1, 2019." The proposed form is modeled after current form EFS-005-CV, *Consent to Electronic Service and Notice of Electronic Service Address.*

Alternatives Considered

Because the form is required by statute, no alternative was considered.

Implementation Requirements, Costs, and Operational Impacts

It is not expected that the new form will result in any significant costs or operational impacts on the courts.

Attachments and Links.

1. Proposed Judicial Council form EFS-006-CV, *Withdrawal of Consent to Electronic Service*.
2. Code of Civil Procedure section 1010.6, *http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1010.6&lawCode=CCP*.

EFS-006-CV

ATTORNEY OR PARTY WITHOUT ATTORNEY: STATE BAR NO: NAME: FIRM NAME: STREET ADDRESS: CITY: STATE: ZIP CODE: TELEPHONE NO.: FAX NO. : E-MAIL ADDRESS: ATTORNEY FOR (*name*):	***FOR COURT USE ONLY***
SUPERIOR COURT OF CALIFORNIA, COUNTY OF STREET ADDRESS: MAILING ADDRESS: CITY AND ZIP CODE: BRANCH NAME:	CASE NUMBER:
Plaintiff/Petitioner: Defendant/Respondent:	JUDICIAL OFFICER:
WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE	DEPARTMENT:

1. ☐ The following party or ☐ the attorney for:
   a. ☐ plaintiff *(name):*
   b. ☐ defendant *(name):*
   c. ☐ petitioner *(name):*
   d. ☐ respondent *(name):*
   e. ☐ other *(describe):*

   withdraws consent to electronic service of notices and documents in the above-captioned action.

2. The mailing address for service on the person identified in item 1 is *(specify):*
   Street:
   City:
   State: Zip:

3. All notices and documents regarding the action shall be served on the person identified in item 1 at the address in item 2 as of *(date):*

Date:

TYPE OR PRINT NAME

▶ (SIGNATURE OF PARTY OR ATTORNEY)

Form Approved for Optional Use
Judicial Council of California
EFS-006-CV [New January 1, 2019]

WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE
(Electronic Filing and Service)

Code Civ. Proc., § 1010.6(a)(6)
www.courts.ca.gov

CASE NAME:	CASE NUMBER:

(Note: *If you serve* Withdrawal of Consent to Electronic Service *by mail, you should use form POS-030,* Proof of Service by First-Class Mail–Civil, *instead of using this page.)*

PROOF OF ELECTRONIC SERVICE

WITHDRAWAL OF CONSENT TO ELECTRONIC SERVICE

1. I am at least 18 years old.

   My residence or business address is *(specify):*

2. I electronically served a copy of the *Withdrawal of Consent to Electronic Service* as follows:

   a. Name of person served:

   b. Electronic service address of person served:

      On behalf of *(name or names of parties represented, if person served is an attorney):*

   c. On *(date):*

   ☐ Electronic service of the *Withdrawal of Consent to Electronic Service* on additional persons is described in an attachment.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Date:

(TYPE OR PRINT NAME OF DECLARANT)

(SIGNATURE OF DECLARANT)

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue · San Francisco, California 94102-3688
www.courts.ca.gov/policyadmin-invitationstocomment.htm

INVITATION TO COMMENT

[ItC prefix as assigned]-__

Title
Technology: Remote Access to Electronic Records

Proposed Rules, Forms, Standards, or Statutes
Amend Cal. Rules of Court, rules 2.500—2.503; adopt rules 2.515—2.528 and rules 2.540—2.545.

Proposed by
Information Technology Advisory Committee
Hon. Sheila F. Hanson, Chair

Action Requested
Review and submit comments by June 8, 2018

Proposed Effective Date
January 1, 2019

Contact
Andrea L. Jaramillo, (916) 263-0991
andrea.jaramillo@jud.ca.gov

Executive Summary and Origin

The proposal makes limited amendments to rules governing public access to electronic trial court records, and creates a new set of rules governing remote access to such records by parties, parties' attorneys, court-appointed persons, authorized persons working in a legal organization or qualified legal services project, and government entities. The purpose of the proposal is to facilitate existing relationships and provide clear authority to the courts.

The project to develop the new rules originated with the *California Judicial Branch Tactical Plan for Technology (2017-2018)*. Under the tactical plan, a major task under the "Technology Initiatives to Promote Rule and Legislative Changes" is to develop rules "for online access to court records for parties and justice partners[.]" (Judicial Council of Cal., *California Judicial Branch Tactical Plan for Technology (2017-2018)* (2017), p. 47.)

Background

Existing rules govern public access to electronic trial court records (Cal. Rules of Court, rules 2.500—2.507), but do not govern access to such records by parties, their attorneys, or justice partners. (See Cal. Rules of Court, rule 2.501(b).) Because courts are moving swiftly forward with making remote access to records available to these persons and entities, it is important to provide authority and guidance for the courts and others on these expanded forms of remote access.

Under the leadership of the Information Technology Committee (ITAC), nine advisory committees[1] formed the Joint Ad Hoc Subcommittee on Remote Access to develop remote access rules applicable to parties, their attorneys, and justice partners. The formation of the Joint Ad Hoc Subcommittee for this purpose was approved by the advisory bodies' internal oversight committees.

The Proposal

The existing rules governing electronic access to trial court records are found in of chapter 2 of division 4 of title 2 of the California Rules of Court (hereafter, chapter 2). Chapter 2's rules currently apply "only to access to court records by the public" and limit what is remotely accessible by the public to registers of action, calendars, indexes, and court records in specific case types. (Cal. Rules of Court, rules 2.501(b), 2.503(b).) The rules in chapter 2 "do not limit access to court records by a party to an action or proceeding, by the attorney of a party, or by other persons or entities that are entitled to access by statute or rule." (Rule 2.501(b).)

Because chapter 2 only limits *public* remote access, there is a gap in the rules with respect to persons and entities that are not the public at large such as parties, parties' attorneys, and justice partners. Courts have had to fill this gap on a piecemeal, ad hoc basis. The purpose of the proposal is to create a new set of rules applicable statewide governing remote access to electronic records to provide more structure, guidance, and authority for the courts. The proposal does not create a right to remote access and it does not provide for a higher level of access to court records using remote access than one would get by viewing court records at the courthouse.

The proposal restructures and expands the scope of chapter 2. The proposal breaks chapter 2 into four articles to cover not only access by the public, but also to cover access by parties, their attorneys, legal organizations, court-appointed persons, and government entities. In brief, the new structure consists of:

- **Article 1: General Provisions.** This article builds on existing rules, covers broad concepts on access to electronic records, and expands on the definitions of terms used in chapter 2.
- **Article 2: Public Access.** This article consists of the existing public access rules, with minor amendments.
- **Article 3: Remote Electronic Access by a Party, Party's Attorney, Court-Appointed Person, or Authorized Persons Working in a Legal Organization or Qualified Legal Services Project.** The content of this article is new and covers remote electronic access by those listed in the article's title.

[1] ITAC, Appellate Advisory Committee, Family and Juvenile Law Advisory Committee, Probate and Mental Health Advisory Committee, Advisory Committee on Providing Access and Fairness, Traffic Advisory Committee, Civil and Small Claims Advisory Committee, Criminal Law Advisory Committee, and Tribal Court-State Court Forum.

- **Article 4: Remote Electronic Access by Government Entities.** The content of this article is new and covers remote electronic access by government entities.

Article 1: General Provisions

This article builds on existing rules and broadens the scope of chapter 2 beyond public access.

Rule 2.500. Statement of Purpose. The proposal amends the rule to expand the scope of the chapter to include access by parties, parties' attorneys, legal organizations, court-appointed persons, and government entities. Language on access to confidential and sealed records is stricken from subdivision (c) because the rules do allow access to such records for those who would be legally entitled to access them, e.g., while the public at large may not be legally entitled to access a sealed record under any circumstance, a party that could access a sealed record at the courthouse would be able to access that record remotely under the new rules.

Rule 2.501. Application, scope, and information to the public. The proposal amends subdivision (a) to provide more explanation of what types of records are and are not within the scope of chapter 2's provisions. Chapter 2 only governs access to "court records" as defined in chapter 2 and not any other type of record that is not a "court record." The proposal also adds an advisory committee comment providing additional details about the limitation in the scope of the rules to "court records."

The proposal amends subdivision (b) by striking out the existing language and replacing it with a new provision. The existing language is stricken out because the rules of the chapter in the proposal expand the scope beyond public access and so the limitations in the existing language are no longer applicable. Because the new rules expand the scope of remote access by allowing a greater level of remote access by certain persons and entities, the new provision requires courts to provide information to the public on who may access their court records under the rules of the chapter. Courts may provide the information by linking to information that will be publicly posted on courts.ca.gov and may also supplement with information on their own sites in plain language.

Rule 2.502. Definitions. The proposal expands on the definitions found in rule 2.502 by adding new terms applicable to the expanded scope of chapter 2. The proposal also makes minor edits to the existing definitions. Most of the definitions are discussed in other sections below where the terms are applicable. For example, the meaning of "government entity" is discussed below in conjunction with article 4, which covers remote access by government entities.

One item of note, however, is that within the scope of chapter 2, a "person" is a natural human being. The reason for this is that the remote access rules are highly person-centric when describing who can access what. Ultimately, the new rules contemplate that there will be some natural human being remotely accessing electronic court records and the rules identify which natural humans are authorized to do so. This is not to say the organizational entities cannot have access, but they must do so through natural persons.

Article 2: Public Access

Article 2 largely retains the existing public access rules found in rules 2.503—2.507. Rule 2.503 is the only one of these rules with substantive amendments and those amendments are minor. The amendments clarify that the rules in article 2 only apply to access to electronic records by the public.

The amendments also make a technical change to the list of electronic records to which a court must provide for electronic access by the public. Under rule 2.503(b), all records in civil cases must be available remotely, if feasible, except for those listed in rule 2.503(c)(1)—(9). Rule 2.503(c) lists all the case types where electronic access must be provided at the courthouse, but must not be provided remotely. However, under rule 2.503(c) there are ten case types, not nine. The omission in rule 2.503(b) of the tenth case type was accidental. Rule 2.503(c) was amended effective January 1, 2012 with an addition of a tenth case type, but there was no corresponding amendment to the reference to the list in rule 2.503(b). The proposal corrects the incongruity between subdivisions (b) and (c) of rule 2.503.

Article 3: Remote Electronic Access by a Party, Party's Attorney, Court-Appointed Person, or Authorized Persons Working in a Legal Organization or Qualified Legal Services Project

Article 3 contains new rules to cover remote electronic access by a party, party's attorney, court-appointed person, or authorized persons working in a legal organization or qualified legal services project. Each of these types of remote accessors are discussed below. The rules make clear that article 3 is not intended to limit remote electronic access available under article 2 (the public access rules). Accordingly, if someone could have remote electronic access to a court record under article 2, that person may do so without meeting the requirements of article 3. The rules under article 3, like the public access rules, require courts to provide remote electronic access if it is feasible to do so. Finally, the rules in article 3 include requirements for identity verification, security of confidential information, and additional conditions of access.

The rules in article 3 have occasional, intentional repetition with a goal of ensuring that the rules are clear for a person accessing the records. For example, under rule 2.515, which is the rule explaining the scope of article 3, there is a provision stating that article 3 does not limit the access available under article 2. This is repeated in rule 2.517, which is the rule applicable to parties. This is so that parties, who may not be versed in reading rules of court, do not have to search to understand that their ability to gain public access in article 2 is not limited by rule.

Rule 2.515. Application and scope. The proposed rule provides an overview of the scope of article 3 and who may access electronic records under article 3.

Rule 2.516. Remote access to extent feasible. The proposed rule requires courts to allow remote access to electronic records to the types of users identified in rule 2.515. This is similar to the

public access requirement existing in rule 2.503. The advisory committee comment recognizes financial means of technical capabilities may impact the feasibility of providing remote access.

Rule 2.517. Remote access by a party. The proposed rule allows broad access to remote electronic court records to a person (defined as a natural human being in the definitions in rule 2.502) when accessing electronic records in actions or proceedings in which that person is a party. The reason for this limitation is that there must ultimately be a natural human being who accesses the records. Parties that are not natural human beings can still gain access to their own electronic records, but must do though through an attorney or other "authorized person" under the other rules in article 3 or, for certain government entities, article 4.

Rule 2.518. Remote access by a party's designee. The proposed rule allows a party who is a natural person to designate other persons to access the party's electronic records provided that the party is at least 18 years of age. The rule allows the party to set limits on the designee's access such as to specific cases or for a specific period of time. In addition, the designee may only have the same access to a party's electronic records that a member of the public would be entitled to if he or she were to inspect the party's court records at the courthouse. For example, if a court record is sealed and the designee would not be entitled to view the court record at the courthouse, the designee cannot remotely access the electronic record. The rule sets forth basic terms of access, though there may be additional terms in a user agreement set by the court. The rule does not prescribe a particular method for establishing a designation as this may depend on the preferences and technical capabilities of individual courts.

Rule 2.519. Remote access by a party's attorney. The proposed rule allows a party's attorney to remotely access electronic records in the party's actions or proceedings. Remote access may also be provided to an attorney appointed by the court to represent a party pending the final order of appointment. Attorneys may also potentially gain access through rule 2.518, in which case, the provisions of that rule rather than 2.519 would apply.

Attorneys who are attorneys of record should be known to the court for remote access purposes since they are of record. The rule also accounts for providing remote access to attorneys who are not the attorneys of record in an underlying proceeding who may nonetheless be assisting a party. For example, an attorney may be assisting a party with limited aspects of their case, like document preparation, without becoming the attorney of record. Rule 2.518(c) requires an attorney who is not of record to obtain the party's consent to remotely access the party's court records and represent to the court in the remote access system that the attorney has obtained the party's consent. This provides a mechanism for an attorney not of record to be known to the court and provides the court with assurance that the party has agreed to allow the attorney to remotely access the party's electronic records. The proposed rule also sets forth basic terms of access.

Rule 2.520. Remote access by persons working in the same legal organization as a party's attorney. Because attorneys often work with other attorneys and legal staff, proposed rule 2.519

allows remote access by persons "working in" the same "legal organization" as a party's attorney. Both "legal organization" and "working in" are broad in scope. Under the definitions in rule 2.502, "legal organization" means "a licensed attorney or group of attorneys, nonprofit legal aid organization, government legal office, in-house legal office of a non-governmental organization, or legal program organized to provide for indigent criminal, civil, or juvenile law representation." Those "working in" the same legal organization as a party's attorney may include partners, associates, employees, volunteers, and contractors. The goal with the definition of "legal organization" and the scope of "working in" is intended to capture a full range of ways that attorneys may be working together and with others to provide representation to a party.

Under rule 2.519, a party's attorney can designate other persons working in the same legal organization to have remote access and the attorney must certify that those persons are working in the same legal organization and assisting the attorney with the party's case. The rule does not require certification to take any specific form. The proposed rule also sets forth basic terms of access.

Rule 2.521. Remote access by a court-appointed person. There are proceedings where the court may appoint someone to participate in a proceeding or represent the interests of someone who is not technically a "party" to a proceeding (e.g., a minor child in a custody proceeding). The rule provides common examples of court-appointed persons, but does not limit remote access to those examples. The proposed rule also sets forth basic terms of access.

Rule 2.522. Remote access by persons working in a qualified legal services project providing brief legal services. The proposed rule allows remote access to electronic records by persons "working in" a "qualified legal services project" providing "brief legal services." The rule contemplates legal aid programs offering limited, short-term services to individuals with their court matters.

"Brief legal services" for purposes of chapter 2 is defined in rule 2.502 and means "legal assistance provided without, or prior to, becoming a party's attorney. It includes advice, consultation, research, investigating case facts, drafting documents, and making limited third party contacts on behalf of a client."

The rule only applies to qualified legal services projects as defined in Business and Professions Code section 6213(a). The purpose of this limitation is to ensure that the organizations are bona fide entities subject to professional standards. The definition of "qualified legal services project" under Business and Professions Code 6213(a) is:

(1) A nonprofit project incorporated and operated exclusively in California that provides as its primary purpose and function legal services without charge to indigent persons and that has quality control procedures approved by the State Bar of California.

(2) A program operated exclusively in California by a nonprofit law school accredited by the State Bar of California that meets the requirements of subparagraphs (A) and (B).

(A) The program shall have operated for at least two years at a cost of at least twenty thousand dollars ($20,000) per year as an identifiable law school unit with a primary purpose and function of providing legal services without charge to indigent persons.

(B) The program shall have quality control procedures approved by the State Bar of California.

Where an attorney from a qualified legal services project does become a party's attorney and offers services beyond the scope contemplated under this rule, the remote access rules for a party's attorney would also provide a mechanism for access as could the party's designee rule. The proposed rule also sets forth basic terms of access.

Rule 2.523. Identity verification, identity management, and user access. The proposed rule requires a court to verify of a person eligible to have remote access to electronic records under article 3. Subdivision (b) describes the responsibilities of the court to verify identities and provide unique credentials to users. The rule does not prescribe any particular mechanism for identity verification or credentials as the best solutions may differ from court-to-court. Subdivision (c) describes responsibilities of users to provide necessary information for identity verification, consent to conditions of access, and only access the records the user is authorized to access. Subdivision (d) describes responsibilities of legal organizations and qualified legal services projects to verify the identity of users it designates and notify the court when a user is no longer working in the legal organization or qualified legal services project. Subdivision (e) makes it clear that courts may enter into contracts or participate in statewide master agreements for identity verification, identity management, or access management systems.

Rule 2.524. Security of confidential information. The proposed rule requires that where there is information in an electronic record that is confidential by law or sealed by court order, remote access must be provided through a secure platform and transmissions of the information must be encrypted. Like with the identity verification requirements, courts may participate in contracts for secure access and encryption services.

Rule 2.525. Searches and access to electronic records in search results. The proposed rule allows users who have access under article 3 to search for records by case number or case caption. The court must ensure that only users authorized to remotely access electronic records are able to access those records. The limitation on searches by case number or case caption is intended to prevent inadvertent unauthorized access. However, recognizing that unauthorized access may still occur, the rule includes measures for the user to take in that event.

Rule 2.526. Audit trails. The purpose of the proposed rule is to ensure courts are able to see who remotely accessed electronic records, under whose authority the user gained access, what electronic records were accessed, and under whose authority the user gained access. The audit trail is a tool to assist the courts in identifying and investigating any potential issues or misuse of remote access. The rule also requires the court to provide limited audit trails to authorized users remotely accessing remote records under article 3. The limited audit trail would only show who remotely access electronic records in a particular case, but would not show which specific electronic records were accessed. The reason for this more limited view at the case level rather than individual electronic record level is to protect confidential information.

Rule 2.527. Additional conditions of access. The proposed rule requires courts to impose reasonable conditions on remote electronic access to preserve the integrity of court records, prevent the unauthorized use of information, and limit possible legal liability. The court may require users to enter into user agreements defining the terms of access, providing for compliance audits, specifying the scope of any liability, and providing for sanctions for misuse up to and including termination of remote access. The court may require each user to submit a signed, written agreement, but the rule does not prescribe any particular format or technical solution for the signature or agreement.

Rule 2.528. Termination of remote access. The proposed rule makes clear that remote access to electronic records is a privilege and not a right and that courts may terminate any grant of permission for remote access.

Article 4: Remote Electronic Access by Government Entities

Article 4 contains new rules to cover remote access by government entities for legitimate governmental purposes by persons the government entities authorize. Under the definitions in rule 2.502, "government entity" means "a legal entity organized to carry on some function of the State of California or a political subdivision of the State of California. A government entity is also a federally recognized Indian tribe or a reservation, department, subdivision, or court of a federally recognized Indian tribe."

Rule 2.540. Application and scope. The proposed rule identifies which government entities may have remote access to which types of electronic records and is geared toward government entities that have a high volume of business before the court with respect to certain case types. Because it may be impossible to anticipate all needs across California's 58 counties and superior courts, the rule includes a "good cause" provision under which a court may grant remote access to electronic court records in particular case types beyond those specifically identified in the rule. The standard for "good cause" is that the government entity requires access to the electronic records in order to adequately perform its statutory duties or fulfill its responsibilities in litigation.

The proposed rule does not preclude government entities from gaining access to court records through articles 2 and 3. The proposed rule does not grant higher levels of access to court records

than currently exists. Rather, like with the rules under article 3, it only provides for remote access to records that the government entity would be able to obtain if its agents appeared at the courthouse to inspect the records in person.

Rule 2.541. Identity verification, identity management, and user access. The proposed rule largely mirrors rule 2.523 and describes responsibilities of the court, authorized persons, and government entities for identity verification and user access. The proposed rule also makes it clear that courts may enter into contracts or participate in statewide master agreements for identity verification, identity management, or access management systems.

Rule 2.542. Security of confidential information. The proposed rule largely mirrors rule 2.524 in requiring secured platforms and encryption of confidential or sealed electronic records, and authorizes courts to participate in contracts for secure access and encryption services.

Rule 2.543. Audit trails. The proposed rule mirrors rule 2.526 requiring the court to be able to generate audit trails and provide limited audit trails to authorized users.

Rule 2.544. Additional conditions of access. The proposed rule mirrors rule 2.527 requiring courts to impose reasonable conditions of access.

Rule 2.545. Termination of remote access. The proposed rule makes clear that remote access to electronic records is a privilege and not a right and that courts may terminate any grant of permission for remote access.

Implementation Requirements, Costs, and Operational Impacts

The rules require the courts to provide remote access under the new rules if it is feasible to do so and the rules recognize that financial and technological limitations may impact the feasibility of providing remote access. If feasible, implementation would require courts to create user agreements and have systems capable of complying with the rules. Costs and specific implementation requirements would be variable across the courts depending on current capabilities and approach to providing services.

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments on the following:

- Does the proposal appropriately address the stated purpose?
- Proposed rule 2.518 would allow a person who is a party and who is at least 18 years of age, to designate other persons to have remote access to the party's electronic records. What exceptions, if any, should apply where a person under 18 years of age could designate another?
- The reference to "concurrent jurisdiction" in proposed rule 2.540(b)(1)(xi) is intended to capture cases in which a tribal entity would have a right to access the court records at the court depending on the nature of the case and type of tribal involvement. Is "concurrent jurisdiction" the best way to describe such cases or would a different phrasing be more accurate?
- Is the standard for "good cause" in proposed rule 2.540(b)(1)(xii) clear?
- The proposed rules have some internal redundancies. This was intentional in development of the rules with the goal of reducing the number of places someone reading the rules would need to look to understand how they apply. For example, "terms of access" in article 4 repeat across different types of users to limit how many rules a user would need to review to understand certain requirements. As another example, rules on identity verification requirements repeat in articles 4 and 5. Does the organization of the rules, including the redundant language, provide clear guidance? Would another organizational scheme be clearer?

The advisory committee also seeks comments from *courts* on the following cost and implementation matters:

- Would the proposal provide cost savings? If so please quantify.
- What would the implementation requirements be for courts? For example, training staff (please identify position and expected hours of training), revising processes and procedures (please describe), changing docket codes in case management systems, or modifying case management systems.
- What implementation guidance, if any, would courts find helpful?

Attachments and Links

1. Proposed rules 2.500, 2.501, 2.502, 2.503, 2.515, 2.516, 2.517, 2.518, 2.519, 2.520, 2.521, 2.522, 2.523, 2.524, 2.525, 2.526, 2.527, 2.528, 2.540, 2.541, 2.542, 2.543, 2.544, and 2.545 of the California Rules of Court.

Rules 2.500, 2.501, 2.502, and 2.503 of the California Rules of Court are amended and rules 2.515, 2.516, 2.517, 2.518, 2.519, 2.520, 2.521, 2.522, 2.523, 2.524, 2.525, 2.526, 2.527, 2.528, 2.540, 2.541, 2.542, 2.543, 2.544, and 2.545 of the California Rules of Court are adopted, effective January 1, 2019, to read:

Title 2. Trial Court Rules

Division 1. General Provisions

Chapter 2. ~~Public~~ Access to Electronic Trial Court Records

Article 1. General Provisions

Rule 2.500. Statement of purpose

(a) Intent

The rules in this chapter are intended to provide the public, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities with reasonable access to trial court records that are maintained in electronic form, while protecting privacy interests.

(b) Improved technologies provide courts with many alternatives to the historical paper-based record receipt and retention process, including the creation and use of court records maintained in electronic form. Providing ~~public~~ access to trial court records that are maintained in electronic form may save the courts, ~~and~~ the public, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities time, money, and effort and encourage courts to be more efficient in their operations. Improved access to trial court records may also foster in the public a more comprehensive understanding of the trial court system.

(c) No creation of rights

The rules in this chapter are not intended to give the public, parties, parties' attorneys, legal organizations, court-appointed persons, and government entities a right of access to any record that they are not otherwise legally entitled to access. ~~The rules do not create any right of access to records that are sealed by court order or confidential as a matter of law.~~

Advisory Committee Comment

The rules in this chapter acknowledge the benefits that electronic ~~court~~ records provide but attempt to limit the potential for unjustified intrusions into the privacy of individuals involved in litigation that can occur as a result of remote access to electronic ~~court~~ records. The proposed rules take into account the limited resources currently available in the trial courts. It is contemplated that the rules may be modified to provide greater electronic access as ~~the~~ courts'

technical capabilities improve and ~~with the~~ knowledge is gained from the experience of ~~the courts in~~ providing electronic access under these rules.

Rule 2.501. Application, ~~and~~ scope, and information to the public

(a) Application and scope

The rules in this chapter apply only to trial court records as defined in Rule 2.502 (4). They do not apply to statutorily mandated reporting between or within government entities, the California Courts Protective Order Registry, or any other documents or materials that are not court records.

(b) ~~Access by parties and attorneys~~ Information to the public

~~The rules in this chapter apply only to access to court records by the public. They do not limit access to court records by a party to an action or proceeding, by the attorney of a party, or by other persons or entities that are entitled to access by statute or rule.~~

The website for each trial court must include a link to information that will inform the public of who may access their electronic records under the rules in this chapter and under what conditions they may do so. This information will be posted publicly on *www.courts.ca.gov*. Each trial court may post additional information, in plain language, as necessary to inform the public about the level of access that the particular trial court is providing.

Advisory Committee Comment

The rules on remote access do not apply beyond court records to other types of documents, information, or data. Rule 2.502 defines a court record as "any document, paper, or exhibit filed in an action or proceeding; any order or judgment of the court; and any item listed in Government Code section 68151(a), 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, materials in the California Courts Protective Order Registry, statutorily mandated reporting between government entities, judicial administrative records, court case information, or compilations of data drawn from court records where the compilations are not themselves contained in a court record." (Rule 2.502(4), Cal. Rules of Court.) Thus, courts generate and maintain many types of information that are not court records and to which access may be restricted by law. Such information is not remotely accessible as court records, even to parties and their attorneys. If parties and their attorneys are entitled to access to any such additional information, separate and independent grounds for that access must exist.

Rule 2.502. Definitions

As used in this chapter, the following definitions apply:

(1) "Authorized person" means a person authorized by a legal organization, qualified legal services project, or government entity to access electronic records.

(2) "Brief legal services" means legal assistance provided without, or before, becoming a party's attorney. It includes advice, consultation, research, investigating case facts, drafting documents, and making limited third party contacts on behalf of a client.

~~(1)~~(3) "Court record" is any document, paper, or exhibit filed ~~by the parties to~~ in an action or proceeding; any order or judgment of the court; and any item listed in Government Code section 68151(a), excluding any reporter's transcript for which the reporter is entitled to receive a fee for any copy, that is maintained by the court in the ordinary course of the judicial process. The term does not include the personal notes or preliminary memoranda of judges or other judicial branch personnel, materials in the California Courts Protective Order Registry, statutorily mandated reporting between or within government entities, judicial administrative records, court case information, or compilations of data drawn from court records where the compilations are not themselves contained in a court record.

(4) "Court case information" consists of information created and maintained by a court about a case or cases that is not part of the court records that are filed with the court. This includes information in the case management system and case histories.

~~(4)~~(5) "Electronic access" means ~~computer~~ access by electronic means to court records available ~~to the public~~ through both public terminals at the courthouse and remotely, unless otherwise specified in the rules in this chapter.

~~(2)~~(6) "Electronic record" is a ~~computerized~~ court record that requires the use of an electronic device to access~~, regardless of the manner in which it has been computerized~~. The term includes both a ~~document~~ record that has been filed electronically and an electronic copy or version of a record that was filed in paper form. The term does not include a court record that is maintained only on paper, microfiche, or any other medium that can be read without the use of an electronic device.

(7) "Government entity" means a legal entity organized to carry on some function of the State of California or a political subdivision of the State of California. A

government entity is also a federally recognized Indian tribe or a reservation, department, subdivision, or court of a federally recognized Indian tribe.

(8) "Legal organization" means a licensed attorney or group of attorneys, nonprofit legal aid organization, government legal office, in-house legal office of a non-governmental organization, or legal program organized to provide for indigent criminal, civil, or juvenile law representation.

(9) "Party" means a plaintiff, defendant, cross-complainant, cross-defendant, petitioner, respondent, intervenor, objector, or anyone expressly defined by statute as a party in a court case.

(10) "Person" means a natural human being.

~~(3)~~(11) "The public" means a person, a group, or an entity, including print or electronic media, ~~or the representative of an individual, a group, or an entity~~ regardless of any legal or other interest in a particular court record.

(12) "Qualified legal services project" has the same meaning under the rules of this chapter as in 6213(a) of the Business and Professions Code.

(13) "Remote access" means electronic access from a location other than a public terminal at the courthouse.

(14) "User" means an individual person, a group, or an entity that accesses electronic records.

Article 2. Public Access

Rule 2.503. ~~Public access~~ Application and scope

(a) General right of access by the public

(1) All electronic records must be made reasonably available to the public in some form, whether in electronic or in paper form, except those that are sealed by court order or made confidential by law.

(2) The rules in this article apply only to access to electronic records by the public.

(b) Electronic access required to extent feasible

A court that maintains the following records in electronic form must provide electronic access to them, both remotely and at the courthouse, to the extent it is feasible to do so:

(1) * * *

(2) All records in civil cases, except those listed in (c)(1)–~~(9)~~(10).

(c) Courthouse electronic access only

A court that maintains the following records in electronic form must provide electronic access to them at the courthouse, to the extent it is feasible to do so, but may provide public remote ~~electronic~~ access only to the records ~~governed by~~ specified in subsection (b):

(1)–(10) * * *

(d) * * *

(e) Remote ~~electronic~~ access allowed in extraordinary criminal cases

Notwithstanding (c)(5), the presiding judge of the court, or a judge assigned by the presiding judge, may exercise discretion, subject to (e)(1), to permit remote ~~electronic~~ access by the public to all or a portion of the public court records in an individual criminal case if (1) the number of requests for access to documents in the case is extraordinarily high and (2) responding to those requests would significantly burden the operations of the court. An individualized determination must be made in each case in which such remote ~~electronic~~ access is provided.

(1) In exercising discretion under (e), the judge should consider the relevant factors, such as:

(A) * * *

(B) The benefits to and burdens on the parties in allowing remote ~~electronic~~ access, including possible impacts on jury selection; and

(C) * * *

(2) The court should, to the extent feasible, redact the following information from records to which it allows remote access under (e): driver license numbers; dates of birth; social security numbers; Criminal Identification and Information and National Crime Information numbers; 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. This subdivision does not apply to any document in the original court file; it applies only to documents that are available by remote ~~electronic~~ access.

(3) Five days' notice must be provided to the parties and the public before the court makes a determination to provide remote ~~electronic~~ access under this rule. Notice to the public may be accomplished by posting notice on the court's Web site. Any person may file comments with the court for consideration, but no hearing is required.

(4) The court's order permitting remote ~~electronic~~ access must specify which court records will be available by remote ~~electronic~~ access and what categories of information are to be redacted. The court is not required to make findings of fact. The court's order must be posted on the court's Web site and a copy sent to the Judicial Council.

(f)-(i) * * *

Advisory Committee Comment

The rule allows a level of access by the public to all electronic records that is at least equivalent to the access that is available for paper records and, for some types of records, is much greater. At the same time, it seeks to protect legitimate privacy concerns.

Subdivision (c). This subdivision excludes certain records (those other than the register, calendar, and indexes) in specified types of cases (notably criminal, juvenile, and family court matters) from public remote ~~electronic~~ access. The committee recognized that while these case records are public records and should remain available at the courthouse, either in paper or electronic form, they often contain sensitive personal information. The court should not publish that information over the Internet. However, the committee also recognized that the use of the Internet may be appropriate in certain criminal cases of extraordinary public interest where information regarding a case will be widely disseminated through the media. In such cases, posting of selected nonconfidential court records, redacted where necessary to protect the privacy of the participants, may provide more timely and accurate information regarding the court proceedings, and may relieve substantial burdens on court staff in responding to individual requests for documents and information. Thus, under subdivision (e), if the presiding judge makes individualized

determinations in a specific case, certain records in criminal cases may be made available over the Internet.

Subdivisions (f) and (g). These subdivisions limit electronic access to records (other than the register, calendars, or indexes) to a case-by-case basis and prohibit bulk distribution of those records. These limitations are based on the qualitative difference between obtaining information from a specific case file and obtaining bulk information that may be manipulated to compile personal information culled from any document, paper, or exhibit filed in a lawsuit. This type of aggregate information may be exploited for commercial or other purposes unrelated to the operations of the courts, at the expense of privacy rights of individuals.

Courts must send a copy of the order permitting remote ~~electronic~~ access in extraordinary criminal cases to: Criminal Justice Services, Judicial Council of California, 455 Golden Gate Avenue, San Francisco, CA 94102-3688.

Rule 2.504-2.507 * * *

Article 3. Remote Access by a Party, Party's Attorney, Court-Appointed Person, or Authorized Person Working in a Legal Organization or Qualified Legal Services Project

Rule 2.515. Application and scope

(a) No limitation on access to electronic records available through article 2

The rules in this article do not limit remote access to electronic records available under article 2.

(b) Who may access

The rules in this article apply to remote access to electronic records by:

(1) A person who is a party;

(2) A party's attorney;

(3) An authorized person working in the same legal organization as a party's attorney;

(4) An authorized person working in a qualified legal services project providing brief legal services;

(5) A court-appointed person.

Advisory Committee Comment

Article 2 allows remote access in most civil cases and the rules in article 3 are not intended to limit that access. Rather, the article 3 rules allow broader remote access by parties, parties' attorneys, authorized persons working in legal organizations, authorized persons working in a qualified legal services project providing brief services, and court-appointed persons to those electronic records where remote access by the public is not allowed.

Under the rules in article 3, a party, a party's attorney, an authorized person working in the same legal organization as a party's attorney, or a person appointed by the court in the proceeding basically has the same level of access to electronic records remotely that they would have if they were to seek to inspect the records in person at the courthouse. Thus, if they are legally entitled to inspect certain records at the courthouse, they could view the same records remotely; on the other hand, if they are restricted from inspecting certain court records at the courthouse (for example, because the records are confidential or sealed), they would not be permitted to view the records remotely. In some types of cases, such as unlimited civil cases, the access available to parties and their attorneys is generally similar to the public's but in other types of cases, such as juvenile cases, it is much more extensive (see Cal. Rules of Court, rule 5.552).

For authorized persons working in a qualified legal services program, the rule contemplates services offered in high-volume environments on an ad hoc basis. There are some limitations on access under the rule for qualified legal services projects. Where an attorney at a qualified legal services project does become a party's attorney and offers services beyond the scope contemplated under this rule, the access rules for a party's attorney would apply.

Rule 2.516. Remote access to extent feasible

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 conditions and limitations stated in this article and otherwise provided by law.

Advisory Committee Comment

This rule takes into account the limited resources currently available in some trial courts. Many courts may not have the financial means or the technical capabilities necessary to provide the full range of remote access to electronic records authorized by this article. When it is more feasible and courts have more experience with remote access, these rules may be modified to further expand remote access.

Rule 2.517. Remote access by a party

(a) Remote access generally permitted

A person may have remote access to electronic records in actions or proceedings in which that person is a party.

(b) Level of remote access

(1) In any action or proceeding a party may be provided remote access to the same electronic records that he or she would be legally entitled to inspect at the courthouse.

(2) This rule does not limit remote access to electronic records available under article 2.

(3) This rule applies only to electronic records. A person is not entitled under these rules to remote access to any documents, information, data, or other types of materials created or maintained by the courts that are not electronic records.

Advisory Committee Comment

Because this rule only permits remote access by a party who is a person (defined under rule 2.501 as a natural person), it would not apply to organizational parties, which would need to gain remote access through the party's attorney rule or, for certain government entities with respect to specified electronic records, the rules in article 4.

Rule 2.518. Remote access by a party's designee

(a) Remote access generally permitted

A person, who is at least 18 years of age, may designate other persons to have remote access to electronic records in actions or proceedings in which that person is a party.

(b) Level of remote access

(1) A party's designee may have the same access to a party's electronic records that a member of the public would be entitled to if he or she were to inspect the party's court records at the courthouse.

(2) A party may limit the access to be afforded a designee to specific cases.

(3) A party may limit the access to be afforded a designee to a specific period of time.

(4) A party may modify or revoke a designee's level of access at any time.

(c) Terms of access

(1) A party's designee may access electronic records only for the purpose of assisting the party or the party's attorney in the action or proceeding.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to the records obtained under this article.

(4) Party designees must comply with any other terms of remote access required by the court.

(5) Failure to comply with these rules may result in the imposition of sanctions including termination of access.

Advisory Committee Comment

A party must be a natural person to authorize designees for remote access. Under rule 2.501, for purposes of the rules, "persons" are natural persons. Accordingly, the party designee rule would not apply to organizational parties, which would need to gain remote access through the party's attorney rule or, for certain government entities with respect to specified electronic records, the rules in article 4.

Rule 2.519. Remote access by a party's attorney

(a) Remote access generally permitted

(1) A party's attorney may have remote access to electronic records in the party's actions or proceedings under this rule or rule 2.518. If a party's attorney gains remote access through rule 2.518, the requirements of rule 2.519 do not apply

(3) If a court notifies an attorney of the court's intent to appoint the attorney to represent a party in a criminal, juvenile justice, child welfare, family law, or

probate proceeding, the court may grant remote access to that attorney before an order of appointment is issued by the court.

(b) Level of remote access

A party's attorney may be provided remote access to the same electronic records in the party's actions or proceedings that the party's attorney would be legally entitled to view at the courthouse.

(c) Terms of remote access for attorneys who are not the attorney of record in the party's actions or proceedings in the trial court

An attorney who represents a party, but who is not the party's attorney of record, may remotely access the party's electronic records, provided that the attorney:

(1) Obtains the party's consent to remotely access the party's electronic records.

(2) Represents to the court in the remote access system that the attorney has obtained the party's consent to remotely access the party's electronic records.

(d) Terms of remote access for all attorneys accessing electronic records

(1) A party's attorney may remotely accesses the electronic records only for the purposes of assisting the party with the party's court matter.

(2) A party's attorney may not distribute for sale any electronic records obtained remotely under the rules in this article. Such sale is strictly prohibited.

(3) A party's attorney must comply with any other terms of remote access required by the court.

(4) Failure to comply with these rules may result in the imposition of sanctions including termination of access.

Advisory Committee Comment

Subdivision (c). An attorney of record will be known to the court for purposes of remote access. However, there may be circumstances when a person engages an attorney for assistance, but that attorney is not the attorney of record in an action or proceeding in which the person is a party. Examples include, but are not limited to, when a party engages an attorney to (1) prepare legal documents, but not appear in the party's action (e.g., provide limited scope representation); (2) assist the party with dismissal/expungement or sealing of a criminal record where the attorney did not represent the party in the criminal proceeding; or (3) represent the party in an appellate matter

when the attorney did not represent the party in the trial court. Subdivision (c) provides a mechanism for an attorney not of record to be known to the court for purposes of remote access.

Rule 2.520. Remote access by persons working in the same legal organization as a party's attorney

(a) Application and scope

(1) This rule applies when a party's attorney is assisted by others working in the same legal organization.

(2) "Working in the same legal organization" under this rule includes partners, associates, employees, volunteers, and contractors.

(3) This rule does not apply when a person working in the same legal organization as a party's attorney gains remote access to records as a party's designee under rule 2.518.

(b) Designation and certification

(1) A party's attorney may designate that other persons working in the same legal organization as the party's attorney have remote access.

(2) A party's attorney must certify that the other persons authorized for access are working in the same legal organization as the party's attorney and are assisting the party's attorney in the action or proceeding.

(c) Level of remote access

(1) Persons designated by a party's attorney under subdivision (b) must be provided access to the same electronic records as the party.

(2) Notwithstanding subdivision (b), when a court designates a legal organization to represent parties in criminal, juvenile, family, or probate proceedings, the court may grant remote access to a person working in the organization who assigns cases to attorneys working in that legal organization.

(d) Terms of remote access

(1) Persons working in a legal organization may remotely access electronic records only for purposes of assigning or assisting a party's attorney.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to the records obtained under this article.

(4) Persons working in a legal organization must comply with any other terms of remote access required by the court.

(5) Failure to comply with these rules may result in the imposition of sanctions including termination of access.

Rule 2.521. Remote access by a court-appointed person

(a) Remote access generally permitted

(1) A court may grant a court-appointed person remote access to electronic records in any action or proceeding in which the person has been appointed by the court.

(2) Court-appointed persons include an attorney appointed to represent a minor child under Family Code section 3150; a Court Appointed Special Advocate volunteer in a juvenile proceeding; an attorney appointed under Probate Code section 1470, 1471, or 1474; an investigator appointed under Probate Code section 1454; a probate referee designated under Probate Code section 8920; a fiduciary, as defined in Probate Code section 39; an attorney appointed under Welfare and Institutions Code section 5365; or a guardian ad litem appointed under Code of Civil Procedure section 372 or Probate Code section 1003.

(b) Level of remote access

A court-appointed person may be provided with the same level of remote access to electronic records as the court-appointed person would be legally entitled if he or she were to appear at the courthouse to inspect the court records.

(c) Terms of remote access

(1) A court-appointed person may remotely access electronic records only for purposes of fulfilling the responsibilities for which he or she was appointed.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to the records obtained under this article.

(4) A court-appointed person must comply with any other terms of remote access required by the court.

(5) Failure to comply with these rules may result in the imposition of sanctions including termination of access.

Rule 2.522. Remote access by persons working in a qualified legal services project providing brief legal services

(a) Application and scope

(1) This rule applies to qualified legal services projects as defined in section 6213(a) of the Business and Professions Code.

(2) "Working in a qualified legal services project" under this rule means attorneys, employees, and volunteers.

(3) This rule does not apply to a person working in or otherwise associated with a qualified legal services project who gains remote access to court records as a party's designee under rule 2.518.

(b) Designation and certification

(1) A qualified legal services project may designate persons working in the qualified legal services project who provide brief legal services, as defined in article 1, to have remote access.

(2) The qualified legal services project must certify that the authorized persons work in their organization.

(c) Level of remote access

Authorized persons may be provided remote access to the same electronic records to which the authorized person would be legally entitled to inspect at the courthouse.

(d) Terms of remote access

(1) Qualified legal services projects must obtain the party's consent to remotely access the party's electronic records.

(2) Authorized persons must represent to the court in the remote access system that the qualified legal services project has obtained the party's consent to remotely access the party's electronic records.

(3) Qualified legal services projects providing services under this rule may remotely access electronic records only to provide brief legal services.

(4) Any distribution for sale of electronic records obtained under the rules in this article is strictly prohibited.

(5) All laws governing confidentiality and disclosure of court records apply to electronic records obtained under this article.

(6) Qualified legal services projects must comply with any other terms of remote access required by the court.

(7) Failure to comply with these rules may result in the imposition of sanctions including termination of access.

Rule 2.523. Identify verification, identity management, and user access

(a) Identity verification required

Before allowing a person who is eligible under the rules in article 3 to have remote access to electronic records, a court must verify the identity of the person seeking access.

(b) Responsibilities of the court

A court that allows persons eligible under the rules in article 3 to have remote access to electronic records must have an identity proofing solution that verifies the identity of, and provides a unique credential to, each person who is permitted remote access to the electronic records. The court may authorize remote access by a person only if that person's identity has been verified, the person accesses records using the credential provided to that individual, and the person complies with the terms and conditions of access, as prescribed by the court.

(c) Responsibilities of persons accessing records

A person eligible to be given remote access to electronic records under the rules in article 3 may be given such access only if that person:

(1) Provides the court with all information it directs in order to identify the person to be a user;

(2) Consents to all conditions for remote access required by article 3 and the court; and

(3) Is authorized by the court to have remote access to electronic records.

(d) Responsibilities of the legal organizations or qualified legal services projects

(1) If a person is accessing electronic records on behalf of a legal organization or qualified legal services project, the organization or project must approve granting access to that person, verify the person's identity, and provide the court with all the information it directs in order to authorize that person to have access to electronic records.

(2) If a person accessing electronic records on behalf of a legal organization or qualified legal services project leaves his or her position or for any other reason is no longer entitled to access, the organization or project must immediately notify the court so that it can terminate the person's access.

(e) Vendor contracts, statewide master agreements, and identity and access management systems

A court may enter into a contract with a vendor to provide identity verification, identity management, or user access services. Alternatively, if a statewide identity verification, identity management, or access management system, or a statewide master agreement for such systems is available, courts may use those for identity verification, identity management, and user access services.

Rule 2.524. Security of confidential information

(a) Secure access and encryption required

If any information in an electronic record that is confidential by law or sealed by court order may lawfully be provided remotely to a person or organization described in rule 2.515, any remote access to the confidential information must be provided through a secure platform and any electronic transmission of the information must be encrypted.

(b) Vendor contracts and statewide master agreements

A court may enter into a contract with a vendor to provide secure access and encryption services. Alternatively, if a statewide master agreement is available for secure access and encryption services, courts may use that master agreement.

Advisory Committee Comment

This rule describes security and encryption requirements while levels of access are provided for in rules 2.517–2.522.

Rule 2.525. Searches and access to electronic records in search results

(a) Searches

A user authorized under this article to remotely access a party's electronic records may search for the records by case number or case caption.

(b) Access to electronic records in search results

A court providing remote access to electronic records under this article must ensure that authorized users are only able to access the electronic records at the levels provided in this article.

(c) Unauthorized access

If a user gains access to an electronic record that the user is not authorized to access under this article, the user must:

(1) Report the unauthorized access to the court as directed by the court for that purpose;

(2) Destroy all copies, in any form, of the record; and

(3) Delete from the user's browser history all information that identifies the record.

Rule 2.526. Audit trails

(a) Ability to generate audit trails required

The court must have the ability to generate an audit trail that identifies each remotely accessed record, when an electronic record was remotely accessed, who remotely accessed the electronic record, and under whose authority the user gained access to the electronic record.

(b) Limited audit trails available to authorized users

(1) A court providing remote access to electronic records under this article must make limited audit trails available to authorized users under this article

(2) A limited audit trail must show the user who remotely accessed electronic records in a particular case, but must not show which specific electronic records were accessed.

Rule 2.527. Additional conditions of access

To the extent consistent with these rules and other applicable law, a court must impose reasonable conditions on remote access to preserve the integrity of its records, prevent the unauthorized use of information, and limit possible legal liability. The court may choose to require each user to submit a signed, written agreement enumerating those conditions before it permits that user to remotely access electronic records. The agreements may define the terms of access, provide for compliance audits, specify the scope of liability, and provide for the imposition of sanctions for misuse up to and including termination of remote access.

Rule 2.528. Termination of remote access

(a) Remote access a privilege

Remote access to electronic records under this article is a privilege and not a right.

(b) Termination by court

A court that provides remote access may terminate the permission granted to any person eligible under the rules in article 3 to remotely access electronic records at any time for any reason.

Article 4. Remote Access by Government Entities

Rule 2.540. Application and scope

(a) Applicability to government entities

The rules in this article provide for remote access to electronic records by government entities described in subsection (b) below. The access allowed under these rules is in addition to any access these entities or authorized persons working for such entities may have under the rules in articles 2–3.

(b) Level of remote access

(1) A court may provide authorized persons from government entities with remote access to electronic records as follows:

(i) Office of the Attorney General: criminal electronic records and juvenile justice electronic records.

(ii) California Department of Child Support Services: family electronic records.

(iii) Office of a district attorney: criminal electronic records and juvenile justice electronic records.

(iv) Office of a public defender: criminal electronic records and juvenile justice electronic records.

(v) County department of probation: criminal electronic records, juvenile justice electronic records, and child welfare electronic records.

(vi) Office of city attorney: criminal electronic records, juvenile justice electronic records, and child welfare electronic records.

(vii) Office of county counsel: criminal electronic records, mental health electronic records, child welfare electronic records, and probate electronic records.

(viii) County child welfare agency: child welfare electronic records.

(ix) County public guardian: criminal electronic records, mental health electronic records, and probate electronic records

(x) County agency designated by the board of supervisors to provide conservatorship investigation under chapter 3 of the Lanterman-Petris-Short Act (Welf. & Inst. Code, §§ 5350–5372): criminal electronic records, mental health electronic records, and probate electronic records.

(xi) Federally recognized Indian tribe (including any reservation, department, subdivision, or court of the tribe) with concurrent jurisdiction: child welfare electronic records, family electronic records, juvenile justice electronic records, and probate electronic records.

(xii) For good cause, a court may grant remote access to electronic records in particular case types to government entities beyond those listed in (b)(1)(i)-(xi). For purposes of this rule, "good cause" means that the government entity requires access to the electronic records in order to adequately perform its statutory duties or fulfill its responsibilities in litigation.

(xiii) All other remote access for government entities is governed by articles 2–3.

(2) Subject to (b)(1), the court may provide a government entity with the same level of remote access to electronic records as the government entity would be legally entitled to 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.

(3) This rule applies only to electronic records. A government entity is not entitled under these rules to remote access to any documents, information, data, or other types of materials created or maintained by the courts that are not electronic records.

(c) Terms of remote access

(1) Government entities may remotely access electronic records only to perform official duties and for legitimate governmental purposes.

(2) Any distribution for sale of electronic records obtained remotely under the rules in this article is strictly prohibited.

(3) All laws governing confidentiality and disclosure of court records apply to electronic records obtained under this article.

(4) Government entities must comply with any other terms of remote access required by the court.

(5) Failure to comply with these requirements may result in the imposition of sanctions including termination of access.

Advisory Committee Comment

Subdivision (b)(3). On the applicability of the rules on remote access only to electronic records, see Advisory Committee Comment to rule 2.501.

Rule 2.541. Identify verification, identity management, and user access

(a) Identity verification required

Before allowing a person or entity eligible under the rules in article 4 to have remote access to electronic records, a court must verify the identity of the person seeking access.

(b) Responsibilities of the courts

A court that allows persons eligible under the rules in article 4 to have remote access to electronic records must have an identity proofing solution that verifies the identity of, and provides a unique credential to, each person who is permitted remote access to the electronic records. The court may authorize remote access by a person only if that person's identity has been verified, the person accesses records using the name and password provided to that individual, and the person complies with the terms and conditions of access, as prescribed by the court.

(c) Responsibilities of persons accessing records

A person eligible to remote access to electronic records under the rules in article 4 may be given such access only if that person:

(1) Provides the court with all information it needs to identify the person to be a user;

(2) Consents to all conditions for remote access required by article 4 and the court; and

(3) Is authorized by the court to have remote access to electronic records.

(d) Responsibilities of government entities

(1) If a person is accessing electronic records on behalf of a government entity, the government entity must approve granting 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.

(2) If a person accessing electronic records on behalf of a government entity leaves his or her position or for any other reason is no longer entitled to access, the government entity must immediately notify the court so that it can terminate the person's access.

(e) Vendor contracts, statewide master agreements, and identity and access management systems

A court may enter into a contract with a vendor to provide identity verification, identity management, or user access services. Alternatively, if a statewide identity verification, identity management, or access management system or a statewide master agreement for such systems is available, courts may use those to for identity verification, identity management, and user access services.

Rule 2.542. Security of confidential information

(a) Secure access and encryption required

If any information in an electronic record that is confidential by law or sealed by court order may lawfully be provided remotely to a government entity, any remote access to the confidential information must be provided through a secure platform and any electronic transmission of the information must be encrypted.

(b) Vendor contracts and statewide master agreements

A court may enter into a contract with a vendor to provide secure access and encryption services. Alternatively, if a statewide master agreement is available for secure access and encryption services, courts may use that master agreement.

Rule 2.543. Audit trails

(a) Ability to generate audit trails required

The court must have the ability to generate an audit trail identifying when an electronic record was remotely accessed, who remotely accessed the electronic record, and under whose authority the user gained access to the electronic record.

(b) Audit trails available to government entity

(3) A court providing remote access to electronic records under this article must make limited audit trails available to authorized users of the government entity.

(4) A limited audit trail must show the user who remotely accessed electronic records in a particular case, but must not show which specific electronic records were accessed.

Rule 2.544. Additional conditions of access]

To the extent consistent with these rules and other applicable law, a court must impose reasonable conditions on remote access to preserve the integrity of its records, prevent the unauthorized use of information, and protect itself from liability. The court may choose to require each user to submit a signed, written agreement enumerating those conditions before it permits that user to access electronic records remotely. The agreements may define the terms of access, provide for compliance audits, specify the scope of liability, and provide for sanctions for misuse up to and including termination of remote access.

Rule 2.545. Termination of remote access

(a) Remote access a privilege

Remote access under this article is a privilege and not a right.

(b) Termination by court

A court that provides remote access may terminate the permission granted to any person or entity eligible under the rules in article 4 to remotely access electronic records at any time for any reason.