CALIFORNIA JUDICIAL BRANCH

Branchwide Identity and Access Management Workstream

Findings and Recommendations (2021)

VERSION 1.0

NOVEMBER 9, 2021

JUDICIAL COUNCIL OF CALIFORNIA
INFORMATION TECHNOLOGY ADVISORY COMMITTEE

Table of Contents

1.0 EXECUTIVE SUMMARY

This report is the work product of the Identity and Access Management (IAM) Workstream, charged with developing a judicial branch identity management strategy and consulting on the selection of an identity management provider. The goal was to acquire an identity and access management service that will allow customers to access courts and court-related service providers (such as court case management portals and electronic filing service providers) using a single sign-on mechanism.

The recommendations in this report provide a path to ensuring that electronic access for the public, the courts, and justice partners to judicial branch resources is both secure and easy to use. Courts and the Judicial Council have already deployed solutions using the branchwide identity management platform selected: Microsoft Azure Identity Management.

The Identity and Access Management Workstream attempted to (1) understand the use cases, (2) make recommendations on technologies and technology standards, and (3) inform policy-making bodies of how identity and access management can further the mission of the branch.

Use cases that benefit from IAM include:

- Privileged remote access to case information
- Electronic filing
- Online payments of fees and fines
- Online reservations for court services
- Online document assembly
- Online dispute resolution
- Digital evidence management, and
- Remote participation in court hearings

These use cases (and many others) informed the workstream's evaluation in the areas of technology standards to adopt and technology products to be leveraged.

Recommendations

In summary, the workstream makes the following recommendations. For additional details, please see section 7.0, Workstream Recommendations:

1. Establish ongoing governance and a process for policy and technology decisions.
2. Develop and deploy a branchwide identity management platform and program supported by Judicial Council Information Technology (JCIT) that would:
    (1) Create a branchwide ID (CalCourtID) with clearly defined minimum identity attributes and the ability for users to control sharing.
    (2) Establish a process for identity proofing where the judicial branch will be the authentication authority for public users (business-to-consumer, B2C), and

authentication for courts and justice partners with MOUs (business-to-business, B2B) will be federated.

(3) Enable migration of existing identity management implementations used by courts and other service providers.

(4) Implement multi-factor authentication (MFA) and use it everywhere access needs to be protected.

(5) Provide litigants and attorneys the ability to temporarily delegate their access levels to another registered user. Delegated access should be reaffirmed every six (6) months, and the delegator should have access to delegee activities.

(6) Include provisions in judicial branch requests for proposal (RFPs) that mandate use of branchwide identity management.

3. Establish funding for branchwide identity management support.

2.0 INTRODUCTION

The digital economy has impacted how we bank, how we shop, and how we connect with others. Every day we use online digital identities to complete tasks, or share an opinion. Even before the pandemic, courts were increasingly moving transactions online that were historically done at the courthouse. Most courts provide the ability to pay traffic tickets online and provide public access to information consistent with California Rules of Court, rule 2.500 et seq.

These more basic online capabilities can largely be done anonymously. While the court will certainly verify the authenticity of the credit card used to pay a traffic ticket, they do not need to know that the ticket was paid for by the defendant, or a family member, or a friend. The court need only capture that the fine was successfully paid.

As courts move to more advanced remote services, anonymity may no longer be appropriate. This is most evident in remote access to case records. Litigants, attorneys, and justice partners are entitled to greater access to case information than the general public (Cal. Rules of Court, rule 2.515 et seq.). Beyond remote access, certainty about the person consuming an online court service enhances justice. Online dispute resolution, electronic filing, electronic evidence submissions, and participants in a confidential remote hearing all benefit from a level of certainty about the person(s) interacting with the court.

While the court is largely a public institution that provides public access to information, the access to some information is protected. A key objective behind existing policies and procedures is to protect individuals and the court from inappropriate disclosure of information.

The purpose of Identity and Access Management (IAM) is to ensure that people have the appropriate access to technology resources. Said differently, IAM keeps unauthorized persons away from protected information. As such, IAM is integral to the mission of the court in the digital age and part of a broader cyber-security capability. But IAM goes beyond protection: It also attempts to improve the user experience and productivity of the court, its partners, and the public.

This is the focus of identity and access management: Connecting physical and online identities in order to conduct business with the court securely and digitally.

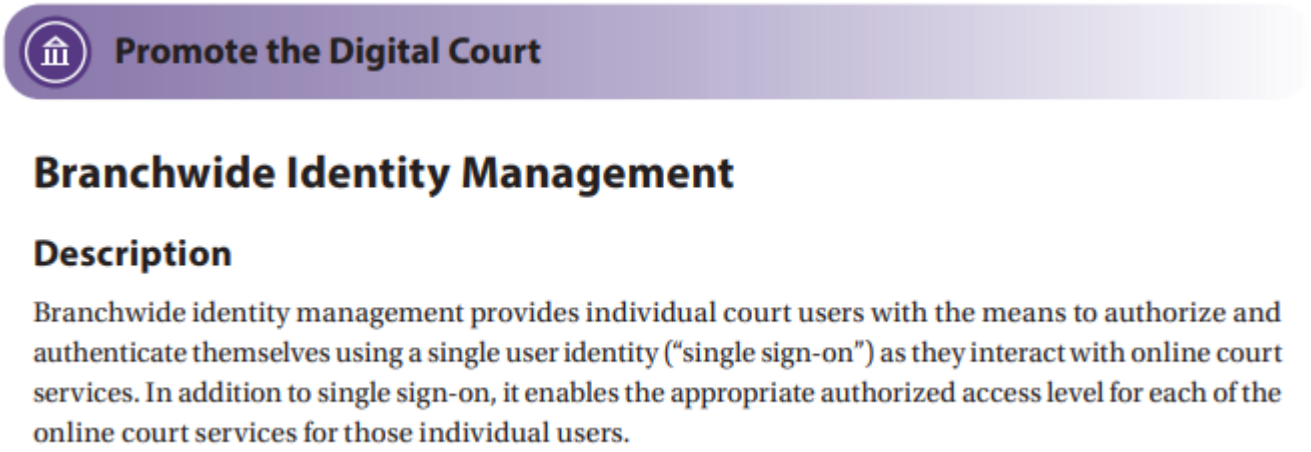
3.0 GOAL ALIGNMENT

Identity and access management aligns directly with the Judicial Council's Strategic Plan for Technology goals to:

1. **Promote the Digital Court**
   Increase access to the courts, administer justice in a timely and efficient manner, and optimize case processing by supporting a foundation for the digital court and by implementing comprehensive digital services for the public and for justice.

3. **Advance IT Security and Infrastructure**
   Invest in a secure, scalable, and reliable technology infrastructure as a foundation for providing digital services and public access, while maintaining a focus on privacy protections and security.

The Judicial Council Information Technology Advisory Committee has explicitly prioritized identity (and access) management in the Tactical Plan for Technology.[1]



4.0 WHAT IS IDENTITY MANAGEMENT?

There are many definitions of identity management, but almost all of them settle on the technologies, policies, and processes required to ensure that people have the appropriate access to information and resources. Or, that unauthorized people do not have access to protected information and resources.

[1] Judicial Council of Cal., *Tactical Plan for Technology 2021–2022* (Dec. 2020), pp. 17–19, https://www.courts.ca.gov/documents/jctc-Court-Technology-Tactical-Plan.pdf

The National Institute of Standards and Technology definition of identity management is:

> *Identity management may be described as the process of managing the identification, authentication, and authorization associated with individuals or entities (devices, processes, etc.).*

Source: NIST http://dx.doi.org/10.6028/NIST.IR.8014

Case: Privileged remote access to case information

Identification

Fundamentally, there are two types of user identities, internal and external.

Internal user identities are managed by the organization to which the individual is affiliated. The organization is responsible for adding and deleting users and modify their privileges consistent with their duties. Organizations have policies and procedures for managing identities and thus these individuals are treated differently than external users.

Examples of court-related internal identities include:

- Judicial officer;
- Court employee;
- Employee of the district attorney; and
- Employee of Child Welfare Services.

For remote access to case information, the active affiliation of the user with the organization is the identification. The analog equivalent is a badge. If the individual shows their official identification they are presumed to be currently affiliated with that organization. Should their affiliation be terminated, the presumption is that the issuing organization has retrieved the badge.

In the digital world, this is managed by activation/deactivation of a user account.

External user identities, on the other hand, are external to the court (or justice partner) and are managed differently. They are not inherently known to the court, and the identity management system and processes must take steps to link the physical and online identities of these individuals and determine what systems and services they are authorized to interact with, and what actions they can perform within those systems and services.

Examples of court-related external identities include:

- Litigant;
- Attorney;
- Member of the public; and
- Member of the media.

Authentication

Authentication is "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system."[2]

In the digital world authentication is typically managed by a user identity and password. Occasionally, based on the sensitivity of the information or service being provided a second form of authentication may be required, such as a code sent to your mobile phone (multi-factor authentication).

Whether single or multi-factor, the authentication process relies on the individual to provide the virtual keys to enter.

Authorization

Authorization is "the right or a permission that is granted to a system entity to access a system resource."[3]

A simple illustration is a hotel room key. The key (as well as every other current hotel guest key) will open the lobby doors after hours but will only open a particular room. The holder of the key is authorized to access the lobby and has a privileged authorization to access a specific room.

Likewise, the virtual key provided to an authenticated user will provide access only to the case files the user is allowed to see based on their identity and relationship to the case.

Authentication and authorization combined ensure that the users are who they say they are, and that they have the right to access the requested files.[4]

5.0 WHY DO WE NEED BRANCHWIDE IDENTITY MANAGEMENT?

Identity and access management allows Judicial Branch Entities (JBEs) to protect individuals and courts from unauthorized or malicious access to information and services. It is rooted in security and privacy. But a well-crafted identity management solution can also provide convenience and an improved user experience.

[2] National Institute of Standards and Technology (NIST), *https://csrc.nist.gov/glossary/term/authentication*
[3] National Institute of Standards and Technology (NIST), *https://csrc.nist.gov/glossary/term/Security_Authorization*
[4] Examples of user types contained in the California Rules of Court that must be supported:

- A person who is a party
- A designee of a person who is a party
- A party's attorney
- An authorized person working in the same legal organization as a party's attorney
- An authorized person working in a qualified legal services project providing brief legal services
- A court-appointed person
- Government entities

Today, someone accessing judicial branch services must typically remember a user ID and password for every system they use. For a litigant, this may be a self-help site, an e-filing service provider, a court portal, and a traffic assistance program. For an attorney, this may be multiple courts' portals and multiple e-filing service providers. A branchwide identity management service will enable these users to have a single "CalCourtID" and password that gives them access to multiple services. This is called *single sign-on*.

In addition, some services can bundle access to different systems into a single application. A person using an online dispute resolution (ODR) system may need information from their case file in the case management system. The ODR system can access that information using the person's credentials. Applications and services that are built with identity management at their core provide an enhanced user experience.

Finally, identity management is the foundation for a digital court ecosystem that encompasses courts, justice partners, and vendors. It enables transactions for which knowing the person using or consuming services is important, such as:

- Electronic filing;
- Online payment;
- Online reservations;
- Remote privileged access;
- Online document assembly;
- Remote appearances;
- Online dispute resolution; and
- Electronic evidence management.

Microsoft Azure Active Directory was selected by JCIT as the foundation for the branchwide identity management solution based on a recommendation from the workstream. Microsoft Active Directory is currently used by almost all courts, and selecting this platform will enable courts to easily integrate with branchwide identity management. Below are current examples of how identity management is being deployed by courts in California:

Judicial Council

Online Traffic Adjudication and Ability to Pay (ATP)

ATP provides an online process to assist people struggling with traffic court debt. It offers the public a new way to request a reduction in their fees and fines without appearing at a court hearing. The public accesses the portal and fills out a questionnaire. Because their identity is confirmed using the data they provide, they are not required to create a CalCourtID and authenticate. To review the request and make a decision, court employees and bench officers log on using their local ID as the CalCourtID.

ATP is currently deployed at the Superior Courts of Fresno, Monterey, San Francisco, Santa Clara, Shasta, Tulare, and Ventura Counties.

Online Trial by Declaration

Allows litigants to contest their ticket much the way they would with a trial by written declaration. All parties will use an online system, including law enforcement. Officers will submit their "Officers Declaration" electronically, using their federated user ID as their CalCourtID to access the system.

Superior Court of Placer County

Court Remote Conferencing System

Any party that signs up for a hearing where evidence is being presented, must use the branchwide identity manager to create a username (CalCourtID) and password. The username and password are then registered with the court's conferencing system. Parties may use the branchwide identity manager for all conference types, but it is not required.

Superior Court of Los Angeles County

Attorney Portal

Provides complete access to the electronic case file to attorneys of record on a case. The attorney uses their CalCourtID, and identity proofing happens with the California State Bar.

LACourtConnect (LACC)

LACC is a remote hearing solution for Civil, Family Law, Probate, and Traffic. Remote hearing participants sign up to appear remotely using their CalCourtID. Attorney credentials are verified with the California State Bar. Non-attorney participants must still create a CalCourtID but do not go through a formal identity proofing step.

Remote Audio Attendance System (RAAP)

RAAP provides a live audio stream of a courtroom. It utilizes the audio from LACC or WebEx (used in Criminal/Juvenile). RAAP attendees must create a CalCourtID so the court can verify their email address and then provide the audio stream on the day of their hearing. There is no formal identity proofing since this is a public access service.

Online Dispute Resolution (ODR)

ODR provides a space for litigants to resolve their disputes outside of the courtroom. ODR is available to all Small Claims litigants after the initial case filing. All ODR users must create a CalCourtID to interact with the ODR system and to gain access to their electronic case file (see Litigant Portal below). Their identity is proofed by requiring the user to enter address information from the form SC-100 filing. County-provided mediators also have a CalCourtID, and the court uses the ODR vendor to "proof" their rights to view the electronic case file while they are the mediator of record.

Litigant Portal

Coming in fall 2021, the litigant portal will provide privileged remote access to the case file for all litigants whose identity has been validated upon the creation of their CalCourtID in supported litigation types.

Media Access Portal (MAP)

Access to public information for media organizations is available by registering with MAP. Individual subscribers in a media organization use court IDs, and the Communications Office verifies the media credentials for identity proofing.

6.0 WORKSTREAM APPROACH

The Identity Management Workstream was tasked with several objectives:

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

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

(c) Ensure linkage and alignment with other branchwide initiatives such as e-filing, SRL Portal, Next Generation Hosting, and CMS Migration and Deployment;

(d) Coordinate and plan with JCIT regarding operational support; and

(e) Recommend changes to rules of court as needed and work with the Rules and Policies Subcommittee to draft them.

To accomplish these goals, workstream members participated in one of two tracks, a Policy track or a Technology track. Each track had a lead who facilitated discussions. The tracks met every two weeks to discuss the objectives, provide input on artifacts, and determine next steps.

To ensure alignment with other initiatives, the Branchwide Information Security Roadmap workstream was asked to review the initial findings of this workstream, and their recommendations have been incorporated. The Master Service Agreements (MSA) for E-filing Manager vendors include provisions to use branchwide identity management. The MSAs for case management system (CMS) vendors, Journal Technologies and Justice Systems, Inc., indicate that these CMSs can be integrated easily. Tyler's custom authentication will require a greater level of effort to integrate.

Policy recommendations were documented and presented to the Technology Committee, the Information Technology Advisory Committee, the Court Information Technology Management Forum, the Trial Court Presiding Judges Advisory Committee, and the Court Executives Advisory Committee.

Critical technology functions were identified and solution alternatives explored for:

- User registration and administration—the ability for an administrator to manage users and for users to manage their own profiles;
- Advanced security—multi-factor authentication; and
- Identity proofing—ensuring users are who they say they are and ensuring they are authorized to access the information and services they are requesting.

Services have been implemented at the Superior Courts of Los Angeles and Placer Counties that use branchwide identity management. The Ability to Pay program also uses branchwide identity management. Identity management technology has advanced rapidly and will continue to evolve.

The roster of workstream members is included as Appendix A. The workstream membership, with Chief Information Officer Snorri Ogata of the Superior Court of Los Angeles County as sponsor, included participants from a diverse set of courts.

7.0 WORKSTREAM RECOMMENDATIONS

What follows are the consolidated recommendations from the Policy and the Technology tracks.

1. **Establish ongoing governance and a process for technology decisions**

   Policy questions:

   Policy questions have branchwide impact. These questions should be brought to the Technology Committee to determine who the stakeholders are, and may involve other advisory bodies for input. This should include review of pending legislation to amend section 367.7 of the Code of Civil Procedure.

   Technical questions:

   A working group should be formed of courts implementing or using branchwide identity management and Judicial Council Information Technology representatives. Proposed technical changes can be published to vendors and service providers for comment prior to implementation.

2. **Develop and deploy a branchwide identity management platform and program supported by Judicial Council Information Technology (JCIT)**

   The workstream recommends some of the technologies and tools needed to implement the branchwide identity management platform and related solutions.

   (1) **Create a Branchwide ID (CalCourtID)**

   The CalCourtID is a Global Unique Identifier that all persons who wish to use and access court services should have. As noted above, some courts and programs already implement this approach. With a true branchwide ID, the benefits of a single sign-on can be leveraged across the state.

   For partners that use Office 365/Azure AD and federate, their federated accounts become their CalCourtIDs.

   <u>User profile attributes will include:</u>

   - CalCourtID
   - Email Address: Unique identity for court services
   - Name: Required for more formal/personal communications

- Primary Affiliation Type (for access control): Individual, Party, Attorney, Justice Partner, etc.
- Primary Affiliation Authority: Court, State Bar, Agency, Law Enforcement Agency (LEA)
- Primary Affiliation Identifier: e.g., California Bar Number
- Firm Name: For attorneys
- Mobile Phone: Used for communications, password recovery, and MFA
- Alternate email address—required if no mobile phone

User must be able to control sharing

Identity information will only be shared with service providers with user consent (service provider by service provider).

One of the benefits of identity management is the ability to share common information about the user among service providers to improve the user experience (minimize duplicate data entry).

The user should always be in control of whether identity attributes are shared with each service provider.

To reduce the risk of sharing unauthorized or sensitive information, provide the ability for the user to control what data is shared, beyond the minimum needed to authenticate and authorize access. For example, a checkbox that says, "Click here if you want to only provide the minimum needed information".

JCIT administers operational support

To maximize the benefits of CalCourtID and single sign-on, branchwide support is required. This will include, but not be limited to:

- Resolving production issues;
- Onboarding support for service providers—courts, CMS vendors, Electronic Filing Service Providers (EFSP), etc.;
- Onboarding support for B2B partners—with and without Microsoft Office 365;
- Support for B2C users;
- Monitoring the health of the service;
- Developing a site for users to view their activity and that of their delegates; and
- Developing APIs and code snippets.

(2) Establish a process for identity proofing

Identity proofing is required for privileged access. For information and services available to the public, identity proofing is not necessary. The user profile must indicate whether the user has been identity proofed (and method of identity proofing). Several methods should be available, and validation stored with the profile.

The judicial branch will be the authentication authority for public (B2C) users and will federate authentication for MOU Partners (B2B).

There are two levels or steps of identity proofing:

- **Authentication.** The person is who they say they are (e.g., are you really Jane Smith?); and
- **Authorization**. The person is authorized to access specific information or services (e.g., are you the Jane Smith who is a litigant on this case and therefore allowed to look at case information?).

The court or service provider will identity-proof at the authorization level.

- For **internal identities**, the branchwide identity management Azure Active Directory or the federated Active Directory proves the user's identity (automatically each time during login). The federated partner is responsible for maintaining the authorized users under their access agreement.
- Attorney identity proofing (one time, during user registration).

  Branchwide identity management uses the California State Bar registration database to validate an attorney's Bar number and email through the following steps:

  1. The attorney registers and enters their Bar number.
  2. The State Bar registration database is queried for the email address associated with that Bar number.
  3. A validation email is sent to the email address to confirm the user's identity.

  The State Bar is responsible for maintaining the list of active attorneys for the State of California.

- Identity proofing for a member of the public (one time, during user registration).

  The default method is physical verification. The user will identify themselves at a courthouse, receiving a token (e.g. a 10-digit code valid for 24-hours) that will enable online access. Identities can also be verified through a transactional event (e.g., litigant e-filing).

  In the future, online methods and services for identity proofing will be further investigated.

(3) Enable migration of existing identity management implementations used by courts and other service providers

The migration path will be evaluated on a case-by-case basis. Possible methods include:

- Migrate with invitation-based system. Each user is emailed an invitation that forces a password reset. The user's profile information is migrated to the CalCourtID profile upon successful password reset.
- For database-oriented identity credentials, each user in the database is emailed an invitation that forces re-registering with CalCourtID and password.
- When the user signs in with their local user ID, the application prompts the user to sign in with their CalCourtID or register for a CalCourtID. If the user is registering for a new CalCourtID, the user's profile information is "migrated" to the new CalCourtID profile.

(4) Implement Multi-Factor Authentication (MFA)

Consumers expect MFA services for sensitive data (e.g., banking). Access to court information and services is sensitive and should be protected with confidence. Therefore, the individuals interacting with the online service must be authenticated and authorized for access.

For internal identities using the Microsoft Business-to-Business service, Microsoft MFA can be used and is included with the Business-to-Business platform. If federation is designed correctly, it is unlikely the service limits would be exceeded. Configuring and using Microsoft MFA is recommended.

For external identities, alternative MFA solutions are under evaluation. For example:

- Messaging services are less costly per transaction and per user than Microsoft MFA.
- A custom/third-party MFA can be configured on or off depending on the service. For example, MFA is needed for privileged case access but not to register for a self-help class.
- A custom/third-party MFA can be designed to capture costs by user and service provider.

(5) Provide litigants and attorneys the ability to temporarily delegate their access levels to another *registered* user

Internal Identities will *not* be able to delegate access, as the agency or organization must explicitly grant access to individuals.

Litigants and attorneys may have occasion to delegate their access to certain online services to another individual (relative, paralegal, etc.). An attorney only has remote privileged access to a case while they are an active participant. Once inactive

(substitution, expired bar membership), their access is suspended as is that of all delegees.

Delegee access may not exceed the access of delegator.

Delegated access should be reaffirmed every six (6) months *and* the delegator should have access to delegee activities.

To ensure adherence to branch security practices, the delegee must register with the branchwide identity management system.

Delegee access must be reaffirmed every 6 months.

Delegee activities (at service provider level) should be logged and available for review by the delegator.

(6) Include provisions in branchwide RFPs that mandate use of branchwide identity management

Vendors should be made aware of the benefits and branchwide strategy for identity management so that they can propose solutions that meet our needs and enable a better user experience for the public. There has been success with this approach in recent procurements by incorporating branchwide identity management requirements clearly in RFPs.

3. Establish funding for branchwide identity management buildout and support

Sustainable funding is required to broadly deploy, manage, and maintain this critical infrastructure. Funding would support:

- One-time setup and buildout costs for establishing the branchwide identity management platform.
- Cost of ongoing Microsoft tenant and associated services:
  - Microsoft Azure AD tenants;
  - Microsoft Developer Network (MSDN); and
  - MFA Services.
- Cost for providing ongoing operational support staffing:
  - Operational;
  - Development; and
  - Consulting and integration.

8.0 CONCLUSION

The judicial branch identity management recommendations provide a strategy and a path to enable a common platform for secured access to branch resources, while improving the user experience when accessing multiple court and Judicial Council resources. The policies will evolve over time and incorporate

new concepts and changes as needed to accommodate and reflect any changes in the law, technology, or in branch priorities and requirements in support of our goal to provide increased access to justice.

APPENDIX A: Workstream Membership

Mr. Snorri Ogata, Executive Sponsor
Chief Information Officer, Superior Court of Los Angeles County

Mr. Michael Baliel, Court Lead
Chief Information Officer, Superior Court, of Santa Clara County

Ms. Rebecca Fleming, Policy Track Lead
Court Executive Officer, Superior Court of Santa Clara County

Mr. Michael Pugh, Technical Track Lead
Chief Information Officer, Superior Court of Yuba County

Hon. Nicole M. Heeseman
Judge, Superior Court of Los Angeles County

Hon. Patricia L. Kelly
Judge, Superior Court of Santa Barbara County

Hon. Kimberly Menninger
Judge, Superior Court of Orange County

Hon. Kim Nguyen
Judge, Superior Court of Los Angeles County

Hon. Amy C. Yerkey
Judge, Superior Court of Los Angeles County

Mr. Jake Chatters
Court Executive Officer, Superior Court of Placer County

Mr. Kevin Lane
Clerk/Executive Officer, Court of Appeal, Fourth Appellate District

Ms. Tricia Penrose
Director of Juvenile Operations, Superior Court of Los Angeles County

Mr. Dennis Ma
Court Operations Manager, Civil Department, Superior Court of Orange County

Mr. Daniel Melendrez
Information Technology Manager, Superior Court of San Bernardino County

Mr. Jake Pison
Information Technology Manager, Superior Court of San Diego County

Mr. Brian Rogatsky
Information Technology Applications Manager, California Superior Court, San Diego County

Mr. Mike Sorensen
Project Manager/Data Center Supervisor, Superior Court of San Diego County

Mr. Chris Choi
Software Engineer II, Superior Court of Santa Clara County

Mr. Steve Gaul
Information Specialist II, California Superior Court, Santa Clara County

Mr. John Yee
Lead Enterprise Architect, Judicial Council of California

Mr. Eric Egner
Computer Support Specialist, Judicial Council of California

Mr. Anandkumar Kumar
IS Supervisor II, Judicial Council of California

Ms. Kathleen Fink, Project Manager
Manager, Judicial Council of California

APPENDIX B: Resources

NIST Special Publication 800-63-3

Digital Identity Guidelines (nist.gov)