Promoting Safe and Secure Government Access for All

Guidance and Model Policies to Assist State and Local Agencies in Responding to Immigration Issues Pursuant to Senate Bill 580 (2025)

Rob Bonta
California Attorney General
July 2026

Table of Contents

Introduction and Executive Summary

The California Attorney General issues this publication pursuant to Senate Bill 580 (2025), codified at Government Code section 12532.5, which directs the Attorney General to publish guidance and "model policies for state and local agencies relating to interaction with immigration authorities consistent with federal and state law."[1] As required by Senate Bill 580 (SB 580), this document also provides "guidance, audit criteria, and training recommendations for databases operated by a state or local agency, including databases maintained for the agency by private vendors, aimed at ensuring that the databases are governed in a manner that makes the availability of information therein to anyone or any entity for the purposes of immigration enforcement limited to the fullest extent practicable, consistent with federal and state law."[2] SB 580 requires state and local agencies by January 1, 2027, to adopt the model policies or their equivalent.

In enacting SB 580, the Legislature found and declared: "Immigrants are valuable and essential members of the California community and indiscriminate immigration enforcement against persons who do not pose a public safety risk to Californians has a significant negative impact on state and local functions."[3] Consistent with the Legislature's findings and intent, this document provides guidance and model policies that ensure agency practices reflect the State's interests in protecting privacy rights, preserving public trust, and maintaining the effective functioning of government. The guidance and model policies are also informed by stakeholder engagement, as SB 580 directed. The Attorney General and members of his Office thank the Governor's Office and the state and local agency representatives and members of the public who shared knowledge, experience, and insights prior to this guide's publication.

Consistent with the Legislature's findings and direction and a broad array of federal and state laws, there are several core principles that inform the guidance and model policies set forth in the pages that follow:

- First, state and local resources should not be used to assist in immigration enforcement activities, except as required by state or federal law.
- Second, agencies should limit or restrict the collection, retention, and disclosure of information that could aid in the identification or apprehension of individuals without lawful immigration status, unless required to do so by law or where the agency's lawful administration of a program requires that such information be collected, maintained, or disclosed in some manner.
- Third, where there is no legal obligation to comply with a request from immigration authorities, agencies should require appropriate legal process—such as a judicial warrant, judicial subpoena, or court order—before complying.
- Fourth, all requests for information should be directed or otherwise forwarded to the designated agency staff or legal counsel trained to evaluate such requests and ensure compliance with applicable law and agency policy.
- Fifth, agencies should document interactions with immigration authorities, including requests for information, attempts to access facilities, and the presentation of legal process.

SB 580 applies to *all* state and local agencies in California, unless otherwise exempt under California law. In addition to adopting the new model policies required by SB 580, agencies are encouraged to adopt the guidance, audit criteria, and training recommendations issued by the Attorney General which are designed to assist agencies in meeting privacy law requirements and the Legislature's goal of limiting the availability of information for immigration enforcement purposes to the fullest extent practicable consistent with federal and state law. The effectiveness of agency policies depends not only on their adoption, but also on their integration into the daily operations of the agency.

How to Use this Guide

This guide serves as both a summary of relevant laws in effect as of the date of this publication and a practical resource for implementation of agencies' legal mandates as they relate to interactions with immigration enforcement. Chapter 1 of the guide provides a brief background on federal immigration law enforcement authority, recently changed federal policy on enforcement at "sensitive" locations, states' constitutional right to decline to participate in federal immigration law enforcement, and some of the laws that California has adopted in the exercise of that right. Chapter 2 provides model policies for California agency personnel interactions with immigration authorities who seek to access physical locations, such as agency offices or other locations where agencies provide services to members of the public or conduct other agency functions. Chapter 3 provides model policies for California agency personnel interactions with immigration authorities who seek records, data, or other information from the agency. Chapter 4 provides guidance, training recommendations, and audit criteria for databases. Finally, Chapter 5 offers additional resources that agencies may wish to consult or make available to members of the public who interact with the agency or are otherwise impacted by the agency.

Agencies should use this guide to align their internal policies with this guide's model policies and recommendations, consistent with applicable law. Agencies covered by Assembly Bill 699 or Senate Bill 54 ("SB 54") should consult the more specified guidance and model policy publications, as applicable. They include the following, all of which can be found on the website of the Office of the California Attorney General:

- Guidance and Model Policies to Assist California's Superior Courts
- Guidance and Model Policies to Assist California's Healthcare Facilities
- Guidance and Model Policies to Assist California's Colleges and Universities
- Guidance and Model Policies to Assist California's K-12 Schools
- Guidance and Model Policies to Assist the Division of Labor Standards Enforcement, the Agricultural Labor Relations Board, and the Division of Workers Compensation
- Guidance and Model Policies to Assist California's Public Libraries
- Guidance and Model Policies to Assist California Shelters
- Guidance and Model Policies for Early Childhood Education and Child Care Providers Pursuant to the Family Preparedness Plan Act of 2025

This guide provides a framework for evaluating requests from immigration enforcement authorities and determining the appropriate response consistent with state and federal law, but this guide does not provide legal advice. Nothing in this guidance should be construed as directing state or local agency personnel to obstruct or provide false information to federal officers acting within the scope of their legal authority. State and local agency personnel should also not attempt to physically interfere with federal agents or law enforcement in the operation of their duties.

Where questions arise that are not directly addressed by this guidance, agencies should consult with legal counsel to ensure that their actions are consistent with applicable legal requirements.

Contact the California Attorney General's Office by email at immigration@doj.ca.gov with questions or concerns regarding interactions with immigration authorities or visit Immigration | State of California - Department of Justice - Office of the Attorney General for more information as well as resources for members of the public.

Federal Responsibility for Immigration Law

The federal government is responsible for the formulation, administration, and enforcement of immigration law.[4] U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), two agencies within the Department of Homeland Security (DHS), are primarily responsible for the enforcement of immigration law. A third DHS bureau, U.S. Citizenship and Immigration Services (USCIS), administers immigration benefits and the naturalization process. Pursuant to current policy, other federal law enforcement agencies such as the Federal Bureau of Investigation, Drug Enforcement Administration, and United States Marshals Service, may also assist in immigration enforcement.[5]

As discussed below, with specific limited exceptions, California law prohibits state and local law enforcement agencies from participating in immigration enforcement.[6] In this guide, ICE, CBP, law enforcement or other agencies, such as USCIS, attempting to enforce immigration law are treated the same in terms of the advice given for how state and local agencies should handle interactions with them. Accordingly, this guide uses the term "immigration authorities" to refer to any law enforcement agency—whether DHS, ICE, CBP, another federal agency, or a state or local law enforcement agency—that enforces, attempts to enforce, or otherwise participates in or facilitates immigration law enforcement. Any policy adopted to address interactions between agency personnel and immigration enforcement officers should encompass all law enforcement agencies that seek to enforce immigration law.

Formerly "Protected" (also known as "Sensitive") Locations

For more than thirty years, DHS and a predecessor agency, the Immigration and Naturalization Service, generally prohibited immigration enforcement actions at locations referred to as "sensitive locations" or "protected areas."[7] These locations included schools, hospitals, childcare centers, shelters, churches, funerals, protests, and other locations where individuals receive "essential services" or engage in "essential activities."[8] While the directives limiting enforcement at these locations provided for narrow exceptions, very little enforcement was carried out at sensitive locations as a practical matter. In January 2025, however, DHS rescinded the directive that limited enforcement at formerly protected sensitive locations.[9] The rescission of the protection of sensitive locations is the subject of litigation, but agencies that provide services to the public at such locations may nonetheless see increased immigration enforcement activity. The Trump administration has also rescinded a prior directive that sharply limited civil immigration enforcement at and near courthouses.[10] Since then, courthouses have become sites of increased immigration enforcement, despite law prohibiting civil arrests at courthouses.[11] Immigration enforcement at courthouses and related laws and policies have also been the subject of litigation.

State and local agencies that operate in locations that previously were shielded from immigration enforcement under prior federal agency directives should therefore be prepared for the possibility of immigration enforcement activities at their locations. This is true even where state or federal law may otherwise prohibit or limit certain enforcement activities.

No Federal Law Requires State or Local Agency Participation in Immigration Enforcement

No federal law requires a state or local agency to participate in or facilitate immigration enforcement. Similarly, while some federal and state laws prohibit or restrict data-sharing,[12] no law requires a state or local agency to provide information to immigration enforcement authorities.

A federal statute, 8 U.S.C. § 1373, provides that a "government entity or official may not prohibit, or in any way restrict, any government entity or official from sending to, or receiving from, the [federal immigration enforcement agency] information regarding the citizenship or immigration status, lawful or unlawful, of any individual."[13] Section 1373 also prohibits restrictions on maintaining or exchanging information regarding immigration status with any other federal, state, or local government entity.[14] Some lower courts have ruled that Section 1373 violates the Constitution, but no appeals court has ruled yet on whether Section 1373 is unconstitutional.[15] Regardless, this prohibition on prohibitions or restrictions on information-sharing applies only to citizenship and immigration status[16]—and not to other information such as home or work addresses, location, photographs, or other personal information—and it *does not* require that state or local agencies grant or otherwise respond to federal requests for information about citizenship or immigration status or any other information.[17]

Accordingly, courts have upheld California's and other states' laws prohibiting state and local law enforcement agencies and other agencies from sharing other information, such as a person's home address, work address, physical location, or other personal information, and courts have ruled that these limitations on information-sharing are lawful.[18] (See below for more on these laws.) California agencies can and should follow California law on this subject, and doing so will not violate Section 1373 or Section 1644. This guide does not call for any agency policy restricting agency employees in violation of 8 U.S.C. § 1373, 8 U.S.C. § 1644, or any other federal law. The model policies set forth in this publication account for both federal and state law.

California's TRUST, TRUTH, and Values Acts

Under the Tenth Amendment to the U.S. Constitution, the federal government cannot legally compel states to enact or administer a federal regulatory program.[19] California is thus constitutionally permitted to prohibit or limit the use of state and local resources to participate in, assist, or facilitate immigration enforcement,[20] and, as outlined in this guide, it has enacted a number of laws that do so. A series of enactments applicable to law enforcement agencies are briefly explained here.

In 2013, California enacted Assembly Bill 4, known as the TRUST Act. This law limited the discretion of law enforcement agencies to grant immigration "detainers," also known as "immigration holds."[21] Then, in 2016, California enacted Assembly Bill 2792, known as the Transparent Review of Unjust Transfers and Holds (TRUTH) Act.[22] The TRUTH Act, effective January 1, 2017, created mandatory notice and procedural protections for individuals in the custody of local law enforcement agencies when immigration officers wish to contact them.[23] Specifically, the law requires that when an ICE hold or transfer request is received by a local law enforcement agency, a copy of the request must be provided to the impacted individual, and notice must be given as to whether local law enforcement will comply with that request.[24] The law also requires that, before immigration enforcement can conduct an interview in a local jail, the agency must provide the person who is detained by law enforcement with a written consent form that explains the interview's purpose, that it is voluntary, and that the person can decline or request an attorney.[25] If local law enforcement gives immigration authorities a person's release date/time, the agency must also provide that same notice in writing to the individual and their attorney or designee.[26] The local governing body of any county, city, or city and county in which a local law enforcement agency has provided ICE

access to an individual during the last year must also hold at least one community forum during the following year to provide information to the public about ICE's access to individuals and to receive and consider public comment.[27] As part of this forum, the local law enforcement agency may provide the governing body with data it maintains regarding the number and demographic characteristics of individuals to whom the agency has provided ICE access, the date ICE access was provided, and whether the ICE access was provided through a hold, transfer, or notification request or through other means.[28] Data may be provided in the form of statistics or, if statistics are not maintained, individual records, provided that personally identifiable information shall be redacted.[29]

Senate Bill 54, known as the California Values Act, was signed into law in 2017, went into effect on January 1, 2018, and is codified in Government Code sections 7284, 7284.2, 7284.4, 7284.6, 7284.10, and 7284.12. The California Values Act directs that "California law enforcement agencies shall not … [u]se agency or department moneys or personnel to investigate, interrogate, detain, detect, or arrest persons for immigration enforcement purposes."[30] The statute specifically prohibits law enforcement agencies from providing for immigration enforcement purposes "information regarding a person's release date or responding to requests for notification by providing release dates or other information unless that information is available to the public, or is in response to a notification request from immigration authorities" except under limited, enumerated circumstances.[31] In particular, among other exceptions, law enforcement agencies have discretion to provide information regarding a person's release date or other information if that person has been convicted within the last five years of a misdemeanor for a crime punishable as either a misdemeanor or felony for, or has been convicted within the last fifteen years of a felony for, one or more of a number of enumerated offenses.[32] The California Values Act also prohibits providing for immigration enforcement purposes individuals' "personal information," including, but not limited to, " home address or work address unless that information is available to the public."[33] Through the California Values Act, California also elected not to participate in specific federal immigration enforcement arrangements. The law provides that California law enforcement agencies "shall not… [p]erform[] the functions of an immigration officer, whether pursuant to Section 1357(g) of Title 8 of the United States Code or any other law, regulation, or policy, whether formal or informal," and shall not " [p]lace peace officers under the supervision of federal agencies or employ peace officers deputized as special federal officers or special federal deputies for purposes of immigration enforcement."[34] The Values Act also extended the notice and consent requirements of the TRUTH Act to the California Department of Corrections and Rehabilitation (CDCR), so those requirements apply more broadly than just to county jails.

The California Values Act applies directly to law enforcement agencies. At the same time, it reflects the more broadly applicable findings of the Legislature and the policy of the State that "[i]mmigrants are valuable and essential members of the California community,"[35] trust in "state and local agencies is central to the public safety of the people of California;"[36] "trust is threatened when state and local agencies are entangled with federal immigration enforcement;[37]" "[e]ntangling state and local agencies with federal immigration enforcement programs diverts already limited resources and blurs the lines of accountability between local, state, and federal governments,"[38] and that there is a need "to ensure effective policing, to protect the safety, well-being, and constitutional rights of the people of California, and to direct the state's limited resources to matters of greatest concern to state and local governments."[39]

For more information on responsibilities of law enforcement agencies under the California Values Act, California TRUST Act, and the California TRUTH Act, please see the California Attorney General's Guidance to Assist California Law Enforcement Agencies Defining its Responsibilities Under California Values Act, the TRUTH Act, and TRUST Act. The Attorney General has published law enforcement bulletins that address compliance with governing state laws, including those established by Senate Bill 54.[40] Law enforcement agencies should review and follow these bulletins and any updates that follow.

02 Guidance and Model Policies Regarding Immigration Authorities' Access to State and Local Agency Facilities and Physical Spaces

Purpose of this Chapter

State and local agencies increasingly encounter immigration enforcement activities that occur within or around agency facilities. These interactions often involve attempts by immigration authorities to enter agency property, access nonpublic areas, locate individuals, or otherwise carry out enforcement actions within physical spaces controlled by the agency. These activities by immigration authorities into agency spaces can undermine public safety, hinder an agency's public functions, and disrupt an agency's orderly operations. Importantly, immigration authorities in and around public agencies can diminish the public's trust in the agency. Individuals who seek an agency's services should do so safely without fear or interruption, and agencies should be able to perform their functions without interference by immigration authorities.

This chapter provides agencies with model policies for evaluating and responding to immigration authorities' attempting to access agency property. The sections below address the legal standards governing physical entry into agency spaces, the distinction between public and nonpublic areas, the types of documents immigration authorities may present when seeking access, and the model policies that agencies must adopt to ensure that responses to such requests are lawful, consistent, and appropriately limited.

Governing Law

1. Fourth Amendment

The Fourth Amendment to the United States Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated," and further provides that warrants may issue only upon probable cause.[41] The Fourth Amendment protections apply to areas where there is a reasonable expectation of privacy, including nonpublic areas of government facilities.[42]

The fact that a facility is open to the public in some areas does not mean that all areas within that facility are subject to unrestricted entry by law enforcement, including immigration enforcement officers.[43] Public agencies routinely maintain areas that are not open to unrestricted public access including staff offices, employee-only workspaces, records rooms, data processing equipment rooms, intake areas, secured operational facilities, restricted-access service areas, storage facilities, and controlled administrative spaces.[44] Entry into nonpublic areas or areas where individuals have a reasonable expectation of privacy, such as a client consultation booth, may require a judicial warrant or a recognized exception to the warrant requirement. The presentation of identification does not, alone, authorize entry into protected spaces.[45] This guide does not address all the factual circumstances that may arise relating to an individual's Fourth Amendment protections in different areas of a facility. Agency personnel should immediately contact and consult the agency's legal counsel or other agency designee when presented with legal documents or questions about immigration authorities' intrusion or attempt to intrude areas of an agency where individuals may have a reasonable expectation of privacy.

2. The Immigrant Worker Protection Act

Assembly Bill 450 (AB 450), or the Immigrant Worker Protection Act,[46] imposes restrictions on physical access and records disclosure. The statute provides that "except as otherwise required by federal law, an employer, or a person acting on behalf of an employer, shall not provide voluntary consent to an immigration enforcement agent to enter any nonpublic areas of a place of labor."[47] While the statute does not define the term "voluntary consent," AB 450 guidance states "voluntary consent" should be understood as a decision made in the absence of "duress or coercion, either express or implied."[48] The prohibition against providing access to nonpublic areas does not apply where the law enforcement agent has a judicial warrant.[49] The statute does not define the meaning of "nonpublic" area nor otherwise indicate that the term "nonpublic" should be given anything but its usual or ordinary meaning. Thus, a "nonpublic" area is one that the public is not normally free to enter or access. For example, this could be an office where payroll or personnel records are kept or an area that an employer designates (for instance, by posting signs or keeping doors closed) as restricted to agency employees or management.[50] State and local agencies should work with their legal departments to identify and designate nonpublic areas.

AB 450 further provides that "an employer, or a person acting on behalf of an employer, shall not provide voluntary consent to an immigration enforcement agent to access, review, or obtain the employer's employee records without a subpoena or judicial warrant."[51] The prohibition against the voluntary consent to an immigration enforcement agent's access to employee record does not apply for records accessed pursuant to an I-9 audit and other documents requested in a notice of inspection under federal law.[52] State and local agency personnel should immediately contact their agency's legal counsel for assistance when confronted with legal documents.

AB 450's restrictions apply regardless of how a request is presented. Whether immigration enforcement officers request entry verbally, present administrative documentation, or otherwise seek access, voluntary consent to enter nonpublic areas is prohibited unless the request is supported by legally sufficient authority. Except as required by law, such as when officers present a judicial warrant or are conducting a properly noticed I-9 audit, agencies cannot voluntarily provide immigration enforcement access to nonpublic areas, whether to access individuals or records. For more guidance regarding AB 450, please review AB 450 FAQs.

3. Workplace Know Your Rights Act

The Workplace Know Your Rights Act[53] imposes additional requirements designed to ensure transparency and protect workers in the context of immigration enforcement actions. The statute requires employers to provide notice to employees of certain immigration enforcement inspections and to comply with specific obligations when enforcement activity occurs. First, it requires California employers to distribute a standalone written notice to all employees annually, detailing specified workers' rights as well as constitutional rights of an employee when interacting with law enforcement. Second, employers are required to allow workers to designate an emergency contact who must be notified if the employee is arrested or detained during work hours.[54]

Types of Demands for Access to Physical Spaces

Demands for physical access by immigration authorities may take different forms and may be for varying purposes. Immigration officers may seek to enter agency facilities to locate specific individuals, question employees or members of the public, or conduct other types of enforcement activity within or around agency-controlled spaces. These demands may be accompanied by administrative documents, judicial warrants, subpoenas, or may be unsupported by documentation. Immigration enforcement

intrusions into agency spaces implicate distinct concerns for public agencies. For instance, immigration enforcement's physical presence within agency facilities may disrupt operations, expose sensitive information, interfere with agency functions, deter individuals from accessing public services, or facilitate immigration enforcement actions directed at individuals present within agency facilities.

To protect against these consequences, agencies should evaluate demands for physical access against the laws discussed above and should ensure that personnel understand the distinction between public and nonpublic areas, the legal effect of documents presented by immigration authorities, and the employing agency's operational procedures governing responses to immigration enforcement activity.

1. Public v. Nonpublic Areas

The distinction between public and nonpublic areas is central to evaluating demands to access agency facilities. Public areas generally include portions of agency facilities open to the public during normal business,[55] such as public lobbies, reception areas, public counters, or waiting rooms. Nonpublic may include areas restricted to employees, operational personnel, contractors, or specifically authorized individuals. Nonpublic areas could also include staff offices, employee-only workspaces, records rooms, interview rooms, information technology facilities, employee-only parking areas, and other internal agency workspaces not open to the public. This could also include a private consultation booth in a public space, where a person would have a reasonable expectation of privacy.[56]

The distinction between public and nonpublic areas of a facility has legal significance. Entry into public areas where there is no reasonable expectation of privacy does not, by itself, require a warrant. Entry into nonpublic areas, however, is subject to constitutional and statutory constraints. Absent other lawful authority, immigration authorities may not enter nonpublic areas without a judicial warrant. Accordingly, agencies should consult with their legal counsel to determine the appropriate designation of public and nonpublic areas that are unique to their facilities and ensure that operational policies or practices reinforce the distinction between public and nonpublic areas. This may include signage, badge-access systems, locked doors, visitor procedures, escort requirements, or other operational controls identifying restricted-access areas.

Legal Effects of Documents

Some documents and forms convey legal authority for immigration authorities to enter a physical location or a designated area within a larger physical location while others do not. This section goes over some examples of documents that are commonly seen in the immigration enforcement context and explains which documents convey legal authority for immigration authorities to enter specified locations and which do not.

1. Notice to Appear

A Notice to Appear, sometimes referred to as an NTA, is issued pursuant to 8 U.S.C. § 1229. It serves as the charging document in removal (or deportation) proceedings and is used to initiate those proceedings before an immigration judge—it sets forth the name of the respondent (the individual whose deportation the government is seeking); the alleged citizenship and immigration status of the respondent; the allegations of inadmissibility or deportability against the individual with corresponding charge(s) under relevant statutory provisions; and it provides notice of the time and place of the removal proceedings.[57]

A Notice to Appear is an administrative document issued by an immigration officer, as reflected in the sample provided in **Appendix A**. It does not bear the signature of a judge, does not constitute judicial process, and its legal effect is limited to initiating removal proceedings. It does not confer authority to access nonpublic areas of an agency facility or require state or local agency personnel to provide aid.

Upon presentation of a Notice to Appear, the agency should respond as follows:

- Frontline staff should ask the agent for identification and documentation.
- Frontline staff shall refer the matter to the agency's legal counsel or other designated agency contact.
- Decline to provide access to any non-public area of the agency facility in accordance with AB 450 unless instructed otherwise by legal counsel.
- Decline to provide information regarding the individual's presence, location, or activities.
- Decline to facilitate contact between the individual and immigration authorities.
- Refrain from taking any action that would assist in enforcement.
- Document the interaction.

2. Administrative Arrest Warrants

Administrative arrest warrants are issued by immigration officers pursuant to statutory authority under 8 U.S.C. §§ 1226 and 1231 and implementing regulations.[58] Federal immigration authorities commonly issue administrative arrest warrants on standardized forms, including Form I-200 and Form I-205. However, other federal agencies may use other standardized forms. The guidance below applies to those agencies regardless of the specific form the administrative warrant takes. As reflected by the sample provided in **Appendix B**, administrative arrest warrants are characterized by the following, which distinguishes them from judicial warrants:

- Issued by the Department of Homeland Security.
- Signed by an immigration officer rather than a district court judge or magistrate judge.
- Lack a court seal or case number.

An administrative arrest warrant authorizes federal officers to arrest the individual named in the warrant, subject to the limitations of federal law. It does not, on its own, impose requirements on state or local agencies. An administrative arrest warrant does not:

- Authorize entry into areas where there is a reasonable expectation of privacy.
- Authorize entry into nonpublic areas of agency facilities.
- Require a state or local agency to assist in the arrest.
- Require a state or local agency to provide information or access.

When presented with an administrative arrest warrant, agency personnel should:

- Refer the matter to the agency's legal counsel or other designated agency contact.
- Decline to provide access to any non-public area of the agency facility in accordance with AB 450 and adhere to Fourth Amendment requirements, unless instructed otherwise by legal counsel.
- Decline to provide assistance in locating or identifying the individual.
- Refrain from confirming the individual's presence.
- Document the interaction.

3. Judicial Arrest or Search Warrants

Judicial arrest or search warrants are issued by a court upon a finding of probable cause. Federal judicial warrants are governed by the Fourth Amendment and Federal Rules of Criminal Procedure and reflect a determination by a neutral magistrate judge that sufficient grounds exist to authorize an arrest. As reflected in the samples provided in **Appendices C and D**, a judicial arrest or search warrant will:

- Bear the signature of a judge or magistrate judge.
- Identify the issuing court.
- Reference a criminal proceeding.
- Specify the individual to be arrested or the place to be searched.
- Often include a case number and court seal.

These features distinguish it from administrative warrants. A judicial arrest warrant authorizes law enforcement officers to arrest the individual named in the warrant and, depending on its terms, may authorize entry into specified locations. Similarly, a judicial search warrant authorizes law enforcement officers to search a specific location, person, or vehicle for evidence of a crime and to seize designated property. The scope of that authority is defined by the warrant itself and by applicable law. It does not automatically authorize entry into all areas or require the agency to take actions beyond those necessary to comply with the warrant.[59]

Upon presentation of a judicial arrest or search warrant, the agency should generally not interfere, but still immediately notify legal counsel or their designated personnel. Legal counsel or designated personnel, to the extent possible, should review the warrant to determine its scope and direct the agent to a designated area if one has been chosen.

- While designated personnel or legal counsel review the warrant, staff should invite the officer to wait in a common area.
- At no point should agency staff physically interfere, intervene, or assist with the immigration enforcement officer's execution of the warrant.
- Comply with the warrant as required by law.
- Limit compliance to the scope of the warrant.
- Ensure that any actions taken are consistent with applicable privacy and confidentiality requirements.
- Document all actions taken.

Where the scope of the warrant is unclear, or where compliance would implicate sensitive information or operations, the agency should seek clarification from the issuing court.

Model Policies

The model policies set forth below are intended to ensure that agency responses to immigration enforcement activity occurring within or around agency facilities are consistent with federal and state law, including the governing legal principles discussed in this guidance, and reflect the State's goals of limiting the use of public resources for immigration enforcement, protecting privacy, and maintaining public trust.

Below are the contents of the model policy.

General Response Protocols Regarding Requests or Intrusions by Immigration Authorities into Nonpublic Areas of a Facility

When immigration authorities seek access to state and local agency facilities, individuals, or agency-controlled spaces, agency personnel shall respond in a manner that is consistent, non-escalatory, and grounded in law. This includes the following requirements for personnel:

- Agency personnel shall remain calm and professional, request identification and any documents presented, and immediately notify designated personnel or legal counsel.
- Personnel shall not take any action that would assist or facilitate immigration enforcement unless required by law. This includes refraining from identifying individuals, confirming whether a person is present, providing language interpretation or translation or logistical support, or otherwise enabling enforcement activity.
- Personnel shall not provide voluntary consent to entry into nonpublic areas or to the disclosure of information.
- Personnel shall not rely on or interpret documents presented by immigration authorities as requiring compliance and all such determinations shall be made by designated personnel or legal counsel.
- Personnel shall not provide false information, destroy records, conceal any individual, harass or interfere with officers, or voluntarily assist officers.
- All interactions with immigration authorities shall be documented in accordance with agency policy. When documenting immigration enforcement entries into nonpublic areas or attempts to enter nonpublic areas, personnel shall document:
  - the date and time of the interaction.
  - the names and agencies of officers present.
  - the purpose asserted by immigration authorities.
  - the documents presented.
  - the areas officers sought to access.
  - the actions taken and communications by agency personnel and immigration authorities.
  - communications with legal counsel or supervisors.
  - the ultimate resolution of the interaction.

Designated Personnel or Legal Counsel

Each agency shall designate agency counsel or other agency personnel with sufficient training responsible for evaluating and responding to requests or attempted intrusions by immigration authorities. This designated agency counsel or staff should have authority to speak for the agency and be trained on the legal standards governing physical access to agency facilities, including the distinction between public and nonpublic areas, the legal effect of administrative versus judicial process, and the limits imposed by the Fourth Amendment and AB 450.

All personnel shall immediately notify designated personnel when immigration authorities request access, present legal documents, or are observed attempting to enter nonpublic areas. This requirement applies even where no formal request is made.

Designated personnel shall evaluate whether any document presented constitutes a legally sufficient process, determine whether compliance is required, and coordinate the agency's response. Centralizing these determinations ensures that agency actions are consistent with the law and prevents frontline personnel from making legal judgments outside their role.

Agencies may establish centralized points of contact or entry to ensure that all interactions with immigration authorities are routed through designated personnel.

Access to Public Areas of a Facility and Permitted Activities

Immigration authorities may enter areas of an agency facility that are open to the general public including areas where members of the public or employees do not have a reasonable expectation of privacy. However, an immigration enforcement agent's presence in public areas does not expand their legal authority or authorize access to nonpublic areas, records, or individuals.

Except where required by law, judicial process, or agency operational duties, state and local agency personnel shall not take any action within public areas that facilitate immigration enforcement. Personnel shall not identify individuals, confirm the presence or location of any person, provide information, or assist officers in navigating the facility for enforcement purposes.

To the extent practicable, agency personnel should continue to provide services without disruption. If the presence of immigration authorities causes a delay, denial, or a condition on access to services, programs, or benefits, agency staff shall document this in accordance with agency policy.

State and local agencies shall implement operational safeguards to protect personally identifiable information in public areas, including limiting the visibility of documents, screens, and intake materials, and restricting access to information that is not intended for public disclosure.

Where immigration authorities seek to move beyond public areas, personnel shall inform them that access to nonpublic areas is not permitted and will require a judicial warrant or court order. If immigration authorities persist, agency personnel should immediately notify agency counsel or other designated agency contact and, as needed, also alert a supervisor. Agency personnel should not facilitate access to nonpublic areas nor physically engage with immigration authorities. If an immigration enforcement agency presents in a facility or area open to the general public for the purpose of immigration enforcement, document the encounter to the extent feasible, including whether access refusal to nonpublic areas was met with resistance. This after-incident report may include:

1. The date, time, location, and duration of the encounter.
2. A list or copy of the credentials and contact information of each agent involved, or at least of the Agent who appeared to be in charge.
3. The identity of all personnel who communicated with the agent or personnel who witnessed the interaction.
4. Details of the agent's request, including copies of documents that were obtained.
5. Copies, photographs, or other recordings of information detailing whether the agent presented any documents along with their request to personnel, e.g. whether the agent presented a warrant or subpoena, what was requested in the warrant or subpoena, and whether the warrant or subpoena was signed by a judge.
6. Details documenting personnel's response to the agent's request.
7. Any further actions taken by the agent or any observations made.

State and local agencies can designate entry points where immigration enforcement agents may enter and check-in with state or local agency personnel and centralized contact points. Your agency may consider implementing a desk guide that includes scripts for personnel's use in responding to common or foreseeable requests or interactions with immigration enforcement agents.

Distinction Between Public and Nonpublic Areas

State and local agency policies shall clearly define and identify nonpublic areas of agency facilities, including any areas not open to the public or requiring authorization, escort, or credentialed access. The joint guidance issued by the California Department of Justice and the Labor Commissioner under AB 450 provides that "nonpublic" carries its ordinary meaning—an area that the general public is not normally free to enter or access—and that whether a given space qualifies is a factual, case-by-case determination that will depend on an assessment of all the circumstances in any given situation.[60] Applied to a typical government workplace, nonpublic areas would include staff-only offices, break rooms, file and evidence storage rooms, server rooms, employee-only corridors, detention or holding areas, and areas requiring a badge, key, or staff escort to enter. Accordingly, for purposes of this guidance, "public areas" of a government facility are those spaces the general public is normally free to enter or access without escort, appointment, or special authorization—for example, building lobbies, public counters, waiting areas, hearing rooms or courtrooms open to spectators, and parking areas designated for visitors. "Nonpublic areas," by contrast, are spaces the general public is not normally free to enter, regardless of whether those spaces are locked, marked, or otherwise physically secured.

If feasible, agencies shall maintain physical and administrative controls that reinforce the distinction between public and nonpublic areas, including signage, access controls, visitor protocols, and escort requirements. For more information on how to designate public versus nonpublic areas see AB 450 FAQs.

Requirements Regarding Nonpublic Areas

Agency policies shall establish procedures governing responses based on the type of demand presented.

When no judicial warrant is presented, [Your Agency] staff shall:

1. Immediately notify designated personnel or legal counsel that an agent is onsite.
2. Not authorize entry into nonpublic areas and inform the immigration agent that they lack authority to access. A request for voluntary consent, an administrative warrant, a Notice to Appear, or other similar documents issued by immigration authorities do not constitute judicial process.
3. Request to copy any documents presented or notate the immigration agent's credentials.
4. Immediately contact security, a supervisor, designated personnel or legal counsel if the immigration agent attempts to enter a nonpublic area. Staff should not persist and should not become confrontational when met with refusal or force.
5. Not physically interfere with or assist the immigration agent.
6. Absent a judicial warrant or unless required by federal law, agency shall decline to provide the immigration enforcement officer access to nonpublic areas of an agency facility.

When presented with a judicial search or arrest warrant, [Your Agency] staff shall:

1. Immediately notify designated personnel or legal counsel that an officer is onsite.
2. Request to make a copy of the warrant and the officer's credentials, and allow designated personnel to verify that the warrant is issued by a court, bears a judicial signature, and confirm that the location the officers seek to access is a correct match to the location listed in the warrant, and communicate clearly that access is limited to the scope of the warrant.
3. Direct the officer to wait in a public area while designated personnel or legal counsel verify the validity of the warrant. If the agent refuses to wait during these steps, staff will not block or impede entry even if entry has been denied and they have verbally instructed the agent that they are not permitted to enter.
4. Make a copy or photograph each page of the judicial warrant or court order.
5. Comply with the warrant only to the extent required by law. Compliance shall be strictly limited to the scope of the warrant, and personnel shall not provide additional information, access, or assistance beyond what is required.
6. Where appropriate, designated personnel may accompany officers to ensure that the execution of the warrant remains within its authorized scope.

Note: For a judicial arrest warrant, if the person who is the subject of the warrant is not present, staff are not required to, and therefore should not, tell the agent about the person's whereabouts or call the person to the location if they are not present.

Documentation

Agencies shall require documentation of all interactions with immigration authorities involving requests or attempts to access agency facilities. Documentation shall be maintained in a centralized location (i.e. place where agency resources, records, or operations are concentrated or accessible to agency decisionmakers) and shall include:

- The date, time, and location of the interaction.
- The identity, contact information, and agency affiliation of officers.
- The nature of the request or activity and detail of the officer's request.
- Whether the officer presented a warrant, subpoena, or court order to accompany their request, what was requested in the warrant/subpoena/court order, and whether the warrant/subpoena/court order was signed by a judge.
- The agency's response to the request.
- Any further action taken by the immigration officer.
- Photo or copy of any documents presented by the agent.

Training Regarding Facility Access

Agencies are encouraged to train agency personnel on the agency's policies and procedures. Recommendations for training are provided in this section.

Agencies should prepare personnel for circumstances in which immigration officers are physically present within public portions of facilities. Training should help staff understand the requirements under AB 450 as well as the agency's procedures regarding an immigration enforcement agent's intrusion into nonpublic areas of the agency's facility. Personnel should be trained in the requirements of Government Code sections 7285.1 and 7285.2 regarding physical access to agency facilities.

This includes:

- The agency's policy regarding distinctions between public and nonpublic areas of an agency facility.
- The prohibition on providing voluntary consent to enter nonpublic areas.
- The requirement to refer requests for access to designated personnel.
- The need to avoid facilitating enforcement actions.

Training should address how these rules apply in actual interactions, including situations in which officers verbally request entry, present administrative documents, or assert authority or willfully enter without presenting a judicial warrant. Training should also ensure that frontline personnel are not expected to make the above-discussed determinations and should, instead, forward a request from immigration authorities to the designated agency personnel and/or legal counsel.

Agencies should also incorporate scenario-based guidance into training to assist personnel in applying legal and operational principles consistently in real-world settings. Scenario-based training is a teaching modality where learners engage with realistic, job-relevant situations to practice response and problem-solving. Applying this principle to your agency could include role-playing, interactive digital scenarios, or facilitated discussions centered around the types of immigration enforcement interactions the agency has faced or is likely to face.

For example, immigration authorities may seek access to a staff-only operational workspace while presenting an administrative warrant. In such circumstances, agency personnel should receive training that directs them to request identification and copies of the documents presented, explain that access to nonpublic areas requires review through agency procedures, contact designated personnel or legal counsel, refrain from voluntarily consenting to entry into restricted areas, and document the interaction. Similarly, immigration authorities may seek to question an employee, client, or member of the public located within a nonpublic area of an agency facility. Personnel should receive training reinforcing the principles that, absent lawful authority to enter a nonpublic space, access is restricted to spaces open to the public and that a referral to agency counsel or other designated agency contact should be made consistent with established internal notice and elevation procedures

03 Guidance and Model Policies Regarding Immigration Enforcement Demands for Information

Purpose of this Chapter

State and local agencies collect and maintain significant information while administering programs, providing services, and carrying out regulatory and enforcement functions. The data involved often include personally identifiable information, often referred to as PII. PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII may be maintained in physical or electronic form. Increasingly, information and documents are stored electronically, which can increase the data's vulnerability, but in either event, data are increasingly a target for immigration enforcement purposes.

Information that agencies collect for one purpose—for a state license application or for a public benefits program, for example—can later be sought or otherwise become available for purposes that were not intended when the information was sought by an agency and provided by individuals who entrusted agencies with their personal and often sensitive information. Indeed, there have been recent instances in which individuals' personal data has been shared with DHS even though they were originally assured this would not happen.[61]

Access to data held by state and local agencies for immigration enforcement purposes can severely damage public trust, undermine agencies' ability to administer critical programs and carry out other essential functions, and substantially interfere with the State's ability to protect public safety, health, and welfare and carry out other sovereign functions. Given these serious harms, as well as legal constraints on data-sharing and associated liability risks, agencies should exercise great care and have strict protocols and data security measures in place when assessing whether and how to collect, retain, or produce information that could be acquired by immigration enforcement agents or used in other potentially unauthorized ways.

Governing Law

1. Fourth Amendment

The Fourth Amendment protection against unreasonable governmental searches and seizures applies to government intrusions into records, information, and data. Recent court decisions have recognized important Fourth Amendment implications when the government seeks access to modern digital information systems and datasets.[62] The Fourth Amendment also imposes limits on subpoenas and compelled disclosures of records particularly as it relates to overbroad, generalized, or unduly burdensome information access demands.[63] Modern database systems further complicate Fourth Amendment analysis because copying, extracting, or accessing large datasets may itself constitute a seizure.[64] Agencies should consider the Fourth Amendment implications when deciding whether and the extent to which information should be shared with immigration enforcement authorities.

2. Privacy and Confidentiality

The disclosure of information by state and local agencies is governed by a range of federal and state privacy laws that impose limitations on the collection, retention, and dissemination of information. There are many sources of privacy protection in the law. This publication highlights a few key examples,

but each agency will have to familiarize itself with both broadly applicable privacy laws, such as the Privacy Act of 1974, 5 U.S.C. § 552a (as amended), and more specific privacy laws that govern the agency and the data it may collect and maintain.

The California Constitution confers significant privacy protections. Article I, section 1 of the California Constitution states that all people have an "inalienable right" to "privacy."[65] The provision is self-executing and creates a legally enforceable right protecting against unwarranted governmental and private intrusion, including the compelled disclosure of personal information. "Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone."[66] Courts have recognized that this constitutional protection establishes a "zone of privacy" that limits the disclosure of private information absent sufficient justification.[67] The California constitutional right to privacy has been interpreted to impose limits on the collection,[68] retention,[69] and dissemination of personal information by state actors and to require that intrusions on privacy be justified.[70]

Other California laws impose privacy protections across a wide range of information categories, including public benefits records, employment information, and other sensitive data. These protections reflect a broader legal framework that limits the disclosure of personal information and requires agencies to safeguard information they maintain. Some examples include California laws that govern specific categories of data, like voter data,[71] juvenile data,[72] child abuse data,[73] criminal history data,[74] automated license plate reader data,[75] unemployment records,[76] public benefits data,[77] tax return data,[78] and utility customer data,[79] and carry confidentiality or strict user access requirements. Another important category of data includes California driver's license data. Both the federal Driver's Privacy Protection Act and California law limit the disclosure or use of personal information from motor vehicle records to enumerated permissible uses.[80]

Federal law also imposes privacy limitations on the sharing of information. For example, the Family Educational Rights and Privacy Act protects data and records maintained by educational institutions.[81] It states that "[n]o funds shall be made available…to any educational agency or institution which has a policy or practice of permitting the release of education records…of students without the written consent of their parents," subject to limited exceptions.[82] Similarly, California law generally restricts disclosure of pupil records.[83] For further guidance on the Family Educational Rights and Privacy Act and schools pre-K through 12 and colleges and universities please see the California Attorney General's Guidance and Model Policies to Assist California's K-12 Schools and Guidance and Model Policies to Assist California's Colleges and Universities.

Federal and state laws governing healthcare data also carry privacy protections. The Health Insurance Portability and Accountability Act and its implementing regulations provide that a covered entity "may not use or disclose protected health information, except as permitted or required" by regulations.[84] This federal statutory and regulatory scheme does not contain exceptions for informal requests by immigration enforcement authorities and generally require either individual authorization or legally sufficient process. State laws also protect medical data. California's Confidentiality of Medical Information Act generally prohibits disclosure of medical information absent authorization or a statutory exception.[85] Additionally, all information concerning an individual and obtained for provision of Medi-Cal services "shall be confidential, and shall not be open to examination other than for purposes directly connected with the administration of the Medi-Cal program."[86] For healthcare institutions looking for specific and tailored guidance, please see Guidance and Model Policies to Assist California's Healthcare Facilities.

3. Street Vendor Business Protection Act

Senate Bill Number 635 (2025-2026 Reg. Sess.), which added section 114381.3 to the Health and Safety Code and amended sections 51036, 51038, and 51039 of the Government Code and sections 114368.8 and 114381 of the Health and Safety Code, protects street vendors' personally identifiable information, including individuals' names, business names, home and businesses addresses, birthdates, telephone numbers, California driver's licenses or identification cards, and other related information, by prohibiting local authorities from collecting information on a person's immigration status or providing consent to any individual to access or review records with personally identifiable information on any sidewalk vendors unless there is a valid subpoena or judicial warrant.[87]

Types of Demands

State and local agencies may receive requests from immigration authorities seeking information regarding individuals, agency operations, public benefits records, employment records, addresses, schedules, photographs, or other agency-held information or data. These requests vary in form and in legal effect. Some requests are made informally. Other requests come in the form of, or are accompanied by, a document that may appear to grant immigration enforcement officers authority to obtain requested information, but in fact do not require a response. And some requests will require compliance or formal legal action objecting to the request. The differences can be subtle, but critically important, and thus it is important to be able to spot and understand these differences and have agency counsel involved in reviewing and assessing requests and demands for information.

1. Requests for Information Generally

Agencies should be aware that they may receive requests for information in various forms. Requests may be received by way of legal service or process, such as a judicial subpoena, search warrant, or court order, while other requests for information may present themselves in more informal ways, such as by phone or email or in-person request. Sometimes, requests or demands are made by letter, and whether the agency needs to respond and, if so, how, can depend on the circumstances.

Regardless of the form, requests for information should always be directed or forwarded to the agency's legal counsel or designated personnel for evaluation and a determination of how to proceed. As a related matter, requests for information generally should be made in writing, so the agency has a record of the request, clarity regarding its scope and the asserted legal basis for it, a means of tracking the request, and a record of how it was handled.

Upon receipt of a request for information, the designated agency personnel or legal counsel should then conduct an individualized assessment regarding whether a response is required, the manner in which to respond or challenge the request, and the timeline for handling the request. Requests for information are fact- and law-specific inquiries. While there are myriad ways in which an agency may encounter requests for information, the protocol for handling and evaluating them will not have to vary much. Designated agency personnel or legal counsel should consider the following when evaluating a request for information:

- Subject to limited exceptions such as provided by the California Public Records Act, agencies should insist that all requests for information be made in writing. Where the law permits requests to be made orally, the prudent course is for the receiving agency to produce a written version of the request it has received. This allows the agency to confirm it has correctly understood the nature and scope of the request, and it allows for better tracking of the request once it has been received and documented as received.

- All requests should be forwarded to agency counsel or other designated agency personnel.
- Requests, whether received in writing or not, and whether seemingly formal or informal, should be scrutinized and evaluated on an individual basis, with close attention paid to source, form, and scope of the request and the law invoked as a basis for the request. A document may bear the seal of an agency or include references to legal authority, for example, but still not require a response.
- Consider the form of the request, as discussed below, and determine whether there is a basis to disregard the request, a need to challenge the request, or a legal need to comply in some manner.
- Document your response to the request and notify third parties, such as a notice to consumer, if necessary or required by law.[88]

For information requests or demands that come in specific forms, such as an administrative or judicial subpoena, court order, Public Records Act request, or in connection with the administration of a federally funded program, please read the sections that follow here.

2. Administrative Subpoenas

Administrative subpoenas are issued by federal (or state) agencies pursuant to statutory authority. They may request the production of documents, appearance to provide testimony, or both. Generally, as reflected in the sample provided in **Appendix E**, administrative subpoenas have the following characteristics.

- Issued by an agency, rather than a court.
- Identify a statutory basis to issue the subpoena or request the information.
- Request the production of documents, information, or testimony.
- Include a return date or instructions for compliance.
- Signed by an agency official, and not a judge.

In the immigration context, the authority to issue administrative subpoenas is set forth in 8 U.S.C. § 1225(d)(4), a provision of the Immigration and Nationality Act.[89] A federal regulation, 8 C.F.R. § 287.4, sets forth specific requirements for administrative subpoenas issued by immigration authorities, including the form to be used, who may issue and serve the subpoena, and certain information the subpoena must include.

Importantly, administrative subpoenas issued by immigration enforcement authorities are not self-executing and thus do not require a response.[90] Under no circumstances should a state or local agency provide a response to an administrative subpoena that does not itself comply with the law or would cause the agency to violate state or federal law. If an administrative subpoena seeks bulk or blanket data, such as information on all program participants or a subset thereof, the agency should consider withholding the requested data in whole or in part as production of the data can undermine the public's trust in the state or local agency. In particular, the Ninth Circuit has held that Section 1225 does not authorize broad "John Doe" subpoenas that seek information concerning a group of unidentified persons.[91] If a recipient declines to comply, the issuing agency must seek enforcement in federal court, and a federal court in California recently issued a ruling that can be interpreted as holding that the immigration statute does not authorize enforcement of administrative subpoenas against state agencies or other sovereigns.[92] An administrative subpoena issued by ICE to a state agency can also raise serious concerns under the Tenth Amendment.

When an agency issues an administrative subpoena and the subject does not respond or declines to comply, the issuing federal agency may petition a court to order enforcement. The court will then evaluate "(1) whether Congress has granted the authority to investigate; (2) whether procedural requirements have been followed; and (3) whether the evidence is relevant and material to the investigation."[93] A "reasonableness" inquiry must also be satisfied.[94] "[T]he requirement of reasonableness … comes down to whether specification of the documents to be produced is adequate, but not excessive, for the purposes of the relevant inquiry[,]" and a subpoena should not be enforced if "the party being investigated proves the inquiry is unreasonable because it is overbroad or unduly burdensome."[95] Moreover, an administrative subpoena may not be used to for an improper motive[96] or to conduct a fishing expedition.[97]

Upon receipt of an administrative subpoena from immigration authorities, the state or local agency should:

- Refer the subpoena to agency legal counsel or other designated personnel.
- Take no action—do not comply or otherwise respond to the administrative subpoena, unless and until directed to do so by agency legal counsel or other designated personnel.
- Contact the Office of California's Attorney General, particularly if served with a petition to enforce the subpoena.
- Document all actions taken.

3. Judicial Subpoenas

Judicial subpoenas are issued under the authority of a court. They may be issued in civil or criminal proceedings and can require the sharing of documents or testimony. They do not authorize or require disclosure of information or documents beyond what is specified in the subpoena. A judicial subpoena, as seen in the sample provided in **Appendix F**, will typically include the following[98]:

- A reference to a court proceeding.
- The name of the court.
- The signature of a judge, magistrate judge, or court clerk.
- A specific date and place for compliance.

While judicial subpoenas carry legal force, they can be legally challenged. A recipient can seek to quash or modify the subpoena where appropriate. When an agency receives a judicial subpoena, the agency should:

- Immediately refer the subpoena to agency legal counsel or other designated agency contact.
- Evaluate the subpoena's scope and validity.
- Identify any potential objections to the subpoena.
- Determine whether to comply or challenge the subpoena.
- Limit disclosure to what is legally required.
- Document all actions.

4. Court Orders

Court orders are directives issued by a court that require specific actions. They may include orders to share records, provide testimony, or take other actions. To identify a court order, look for whether it:

- Is issued by a judge.
- Clearly directs the recipient to take specific action.
- May include findings or legal reasoning.
- Is associated with a specific case.

Court orders carry binding legal force and must be complied with unless modified or vacated. A court order authorizes or requires the actions specified but does not require or authorize actions beyond its terms. When an agency receives a court order, the agency should:

- Refer the order to the agency's legal counsel or other designated agency personnel.
- Comply with the order as required.
- Limit compliance to the terms of the order.
- Document all actions taken.

5. Public Records Act Requests

Requests for records under the California Public Records Act are governed by Government Code section 7920.000 et seq. The Public Records Act establishes a general rule of disclosure, providing that public records are open to inspection, subject to statutory exemptions and other legal limitations. Under the Public Records Act, a request made by an immigration authority is evaluated under the same legal framework as a request made by any member of the public. A Public Records Act request typically:

- Seeks identifiable records or categories of records.
- References the Public Records Act or requests records under California law.
- Does not include a judicial or administrative enforcement mechanism within the request itself.

The Public Records Act authorizes the requester to seek disclosure of public records. However, the Public Records Act does not require the agency to disclose records that are exempted, prohibited pursuant to federal or state law, or privileged under the Evidence Code, and it generally does not require an agency to create records.[99] When an agency receives a Public Records Act request, the agency should determine whether the requested records are subject to disclosure and whether any exemptions or other legal prohibitions apply. This includes identifying applicable exemptions or privileges, evaluating privacy interests, and determining whether disclosure would violate other legal obligations. The Act sets forth specific deadlines for responding to the request, determining whether the agency possesses the requested records, and for disclosing the records. The agency must provide only those records that are required to be disclosed and must redact information that is exempt.[100] Requests from immigration authorities must be treated in the same manner as any other request, without providing additional access based on the requester's identity.[101]

Federal Funding Conditions and Federal Program Data Requirements

Federal funding provided to state and local agencies may include conditions relating to program administration, information sharing, reporting obligations, or access to records and facilities. In some circumstances, federal agencies have attempted to condition funding on cooperation with immigration enforcement activities or on disclosure of information relating to program participants, employees,

or agency operations.[102] Federal funding conditions should be carefully evaluated because the federal government's spending power is subject to constitutional and statutory limitations.[103] Accordingly, agencies receiving federal funds should carefully review:

- Grant agreements.
- Notices of funding opportunity.
- Programmatic reporting requirements.
- Data-sharing obligations.
- Certification requirements or other representations required as a condition of application.
- Federal guidance documents.
- Conditions relating to immigration-status information or disclosure obligations.

Agencies should evaluate whether funding conditions are clearly authorized by statute, conflict with state or federal law, or exceed the federal agency's authority. Where funding conditions raise legal concerns, agencies should refer the matter for legal review and not assume that compliance is automatically required merely because a condition appears in agency guidance, grant terms, or funding documents. Agencies should also consider whether reservation of rights language is appropriate to address uncertainties or preserve rights and potential arguments for anticipated litigation.

Regulatory Data Access

Chapter 5 of this document sets forth guidance, training recommendations, and recommended audit criteria for databases, generally. However, because regulatory demands for data are a type of information demand, this section provides guidance regarding the processes agencies should have in place for handling regulatory data demands.

Not all access to agency-held information occurs through discrete requests. Public agencies frequently participate in federal or state programs involving ongoing reporting obligations, shared access to databases, or interagency systems. Regulatory data access can occur through things like:

- Mandatory reporting systems.
- Federal benefits databases.
- Interagency data-sharing agreements.
- Federally administered program systems.
- Audit or compliance reviews.
- Third-party vendor systems.
- Interoperable databases shared across agencies or jurisdictions.

These systems create significant operational and privacy concerns because information initially collected for an agency's programmatic purpose, such as healthcare administration, public benefits eligibility determinations, labor regulation, licensing, or other governmental functions, may later become accessible for immigration enforcement purposes through programmatic access or downstream information sharing, such as from one federal agency to another. As an example, after states produced data regarding Medicaid program participants as required by the federal agency that administers Medicaid, that agency—the Centers for Medicare & Medicaid Services ("CMS")—thereafter shared program participant data with ICE and then executed an agreement to give ICE direct access to Medicaid data submitted by California and other states to CMS, so that ICE can "receive information concerning the identity and location of aliens

in the United States, such as address, telephone number, banking information…email address…or other information ….”[104] In this way, ICE used the federally maintained database and the data California and other states’ agencies report into it as a vehicle to obtain personally identifiable information that it could not otherwise secure directly from California. This has been the subject of ongoing litigation.

Other federal agency actions have raised serious concerns about intentions to misuse and impermissibly share or disclose data. As an example, in May 2025 and repeatedly since then, the U.S. Department of Agriculture (“USDA”) has demanded that states transmit more than five years of data the states collected for the purpose of determining eligibility for and otherwise administering the Supplemental Nutritional Assistance Program (“SNAP”). USDA has been demanding names, Social Security numbers, home addresses, and other personally identifiable information. Several states, including California, have been challenging the legality of USDA’s demands.[105] While that litigation was still pending at the time of this guide’s publication, important lessons have already been learned.

Regulatory data access is typically grounded in federal statutes that authorize specific programs or regulations in administrative guidance implementing those programs. However, the need for careful legal evaluation is not eliminated because of existing requirements that direct compliance with certain federal agency demands for program data. A federal agency’s right to require data submission, including audits and data demands by federal inspector generals, is limited by the statute creating and governing the program and the regulations governing the administration of the program. Moreover, as discussed in Chapter 3 addressing federal funding conditions, agencies may not impose requirements that exceed or otherwise conflict with their statutory authority or that conflict with other constitutional or legal constraints.

When evaluating regulatory data demands or participation in information systems, agencies should:

- Have designated personnel and, preferably, legal counsel evaluate the regulatory demand or information systems request.
- Conduct a legal review of the request including the legal basis for single-instance or ongoing reporting obligations.
- Evaluate whether the data request or submission is required, permitted, limited, or prohibited by statute, regulation, agreement, or other binding document.
- Assess whether the data may be deidentified by the removal or obscuring of personal identifiers or produced in a more limited manner than has been requested.
- Assess whether compliance would result in disclosure for immigration enforcement purposes or violate state or federal law.
- Consult any applicable System of Records Notice (SORN) and Privacy Impact Statement.
- Determine if a data and security protocol is required and in place.
- Ensure that any transfer of data is handled in a secure manner, consistent with all applicable requirements.
- Document the request and response.

Agencies should not assume that all requested data must be provided in full. Where discretion exists, agencies should exercise that discretion in a manner consistent with all applicable laws, including privacy laws, and the Legislature’s objective of governing databases in a manner that limits the availability of information to the fullest extent practicable, consistent with federal and state law.[106] Where questions arise regarding the legality or scope of a data access requirement, the matter should be referred to legal counsel. In appropriate circumstances, agencies may seek clarification from the federal agency or negotiate the scope of the data submission.

Model Policies

Agency policies should establish clear procedures governing review of requests, escalation requirements, authorization procedures, and documentation requirements. Agency policies governing information access or demands should ensure that requests for data are not handled informally or through ad hoc operational practices and require requests for information to be reviewed through designated agency personnel before disclosure occurs.

General Response Protocols

Agency protocols should apply across agency operations and should be designed to ensure consistent, legally compliant responses regardless of the form or asserted urgency of the request. When responding to requests for information, the model policies call for personnel to:

- Try to remain calm and professional.
- Ask for the officer's name, identification number, and agency affiliation.
- Avoid making immediate disclosure decisions without review.
- Require the agent to support their request with documentation. The request and documentation can be submitted through a designated portal, email or mailing address, or other means for service or other request submission.
- Request copies of documents, warrants, subpoenas, or written requests where applicable.
- Immediately refer requests to designated personnel or legal counsel.
- Inform the officer that the request is with the agency's designated person, a supervisor, or legal counsel for assistance.
- Document all communications and actions taken.

Personnel should understand that they are generally not expected to independently determine the legal sufficiency of subpoenas, warrants, or requests for information. Rather, personnel should be trained to route requests to designated agency personnel. The model policies call for procedures to maintain records regarding:

- The date and time of the request.
- The identity of the requesting agency or officer.
- The legal authority asserted.
- The categories of information sought.
- The information disclosed, if any.
- The method of disclosure.
- Any limitations and objections asserted as a basis to withhold information.

Designated Personnel or Legal Counsel

- The agency shall designate personnel responsible for evaluating and responding to requests for information by immigration authorities. Agency written policy regarding the designed personnel shall include, at minimum:
- Contact information [name, title, e-mail addresses, and phone numbers] for the correct person to review and respond to a request for agency records, data, or information.
- Access to sample warrant and subpoena documents that could be used for access to records, data, or information (see sample **Appendices B to F**).
- Designated personnel shall be trained on the legal standards governing information sharing with or access by immigration authorities. This includes training on the legal effect of administrative versus judicial processes, and the limits imposed under state and federal law.
- Designated personnel shall evaluate whether any document presented constitutes a legally sufficient process, determine whether compliance is required, and coordinate the agency's response. Centralizing these determinations ensures that agency actions are consistent with the law and prevents frontline personnel from making legal judgments outside their role.

Collecting and Retaining Information

- The [title of appropriate official or name of unit] shall maintain in writing agency policies and procedures for the gathering, handling, and retention of sensitive client information, and appropriate personnel shall receive training regarding those policies and procedures.
- Any sensitive information, such as a person's personally identifying information or immigration or citizenship status information collected by the [agency] or disclosed by the client, should be maintained only for as long as necessary or required by law.
- Unless required by federal or state law or a state or federal program unrelated to immigration enforcement (such as a federal benefits program), [Your Agency] shall not inquire specifically about a member of the public's citizenship or immigration status or the citizenship or immigration status of any other person in the individual's household; nor shall personnel seek or require, to the exclusion of other permissible documentation or information, documentation or information that may indicate an individual's immigration status, such as a green card, voter registration, a passport, consular identification card, or citizenship papers unless required by a federal or state law or program.

[Your Agency] and personnel shall only collect personally identifiable information on individuals as required to support [Your Agency]'s programmatic work or as required by law.[107] Personal information may include, but is not limited to, name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.[108] Where the records requested are protected by law, such as state or federal privacy, student records, or health laws, [Your Agency] shall only disclose those records in accordance with relevant laws. This limitation also applies to the retention of data elements such that only the information that is legally or programmatically required is collected and retained.

[Your Agency] has [developed or adopted] data and record retention schedules based on legal requirements and privacy best practices or as promulgated by [insert reference to retention schedule

Your Agency has either adopted or follows]. These retention schedules may be found at [insert reference or link to data/record retention schedule adopted or followed by Your Agency.]

In accordance with data and record retention schedules, [Your Agency] has developed or adopted secure deletion methods for data no longer required to fulfill [Your Agency]'s mission or programmatic requirements.

Responses to Information Requests

Agency policies shall establish procedures governing responses based on the type of demand presented.

Where a request is not accompanied by a judicial subpoena or court order.

- Where a request for information is made, or where the request is accompanied by an administrative subpoena, agency personnel shall inform the requesting party that agency policy requires review by designated personnel.
- Agency staff shall refer the request to designated personnel or legal counsel and document the interaction (more details on this provided in Chapter 4). Agencies have no obligation to respond to the informal request for information or a request that is accompanied by an administrative subpoena or some other administrative document.

Where a request is accompanied by a judicial subpoena or court order.

- Where a request for information is accompanied by a judicial subpoena or court order, agency personnel shall inform the requesting party that agency policy requires review by designated personnel and refer the request to designated personnel or legal counsel.
- Agency staff shall refer the request to designated personnel or legal counsel and document the interaction. Designated personnel or legal counsel shall verify that the document is valid and properly issued, determine the scope of required disclosure, and, in cases involving judicial subpoenas, determine whether there is a basis to move to quash or challenge the subpoena. Where a decision to disclose is made, disclose only the information specifically required and take reasonable steps to protect confidential or sensitive information.

Where a request is made under the Public Records Act.

- Where a request for information is made pursuant to the Public Records Act, agency personnel shall refer the request to designated personnel or legal counsel. Designated personnel or legal counsel shall evaluate whether requested records are subject to disclosure, apply all applicable exemptions, including those protecting personal privacy and confidential information, and not disclose information beyond what is required by law.

Where a request is made as part of a federal program.

- Where a request is made for data arising from participation in federal or state programs, the request shall be evaluated based on the governing statutory and regulatory framework and agency personnel shall refer the request to designated personnel or legal counsel. Designated personnel or legal counsel shall determine whether disclosure is required by law or as a lawful condition of program participation. When information is disclosed, agency shall limit disclosure to the minimum information required and ensure compliance with applicable privacy laws and data security protocols

Dissemination of Information to Contractors

[Your Agency] has established role-based access controls to database systems and physical files that restrict who may access sensitive or personally identifiable information. This includes continued restrictions for files housed off-site or with private vendors.

[Agency must append this policy to any contracts, MOUs, or agreements to ensure that vendors and contractors abide by the same policy and limitations.]

Documentation Requirements

Agencies shall require comprehensive documentation of all requests for information from immigration authorities.

Documentation shall include:

- ✓ The date, time, and type of information requested.
- ✓ The identity, contact information, and agency affiliation of officers.
- ✓ The nature or detail of the officer's request.
- ✓ Whether the officer presented a warrant, subpoena, or court order to accompany their request, what was requested in the warrant/subpoena/court order, and whether the warrant/subpoena/court order was signed by a judge.
- ✓ The agency's response to the request.
- ✓ Any further action taken by the immigration officer.
- ✓ Photo or copy of any documents presented by the agent.
- ✓ Documentation should be maintained in a centralized location.

Note: To protect bulk data once it leaves agency's control and possession or access to your agency's database, agencies, as a matter of best practice, should develop procedures and requirements for entering into a written Data Use Agreement prior to the discretionary delivery of sensitive or confidential data. Data Use Agreements should include:

1. A detailed description of the purposes for which the data is being used.
2. The specific confidentiality and information security controls that the requestor must follow (for example, who is allowed to access the data, technological security standards, and how to destroy or return the data after they are no longer needed for the business purpose for which they were obtained),
3. How to handle a privacy breach.

Training Regarding Information Sharing

Agencies are encouraged to train agency personnel on the agency's policies and procedures. Recommendations for training are provided in this section.

Training should aid personnel in identifying and correctly responding to interactions with immigration authorities, understanding the application of the legal frameworks described in this guidance as well as the consequences of information disclosure, and understanding how to minimize disclosures of information consistent with the law and programmatic needs.

Personnel should be trained to identify and distinguish between:

- Administrative immigration warrants.
- Judicial warrants.
- Administrative subpoenas.
- Judicial and grand jury subpoenas.
- Notices to Appear.
- Public Records Act requests

Training should include instruction on the characteristics of each document, the legal effect of each document, and the required agency response. The training should also focus on how and when frontline personnel are expected to forward a request from immigration authorities to the agency's designated personnel or legal counsel and how designated personnel should be able to recognize, in real time, whether a document carries binding legal authority and may require compliance. (A reference guide for immigration enforcement documents is provided at **Appendix G**.)

Agency personnel should also receive training regarding the legal frameworks discussed in this guidance, including the meaning of 8 U.S.C. §§ 1373 and 1644,[109] the California Public Records Act, and federal and state laws that impose privacy, privileges, and access control restrictions on the sharing of data. However, since 8 U.S.C. §§ 1373 and 1644 remain the subject of ongoing constitutional debate, agencies should consult with legal counsel before adopting any policy that could affect communications governed by those statutes.

As discussed earlier, interactions with immigration authorities may occur without advance notice, in real time, and under circumstances that could create a felt pressure to respond immediately. When that occurs the absence of clear training can result in the disclosure of information that is not required or permitted by law, the granting of access that is prohibited by statute, or inconsistent responses across personnel or departments. Training should therefore be designed to eliminate uncertainty and ensure that personnel, especially designated personnel, understand not only what the law provides, but how it also applies in specific contexts. To reinforce the training and principles in this guidance, it is recommended that training be conducted upon your agency's implementation of policies consistent with SB 580 and at regular intervals, including at any point where there are changes in laws, relevant agency policy, or your agency's data technology

Training should also incorporate scenario-based guidance to assist personnel with consistently applying legal and operational policies governing requests for information. Below is an example illustrating scenario-based training.

Example: An immigration enforcement officer verbally asks frontline staff for the contact information and whereabouts of an agency client.

Model response:

- ✓ Frontline staff requests officer's identification and written documentation.
- ✓ Regardless of whether officer provides written documentation or not, frontline staff ask the agent to wait in a public area while the request is considered by their supervisor, designated staff, or legal counsel.
- ✓ Frontline staff provides all information available to them, including the officer's identification and documentation, if provided, to their supervisor, designated staff, or legal counsel.
- ✓ Designated staff or legal counsel evaluates the request and, where there is no judicial subpoena or court order, agency declines to provide information.
- ✓ Staff document the request and notify leadership/counsel immediately.

04 Guidance, Audit Criteria, and Training Recommendations for Databases

Government Code section 12532.5(b) directs the Attorney General to publish guidance, audit criteria, and training recommendations for databases maintained by state and local agencies including databases maintained by private vendors. These recommendations aim to ensure that agencies manage or engage with databases in a manner that makes the availability of information therein to anyone or any entity for purposes of immigration enforcement limited to the "fullest extent practicable, consistent with federal and state law."[110] Accordingly, this Chapter provides guidance and training recommendations regarding databases, commensurate with SB 580's requirements.

Database Guidance

The following provides the Attorney General's guidance on best practices regarding database governance and protections that agencies should consider. When considering this guidance, agencies should evaluate the extent to which laws that specifically apply to their operations or programmatic requirements may also dictate agency policy or practice.

1. Minimize Data

Data minimization is the principle that an agency should only collect information that is necessary for the function of the agency or that which is legally required for agency operations or determinations.[111] The collection of data unnecessary to the function or legal requirements of an agency may create vulnerabilities for that data, including that it may subsequently be accessed for unintended purposes such as immigration enforcement.

While many agencies will need to collect some level of personally identifiable information to make determinations for program eligibility or register individuals for government services or programs, the current best practice is to ensure data collection is limited to the needs and purpose of the agency.[112] The decision whether to collect information is the first and most consequential point of control. Information that is not collected cannot be disclosed. Accordingly, agencies must evaluate each data field to determine whether it is necessary to achieve a legitimate operational objective.

Except where federal or state law expressly requires collection, retention, reporting, or disclosure, agencies should also minimize the collection of immigration proxy data. Proxy data, which refers to the usage of multiple pieces of information as stand ins for direct information, can create hidden vulnerabilities.[113] For example, published studies have often used a combination of year of arrival, occupation, and public benefits receipt to estimate the proportion of the population without current legal status.[114] Data elements such as place of birth, documentation categories, language indicators, household composition, or identification numbers may, individually or in combination, allow inferences regarding immigration status. Agencies should therefore assess whether such data fields are necessary and whether the same objectives can be achieved through less sensitive or less revealing information. Where proxy risks are identified, agencies should eliminate or minimize those fields unless their collection is required.

Lastly, agencies should limit the period for which information is retained in accordance with the legal or pragmatic requirements. Agencies should establish retention schedules that:

- Limit the duration of retention to what is strictly necessary for program administration.
- Require the routine deletion or anonymization of data once it is no longer needed.
- Prevent the accumulation of legacy datasets that serve no ongoing operational purpose.

Retention policies should be evaluated not solely as administrative tools, but as mechanisms for reducing exposure. Data that remains stored continues to pose a risk regardless of whether it is actively used.

2. Adopt Access Controls

Agencies should implement access controls to ensure that information is available only to personnel who require it for legitimate purposes. Access controls should include role-based permissions, authentication mechanisms, and monitoring systems that track and record access to sensitive information.

These controls should apply to all agency employees, contractors, interns, and volunteers. Controls should extend to all third-party vendors, information systems, networks, and physical facilities where the data may be stored. The core principles in guiding access limitations restrictions should be as follows:

1. Least privilege – Users only receive the minimum access required to perform their duties. This includes all front end, reception, and "customer-service" facing roles.
2. Need-to-Know – Users' access to sensitive information is restricted to those who have a legitimate functional need for the data as part of performing their duties.
3. Separation of Duties – Users with greater access to the data will have critical tasks divided among multiple users to reduce risk of misuse.
4. Accountability – All users will have a unique attributable ID to catalog their access and search history.

For each user, access should only be granted after the verification of the user's role and identity. Any access granted should be conditional on the completion of data handling and privacy training and supervisor approval.

3. Special Considerations for High-Risk Database Systems

Certain database systems present elevated risks due to the volume or sensitivity of the information they contain. Agencies should consider the nature of the data or data system when developing security measures and policies regarding the governance or access of agency data. The high-risk systems include:

Federal Program Data (e.g., Benefits Systems)

Programs involving federal funding or reporting requirements may require data submission to federal systems. The sharing of program data with one federal agency increases the risk that data collected for one purpose will be accessible for another. Agencies should evaluate whether such submissions include personally identifiable information and whether that information may be accessed by enforcement entities or whether the sharing of such data is truly legally or programmatically necessary.

Third-party Vendors

Vendor-managed systems may aggregate data across jurisdictions or provide administrative access that exceeds agency control. For state vendor contracts, agencies should consider including provisions that require the vendor to acknowledge that the agency provides access to its confidential or proprietary data for the sole purpose of performing its contractual duties, and that redisclosure to any third party, unless expressly required by law, is strictly prohibited without the prior written consent of the agency. Agencies should also ensure that vendor arrangements do not expand the availability of data beyond what is permissible under state and federal law. For instance, under California Civil Code § 1798.17, contractors are required to maintain equivalent database security and protection for consumers as the state agency with which they work.

For vendors to secure access to agency data, agencies should require the following from vendors:

1. Confirm the identity of vendors and determine their intended usage of the data.
2. Confirm the data usage will not come into conflict with state or federal law or undermine the programmatic purpose for the data.

Contracts with private vendors should include terms that clearly:

1. Prohibit unauthorized access to or disclosure of data.
2. Require agency consent for disclosure.
3. Require prompt notice to the agency if agency data becomes the subject of a subpoena or other legal process or demand.
4. Require vendor to acknowledge that the agency is providing access to its confidential or proprietary data for the sole purpose of performing its contractual duties and that redisclosure to any third party, unless expressly required by law, is strictly prohibited without the prior written consent of the agency.

Bulk or Blanket Data Requests

Requests for bulk or blanket data or system access present heightened risks due to their scale and potential impact. Agencies should treat such requests as requiring elevated scrutiny, including:

- Legal review prior to any response.
- Evaluation of whether the request exceeds statutory authority.
- Consideration of whether deidentified, partial, or aggregated responses may satisfy legal requirements while reducing risk.

Interagency or Interoperable Databases

Agencies that manage, operate, or input data into databases shared with other agencies, including federal agencies, should consider using data sharing agreements or memoranda of understanding that limit the use and distribution of agency data shared or accessed through the interagency database. These agreements or memoranda of understanding should prohibit the sharing of agency information for immigration enforcement purposes absent legal authority. Internal monitoring mechanisms and auditing capabilities should also be established to ensure compliance. Interagency workgroups are also encouraged to only collect information necessary for the purpose of the workgroup. For example, a county education work group to reduce health disparities for students should focus on health services and not collect or share information about immigration status.

Integration or Usage of Artificial Intelligence

Agencies that utilize any Large-Language-Models, Machine-Learning, or Generative Artificial Intelligence (AI) should already have policies governing their usage and platform integration. Additional considerations for the security of PII that is stored within the same network using any variation of AI model, should be assessed by those who fall within the Need-to-Know category of staff. Consistent data cleaning and database maintenance will reduce the likelihood of leakage of PII to AI platforms. However, as usage and proliferation of AI technology to enhance workplace productivity continues, security networks and staff training will need to evolve to meet these risks.

To reduce the risks associated with the usage of AI, agencies should adopt practices that clearly:

- Set a schedule to, at a minimum, bi-annually review AI usage policy among staff.
- Review audit results for outlier usage of AI queries that are integrated into facility search engines.
- Review and update internal data governance policies as needed to ensure information security.

Training Recommendations Regarding Databases

The following are training recommendations agencies should consider regarding the governance and operation of databases.

1. Implement Scenario Based Training

As discussed above, scenario-based training is a teaching approach where learners engage in simulated or reality-based training. In applying this principle, agencies should center training around the types of databases that they manage, own, or into which they enter client information. Below is an example:

Example: Bulk Data Request

Scenario: Immigration enforcement requests a list of all program participants in a non-federal public benefits program, including addresses and contact information via an administrative subpoena.

Model response:

- ✓ Ignore the subpoena. Administrative subpoenas are not self-executing, and binding Ninth Circuit case law prohibits use of an administrative subpoena to conduct a fishing expedition like the one seen in this example. No response is required, and depending on the circumstances, other laws may prohibit the disclosure. A bulk data request for immigration enforcement should be treated as extraordinary and presumptively overbroad and unlawful, and the issue should be raised to counsel. Should the federal agency that issued the subpoena file a petition to enforce the administrative subpoena, state or local agency counsel should apprise themselves of relevant legal authority, including *Peterson v. United States* (9th Cir. 1988) 853 F.2d 692, 695, as well as the Privacy Act and sector specific confidentiality, including but not limited to Welfare & Institutions Code § 10850, and strongly consider contacting the California Attorney General's Office.

2. Center Training on the Relevant Legal Frameworks Governing Information Sharing with Immigration Enforcement

Personnel should be trained on the laws discussed in this guidance, including:

- The meaning of 8 U.S.C. sections 1373 and 1644.[115]
- The requirements of California Government Code sections 7284.6 (where applicable) and 7285.1 and 7285.2.
- The applications of privacy protections, including laws that apply to the agency or those it serves (for example, Health Insurance Portability and Accountability Act, and Family Educational Rights and Privacy Act).
- The requirements of the Public Records Act.

This instruction should include the text of these provisions and their meaning as it pertains to your agency's operations. Personnel should understand that a request from law enforcement or a federal officer does not, by itself, create a legal obligation, that the presentation of a federal document does not necessarily require compliance, and that State law may prohibit actions that would otherwise seem permissible. Training should reinforce the following principles:

- A review of the agency's internal notice and elevation procedures.
- The requirement to limit collection to necessary information.
- The agency's access control policy and protocols.
- The risks associated with retaining unnecessary data.
- The potential for information to be used beyond its original purpose.
- The obligation to evaluate requests for information under applicable law.

Training should emphasize that information disclosure is not a neutral act. It can constitute participation in immigration enforcement when it enables identification, location, or tracking of individuals, and it can be illegal.

Recommendations Regarding Database Audit Criteria

State and local agencies should establish auditing procedures designed to ensure that agency databases, records systems, and information-sharing practices or systems are governed in a manner that limits the availability of information for immigration enforcement purposes to the fullest extent practicable, consistent with state and federal law. Systems should be updated to support needed automation and recordation of required data and activity. This might include adding the capability to generate notification of potential violations or breaches to support auditing. Audit processes developed by the agency or other third party should be structured to evaluate whether agency personnel, contractors, vendors, and interoperable agency databases comply with agency policies governing data collection, retention, access, disclosure, and documentation practices. Audits should be conducted on a recurring basis and should include review of both agency-operated systems and databases maintained on behalf of the agency by third-party vendors or contractors. Audit findings should be documented in writing and should identify any deficiencies, unauthorized access, policy violations, over-collection of information, remedial or corrective actions taken, or gaps in training or technical safeguards.

1. Audits Should Examine Data Collection Practices

Audits should evaluate whether agency personnel and systems are collecting only information necessary for the administration of agency programs, services, or legal obligations. Agencies should assess whether databases contain information relating to immigration status, citizenship, nationality, place of birth, language, family composition, aliases, prior addresses, or other information that could be used directly or indirectly for immigration enforcement purposes. Audits should specifically assess:

- Whether collection of each category of information is legally required or operationally necessary.
- Whether agency forms, intake systems, and electronic databases request information that exceeds programmatic necessity.
- Whether data fields or information collected function as proxies for immigration status or nationality.
- Whether information that is no longer required is retained beyond authorized retention periods.
- Whether agency personnel have been trained regarding data minimization principles and restrictions on unnecessary information collection.

When audits identify information collection practices that exceed legal or operational necessity, agencies should revise forms, databases, intake procedures, and training protocols to reduce unnecessary collection and retention of personally identifiable information.

2. Agencies Should Require Access Logs

Agencies should maintain systems capable of creating detailed access logs for databases containing personally identifiable information or sensitive records. Audit procedures should evaluate whether access logging systems are complete, including whether the access log identifies the user accessing records, the records accessed, the date and time of access, and the actions performed. In addition, audits should examine whether access logs are regularly reviewed for unusual, excessive, or unauthorized access activity, whether database user credentials are shared, and whether database queries involve large-scale exports, bulk searches, or repeated searches involving sensitive populations. Agencies should establish escalation procedures for reviewing suspicious activities in a database and should ensure that personnel responsible for reviewing access logs receive appropriate training regarding privacy, and data security obligations.

3. Incident Documentation

Agencies should maintain written procedures requiring documentation and review of incidents involving suspected unauthorized access, disclosure, sharing, misuse, or attempted acquisition of agency information for immigration enforcement purposes or for reasons unrelated to the data's programmatic purposes. Audits should assess whether agencies consistently document and review requests from immigration enforcement authorities for records, database access, or information; improper database searches or queries; and complaints or reports concerning information-sharing practices with immigration enforcement.

4. Implement Monitoring, Reporting, and Corrective Actions

Agencies should establish ongoing monitoring, reporting, and corrective action procedures designed to ensure compliance with laws and agency policies governing interactions with immigration enforcement authorities including unauthorized disclosures of protected personally identifiable information. Agencies should ensure that personnel understand their reporting obligations and the processes available for reporting suspected violations of agency policy, confidentiality requirements, or data governance protocols. To meet these goals, agencies should establish a process for the reporting of complaints regarding:

- Unauthorized disclosures of information or access to databases or records.
- Unlawful or otherwise improper requests for records or database access.
- Violations of agency privacy or confidentiality policies.
- Improper cooperation with immigration enforcement authorities.
- Misuse of agency systems or credentials.
- Failures to follow escalation or documentation procedures.
- Suspected retaliation against personnel reporting policy concerns.

Agencies should designate responsible personnel or units to receive, review, and investigate complaints or reports of violations of agency policy. Agencies should maintain written documentation of complaints, investigative findings, corrective measures taken, or any resulting policy changes. Where audits or investigations reveal deficiencies or violations of agency policies, agencies should take the necessary steps to implement corrective actions.

05 Additional Information for Agencies and Their Stakeholders

State and local agencies should be aware of the valuable role that community stakeholders play in the administration of state and local governance. In recognition of this contribution, state and local agencies should strive to enhance, promote, and strengthen partnerships within the community and work to engage constructively with the community to ensure collaborative problem-solving and to increase transparency.

State and local agencies should also strive to broaden current efforts to actively participate in community engagement efforts, including participating in local community meetings, making themselves available for community feedback, and working with the community directly by, for example, creating easy points of access for community feedback and input, providing "community feedback" links on websites and social media pages, and ensuring that in addition to posting policies on webpages, that policies are accessible to the public and available in multiple languages in accordance with state law and the Dymally-Alatorre Bilingual Services Act.

If state or local agencies wish to provide clients or members of the public with additional information about resources, below is information agencies are free to consider sharing.

1. ICE Detainee Locator

The ICE online detainee locator can help people determine if someone has been detained and where the individual is being held. In using the ICE detainee locator, it is helpful to know the individual's date of birth and 'A-Number' (Alien Registration Number), if there is one. An individual who entered the United States without inspection may not have an A-number.

Note: The ICE online detainee locator is intended only for locating individuals who are already detained. The website is not updated regularly; if an individual known to be detained does not appear on the website, it should not be interpreted as confirmation that they are no longer detained or have been deported. If a client has general questions about their immigration status, the client should be referred to a list of legal service providers such as those linked in the Legal Assistance section below.

2. Rapid Response Networks

In response to immigration enforcement actions, some immigrant rights and legal advocacy organizations have developed Rapid Response Networks; California Collaborative for Immigrant Justice. These provide hotlines where individuals can call if they see or are impacted by immigration enforcement actions; often mobilize trained responders to verify reports of enforcement activity; and connect individuals to legal assistance, "Know Your Rights" information, and follow-up services. In some cases, they also coordinate rapid attorney activation when someone is detained.

Some examples of Rapid Response Networks include, but are not limited to: Stand Together Contra Costa; San Francisco Rapid Response Network; Sacramento Rapid Response Network; Kern County Rapid Response Network; Multicultural Center of Marin | Marin Rapid Response Network; 805 Immigrant Rapid Response Network in Santa Barbara, Ventura, and San Luis Obispo Counties; and Immigrant Defenders Law Center Rapid Response Network in Los Angeles, San Bernardino, Orange, Riverside, San Diego and Imperial Counties. Valley Watch Network. California Regional Network Hubs for Immigrant Families | Immigrant Legal Resource Center.

Note: Rapid Response Networks are not government agencies—they are community defense systems that help people understand their rights and access legal resources when immigration enforcement actions are taking place locally.

3. Legal Assistance

Immigration lawyers in private practice, United States Department of Justice (USDOJ)-accredited representatives (who assist immigrants in immigration proceedings), or legal-aid organizations may be able to provide legal assistance to secure the release of, or arrange for visits to, a client or client's family member.[116]

- ✓ An individual can determine if lawyers are licensed by and in good standing with the State Bar of California by checking online.
- ✓ Individuals may be able to find legal assistance from legal aid offices and lawyer referral services at the California Department of Social Services website, or at the California Courts website. California courts also operate Self-Help Centers that may also be able to provide legal assistance to individuals. A list of these centers across the state is also available.
- ✓ The Immigration Advocates Network maintains a national immigration legal services directory. The directory allows users to search for free or low-cost immigration legal services providers by state, county, or detention facility. Users can refine their search by areas and types of legal assistance provided, populations served, and languages spoken.
- ✓ The Executive Office for Immigration Review (EOIR), Office of Policy, Public Resources Program (PRP) administers a List of Pro Bono Legal Service Providers. The list is provided to individuals in immigration proceedings and contains information on non-profit organizations and attorneys who have committed to providing at least 50 hours per year of pro bono legal services before the immigration court location where they appear on the list. The list also contains information on pro bono referral services that refer individuals in immigration court proceedings to pro bono counsel.
- ✓ The USDOJ'S Recognition and Accreditation (R&A) Program allows certain individuals, specifically non-attorney employees and volunteers of qualifying non-profit organizations, to represent individual in immigration proceedings before the federal government. To find an "Accredited Representative" to help you with your immigration case, you can contact a nonprofit organization that is a "Recognized Organization" under the Recognition and Accreditation Program.

Note: The fact that an attorney is licensed, accredited, or in good standing with a State Bar does not guarantee competence, diligence, or honesty; individuals should independently verify qualifications and exercise caution to reduce the risk of inadequate representation or fraud. Moreover, individuals should not hire an immigration consultant (often referred to as "notarios" in the Spanish language) if they are seeking advice and assistance regarding their immigration status. Immigration consultants are not attorneys or immigration experts. In fact, they are not legally required to know anything about immigration law because they are only allowed to help with non-legal tasks like translating information. Immigration consultants cannot —and should not—provide advice or direction about an individual's eligibility for different types of immigration relief, which immigration forms to submit, or speak to the government on a client's behalf. In addition, immigration consultants must be bonded and pass background checks with the Secretary of State. To learn whether a specific immigration consultant has complied with these requirements, consult the Secretary of State website.

4. Immigration Court Website and Hotline

If an individual wants to know the status of their immigration case they can consult the Executive Office for Immigration Review (EOIR) Automated Case Information System website and/or call the Immigration Court Hotline at 1-800-898-7180. It is useful to check both the website and hotline since they have different categories of information. The Asylum Seeker Advocacy Project (ASAP) also provides links and resources to navigating the immigration court system.

The EOIR will frequently change the time, date, and potentially even the location of immigration hearings. If EOIR changes this information, it will email a new notice of hearing, but individuals can also always check with the Immigration Court Hotline. Individuals must show up for all of their immigration hearings. If they do not, they may be ordered removed in their absence.

5. Consulate or Embassy

The consulate or embassy of an individual's country of origin may be able to offer additional information and assistance.

Endnotes

[1] Gov. Code, § 12532.5 subdiv. (a)(1).

[2] Gov. Code, § 12532.5 subdiv. (b)(1).

[3] Sen. Bill No. 580 (2025-2026 Reg. Sess.) § 2.

[4] See, e.g., *Arizona v. United States* (2012) 567 U.S. 387, 394–395.

[5] See Benjamine C. Huffman, Acting Secretary, U.S. Dept. of Homeland Security, Memorandum, DOJ Immigration Officer Authorization (Jan. 22, 2025).

[6] Gov. Code, § 7284.6, subd. (a)(1)(G); see also Cal. Dept. of Justice, Information Bulletin No. 2025-DLE-03 (Jan. 17, 2025) *supra*.

[7] See, e.g., Alejandro N. Mayorkas, Secretary, U.S. Dept. of Homeland Security, Memorandum, *Guidelines for Enforcement Actions in or Near Protected Areas* (Oct. 27, 2021), Guidelines for Enforcement Actions in or Near Protected Areas; John Morton, Director, U.S. Immigration and Customs Enforcement, *Memorandum, Enforcement Actions at or Focused on Sensitive Locations* (Oct. 24, 2011) (Policy No. 10029.2).

[8] *Ibid.*

[9] Benjamine C. Huffman, Acting Secretary, U.S. Dept. of Homeland Security, *Memorandum, Enforcement Actions in or Near Protected Areas* (Jan. 20, 2025); Caleb Vitello, Acting Director, U.S. Immigration and Customs Enforcement, *Memorandum, Common Sense Enforcement Actions in or Near Protected Areas* (Jan. 31, 2025).

[10] Caleb Vitello, Acting Director, U.S. Immigration and Customs Enforcement, *Interim Guidance: Civil Immigration Enforcement Actions in or Near Courthouses* (Policy No. 11072.3); Todd M. Lyons, Acting Director, U.S. Immigration and Customs Enforcement, *Memorandum, Civil Immigration Enforcement Actions in or Near Courthouses* (May 27, 2025) (Policy No. 11072.4).

[11] Civ. Code, § 43.54.

[12] Some of these federal law restrictions are discussed in this publication. Others are discussed, or are discussed more fully, in the guidance publications listed in the Introduction and Executive Summary.

[13] Another federal statute, 8 U.S.C. § 1644, is almost identically worded.

[14] 8 U.S.C. § 1373(b).

[15] See, e.g., *City of Chicago v. Sessions* (N.D. Ill. 2018) 321 F.Supp.3d 855, 872 (finding that 8 U.S.C. § 1373 violates the Tenth Amendment), *aff'd and remanded sub nom. City of Chicago v. Barr* (7th Cir. 2020) 961 F.3d 882 (affirming without reaching constitutionality of § 1373); *Cnty. of Ocean v. Grewal* (D. N.J. 2020) 475 F.Supp.3d 355, 374–375 (accumulating district court cases considering the scope of 8 U.S.C. § 1373 in the context of the Edward Byrne Memorial Justice Assistance Grant and the states' challenges to § 1373's constitutionality under the 10th Amendment), *aff'd sub nom. Ocean Cnty. Bd. of Comrs. v. Atty. Gen. of State of N.J.* (3d Cir. 2021) 8 F.4th 176 (affirming without reaching constitutionality of 8 U.S.C. § 1373); see also *United States v. Illinois* (N.D. Ill. 2025) 796 F.Supp.3d 494, 523 (explicitly declining to "decide whether § 1373 is constitutional," but noting several major "state sovereignty concerns that would arise if § 1373 overtook state and local law.") A federal trial court in California has called Section 1373 "highly suspect," but the United States Court of Appeals for the Ninth Circuit, headquartered in California, has not squarely addressed its constitutionality. (*United States v. California* (E.D. Cal. 2018) 314 F.Supp.3d 1077, 1101, *aff'd in part, rev'd in part and remanded* (9th Cir. 2019) 921 F.3d 865.)

[16] See, e.g., *United States v. California* (9th Cir. 2019) 921 F.3d 865, 891; *City & Cnty. of S.F. v. Garland* (9th Cir. 2022) 42 F.4th 1078, 1085 ("We have rejected DOJ's interpretation of Section 1373 repeatedly …. Section 1373 only covers immigration-status information—*i.e.*, 'what one's immigration status is.'") (quoting *United States v. California*, 921 F.3d at 891).

[17] Courts have found that 8 U.S.C. § 1373 and § 1644 are similarly worded and narrow in scope. See *City & Cnty. of S.F. v. Garland* (9th Cir. 2022) 42 F.4th 1078, 1082–1083, 1085–1086; *Steinle v. City & Cnty. of S.F.* (9th Cir. 2019) 919 F.3d 1154, 1164 ("[The statutory text] includes only 'information regarding' 'immigration status,' and nothing in §§ 1373(a) or 1644 addresses information concerning an inmate's *release date*.") (emphasis in original).

[18] See, e.g., *United States v. California* (2019 9th Cir.) 921 F.3d 865.

[19] See, e.g., *Prinz v. United States* (1997) 521 U.S. 898; *New York v. United States* (1992) 505 U.S. 144.

[20] See, e.g., *United States v. California* (2019 9th Cir.) 921 F.3d 865, 889.

[21] Gov. Code, §§ 7282.5, 7284.6.

[22] Gov. Code, §§ 7283, 7283.1, 7283.2

[23] Cal. Dept. of Justice, Information Bulletin No. 2025-DLE-03, (Jan. 17, 2025), *supra*.

[24] Gov. Code, § 7283.1.

[25] *Ibid.*

[26] *Ibid.*

[27] *Ibid.*

[28] *Ibid.*

[29] *Ibid.*

[30] Gov. Code, § 7284.6, subd. (a)(1).

[31] Gov. Code, § 7284.6, subd. (a)(1)(C).

[32] Gov. Code §§ 7282.5, subd. (a)(3); 7284.6, subd. (a)(1)

[33] Gov. Code, § 7284.6, subd. (a)(1)(D).

[34] Gov. Code, § 7284.6 subds. (a)(1)(G), (a)(2).

[35] Gov. Code, § 7284.2, subd. (a).

[36] Gov. Code, § 7284.2, subd. (b).

[37] Gov. Code, § 7284.2, subd. (c).

[38] Gov. Code, § 7284.2, subd. (d).

[39] Gov. Code, § 7284.2, subd. (g).

[40] See, e.g., Cal. Dept. of Justice, Div. of Law Enforcement, Information Bulletin No. 2025-DLE-03, *Updated Responsibilities of Law Enforcement Agencies Under the California Values Act, California TRUST Act, and the California TRUTH Act* (Jan. 17, 2025) [as of June 4, 2026].

[41] U.S. Const., 4th Amend.

[42] The United States Supreme Court has repeatedly recognized that entry into nonpublic commercial or operational areas ordinarily requires lawful authority. In *See v. City of Seattle* (1967) 387 U.S. 541, 545 the Court distinguished between public portions of commercial premises and "portions of commercial premises which are not open to the public." Likewise, in *Camara v. Municipal Court* (1967) 387 U.S. 523, and *Marshall v. Barlow's, Inc.* (1978) 436 U.S. 307, the Court recognized that administrative entry into nonpublic operational spaces implicates Fourth Amendment protections.

[43] See *Marshall v. Barlow's, Inc.* (1978) 436 U.S. 307, 309 ("[w]ithout a warrant, [an inspector] stands in no better position than a member of the public, they may observe what's in public areas but the Fourth Amendment requires a warrant for any intrusion into non-public spaces."). See also *See v. Seattle* (1967) 387 U.S. 541, 545, ("administrative entry, without consent, upon the portions of commercial premises which are not open to the public may only be compelled through prosecution or physical force within the framework of a warrant procedure.").

[44] Fourth Amendment protections also apply to government workspaces, See *Connor v. Ortega* (1987) 480 U.S. 709, 717, and extend to places where a person has an objectively reasonable expectation of privacy, See *Katz v. United States* (1967) 389 U.S. 347, 351, this can include, for example, areas not open to public access, See *See v. Seattle* (1967) 387 U.S. 541.

[45] A search only granted in submission to a claim of lawful of authority without a Fourth Amendment justification is unlawful. See *Schneckloth v. Bustamonte* (1973) 412 U.S. 218.

[46] Gov. Code, §§ 7285.1, 7285.2, 7285.3; Lab. Code, §§ 90.2, 1019.2.

[47] Gov. Code, § 7285.1, subd. (a).

[48] AB 450 FAQs [as of June 19, 2026].

[49] Gov. Code, § 7285.1 subd. (a).

[50] AB 450 FAQs [as of June 19, 2026].

[51] Gov. Code, § 7285.2, subd. (a)(1).

[52] Gov. Code, § 7285.2, subd. (a)(2).

[53] Lab. Code, §§ 1550.

[54] Lab. Code, § 1550 et seq.

[55] As a general principle, the Fourth Amendment protects people, not places and what a person knowingly exposes to the public is not a subject of Fourth Amendment protection, but what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. The inquiry is whether there was an objectively reasonable expectation of privacy from government intrusion. *Katz v. United States* (1967) 389 U.S. 347, 348.

[56] See, e.g., *Katz v. United States*, 389 U.S. 347, finding a person may have an objectively reasonable expectation of privacy in a conversation that takes place in a closed phone booth, even though it is in a public area.

[57] A sample Notice to Appear is provided in Appendix A.

[58] Immigration officers also have authority to make warrantless arrests when certain conditions are met, but this authority is constrained by the constitution, statute, and regulations, and it does not convey authority for the officer to enter nonpublic areas. See, e.g., 8 U.S.C. § 1357(a)(2); 8 C.F.R. § 287.8(c); *Tejeda-Mata v. Immigr. Naturalization Serv.* (9th Cir. 1980) 626 F.2d 721, 725.

[59] See, e.g., *Steagald v. United States* (1981) 451 U.S. 204, 205. Under the Fourth Amendment, a search warrant must be obtained, absent exigent circumstances or consent, for a law enforcement officer to legally search for the subject of an arrest warrant in the home of a third party; *Kidd v. Mayorkas* (C.D.Cal.2024) 734 F.Supp.3d 967. 978–979.

[60] See AB 450 guidance [as of June 19, 2026].

[61] Joffe-Block, *The Justice Department Plans to Share Sensitive Voter Data with Homeland Security* (Mar. 27, 2026) NPR [as of June 19, 2026]; Fields, *IRS Improperly Disclosed Immigrant Tax Data to DHS: Report* (Feb. 11, 2026) The Hill [as of June 19, 2026].

[62] In *Carpenter v. United States* (2018) 585 U.S. 296, the United States Supreme Court held that the government's acquisition of historical cell-site location information constituted a Fourth Amendment search requiring a warrant. The Court emphasized that the fact that information is held by a third party does not automatically eliminate constitutional privacy protections. The Court further recognized that certain categories of information are so revealing, comprehensive, and sensitive that individuals retain reasonable expectations of privacy in that information even where the data is maintained by third parties. Similarly, in *Riley v. California* (2014) 573 U.S. 373, the Court recognized that modern digital data systems contain "the privacies of life" and held that searching digital information on a cell phone generally requires a warrant. These principles are directly relevant to public agencies that maintain extensive electronic records systems, integrated databases, or sensitive personal information. Further, even where *Carpenter*'s recognition of limits on the third-party doctrine may not apply, agencies must still consider privacy protections afforded by statutes and other sources.

[63] Courts have repeatedly recognized that administrative subpoenas and similar demands may not be overbroad, indefinite, or unduly burdensome. For instance, in *United States v. Morton Salt Co*. (1950) 338 U.S. 632, 652–53 the Court explained that while agencies have investigatory authority, it is not unlimited and an administrative demand must not be "too indefinite." Likewise, in *United States v. Powell* (1964) 379 U.S. 48, 57–58, the Court explained that administrative demands must serve legitimate investigatory purposes and seek information relevant to those purposes. Courts have also recognized that overbroad or generalized demands for records may constitute impermissible "fishing expeditions." (*United States v. Golden Valley Elec. Ass'n*, (9th Cir. 2012) 689 F.3d 1108, 1113; *Peters v. United States* (9th Cir. 1988) 853 F.2d 692, 700.)

[64] In *United States v. Comprehensive Drug Testing, Inc.* (9th Cir. 2010) 621 F.3d 579 F.3d 989, 1005 (en banc) (per curiam), the Ninth Circuit recognized that large-scale copying of electronic information may expose substantial quantities of information beyond the scope of lawful authority.

[65] Cal. Const., art. I, § 1.

[66] *Hill v. Nat'l Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 17–18 (quoting *Porten v. Univ. of San Francisco* (1976) 64 Cal. App.3d 825, 829–830).

[67] *Planned Parenthood Golden Gate v. Superior Court* (2000) 83 Cal.App.4th 347, 357.

[68] *Hill v. Nat'l Collegiate Athletic Assn., supra,* 7 Cal.4th at 1, 17–18 ("'[T]he overbroad collection and retention of unnecessary personal information by government *and business interests*' was one of the principal 'mischiefs' at which the Privacy Initiative was directed.") (quoting *White v. Davis* (1975) 13 Cal.3d 757, 775).

[69] *White v. Davis* (1975) 13 Cal.3d 757, 775–76.

[70] *Hill v. Nat'l Collegiate Athletic Assn.*, *supra*, 7 Cal.4th at 38–40; *Loder v. City of Glendale* (1997) 14 Cal.4th 846, 897-898; *Britt v. Superior Court* (1978) 20 Cal.3d 844, 848–849 (observing "the authorities additionally demonstrate that even when such justification is present, the scope of the compelled disclosure must be narrowly circumscribed to avoid undue interference with private associational rights.").

[71] Voter registration elements, including street address, telephone number, email address, voter signatures, and unique identifiers used for identification, are confidential. See Elec. Code, § 2194; Gov. Code, § 7924.000.

[72] Information regarding a juvenile's involvement in a dependency or delinquency proceeding is confidential, with rules for disclosure strictly controlled by statute and court rules. See Welf. & Inst. Code, § 827; Cal. Rules of Court, rule 5.551. Absent a court order or clear statutory authorization, information from a juvenile case file should not be disclosed.

[73] Reports of suspected child abuse or neglect and related information are confidential and may be disclosed only as provided by law. See Pen. Code §§ 11167 subd. (d), 11167.5.

[74] Agencies must not disclose criminal history record information absent explicit statutory authorization and must apply strict access controls and auditing. See Pen. Code, § 11105.

[75] Agencies using automated license plate recognition (ALPR) systems are required to, among other things, implement reasonable security procedures, limit use and sharing of data to authorized purposes, and maintain a publicly available usage and privacy policy. See Civ. Code, §§ 1798.90.5–55. Toll operators must keep personally identifiable information, including ALPR-derived data, confidential, use it only for toll collection and enforcement, and not disclose it except in limited circumstances. See Sts. & Hy. Code, § 31490

[76] Information obtained in administering unemployment insurance programs is confidential and is subject to statutory disclosure limits. Unemp. Ins. Code, § 1094.

[77] Most public social services records are confidential and may only be used or disclosed as authorized by law. Welf. & Inst. Code, § 10850, subd. (a). This protection includes, but is not limited to, a recipient's name, address, or other identifier, household composition, eligibility documentation, and case records. See Welf. & Inst. Code, § 10850, subd. (a).

[78] California tax returns and information derived from tax documents are protected by stringent confidentiality rules, and California public employees may also make disclosures as provided by statute. See Rev. & Tax. Code, § 19542.

[79] Electrical and gas consumption data are protected. Disclosures are limited to specified conditions provided by statute. Agencies holding such data must treat it as confidential. See Pub. Util. Code, §§ 8380–8381; Decision 11-07-056, Cal. Pub. Utils. Comm'n (July 29, 2011) (interpreting consent and privacy requirements under § 8380).

[80] See 18 U.S.C. §§ 2721–2725; Veh. Code § 1808.

[81] 20 U.S.C. § 1232g.

[82] 20 U.S.C. § 1232g(b)(1).

[83] See Educ. Code, § 49076.

[84] 45 C.F.R. § 164.502(a) (implementing 42 U.S.C. § 1320d-2).

[85] See Civ. Code §§ 56 et seq.

[86] Welf. & Inst. Code, § 14100.2, subd. (a).

[87] The definition of personal information is provided by Civ. Code, § 1798.3, subd. (a).

[88] For example, California Code of Civil Procedure section 1985.3, subdivision (b), requires a party subpoenaing the production of records containing "personal information" of a "consumer" to provide the consumer with notice of the subpoena prior to the deadline for responding to the subpoena.

[89] See Appendix E for a sample administrative subpoena (Form I-138).

[90] See 8 U.S.C. § 1225(d)(4); *In re Ramirez* (5th Cir. 1990) 905 F.2d 97, 98.

[91] *Peters v. United States*, *supra*, 853 F.2d at 700 (quashing subpoena seeking records relating to all persons residing at a particular labor camp as overly broad).

[92] *United States v. Baass* (C.D. Cal., Mar. 4, 2026, No. 2:25-mc-00083-JLS-SSC) 2026 WL 898670, at *4, report and recommendation adopted (C.D. Cal., Mar. 31, 2026, No. 2:25-MC-00083-JLS-SSC) 2026 WL 897012 (26-3537, app. pending) (holding Homeland Security Investigations lacked jurisdiction to prosecute California for violating 8 U.S.C. § 1324(a)(1)(A)(iv) since the statute and INA did not authorize a state or state agency employee in their official capacity to be investigated or prosecuted criminally when California's coverage of nonemergency medical services for noncitizens was permitted under federal law.); see *Peters v. United States*, *supra*, 853 F.2d at 699 (quashing INS third-party subpoena issued in connection with a general criminal investigation of a group of unnamed tenants at a camp who may be undocumented immigrants, holding that 8 U.S.C. § 1225 did not authorize the INS to issue broad "John Doe" subpoenas similar to IRS "John Doe" subpoenas, since Congress did not intended for the INS to possess the same subpoena authority given to the IRS as authorized under 26 U.S.C. §§ 7602, 7609).

[93] *United States v. Golden Valley Elec. Ass'n*, *supra*, 689 F.3d at 1113 (citation omitted).

[94] *Ibid.*

[95] *Id.* at 1115 (internal punctuation and citations omitted). See *United States v. Morton Salt Co.*, *supra*, 338 U.S. at 652 ("[A] governmental investigation … may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power.").

[96] See, e.g., *United States v. Powell supra,* 379 U.S. at 58.

[97] *Peters v. United States supra*, 853 F.2d at 700.

[98] See Appendix F for a sample federal judicial subpoena (Form AO 88B).

[99] Gov. Code, § 7922.000 and 7927.705; *Sander v. State Bar of California* (2013) 58 Cal.4th 300, 327; *Haynie v. Superior Court* (2001) 26 Cal.4th 1061, 1073–1074.

[100] Gov. Code, § 7922.525, subd. (b); *Freedom Foundation v. Superior Court* (2022) 87 Cal.App.5th 47, 57, *as modified* (Dec. 30, 2022).

[101] See Gov. Code, § 7921.300 (requiring purpose-neutral access to public records).

[102] See, e.g., *City & Cty. of S.F. v. Trump* (9th Cir. 2018) 897 F.3d 1225, 1234–35.

[103] The United States Supreme Court has explained that conditions on federal funding must be unambiguous, must be related to the federal interest in the program, and must not be coercive. See *South Dakota v. Dole* (1987) 483 U.S. 203, 207–208; *NFIB v. Sebelius* (2012) 567 U.S. 519, 575–585. In addition, federal agencies may not impose conditions that exceed their statutory authority or conflict with other provisions of federal or state law. Where an agency attempts or purports to require state or local entities to take actions that are not authorized by statute, or that are inconsistent with constitutional limits, those conditions may be subject to legal challenge.

[104] See *California v. HHS* (N.D.Cal. Dec. 29, 2025, No. 3:25-cv-05536), Order Granting in Part and Denying in Part Motion for Preliminary Injunction (ECF No. 148) at pp. 6–7 (preliminarily enjoining DHS and HHS from sharing and using some Medicaid data for immigration enforcement purposes).

[105] See *California v. USDA* (N.D.Cal. Oct. 15, 2025, No. 25-cv-06310-MMC) Order Granding Preliminary Injunction (ECF No. 106) at pp. 17–19 (granting a preliminary injunction blocking USDA's demand to share SNAP data after finding States were likely to succeed on the merits because statute permits but does not require disclosure, demand reaches beyond information obtained from households, and announced use exceeds permitted purposes); *California v. USDA*, (N.D.Cal. Feb. 26, 2026) Order Granting in Part Motion to Enforce or Expand Preliminary Injunction (ECF No. 134) at pp. 13–15 (expanding injunction to cover USDA's renewed demand); see also 7 U.S.C. § 2020(e)(8)(a) (addressing safeguards prohibiting the use or disclosure of data obtained from SNAP applicants and permitted exceptions to the safeguards).

[106] Sen. Bill No. 580 (2025-2026 Reg. Sess.), Stats. 2025, ch. 670 (adding Gov. Code, § 12532.5).

[107] See Civ. Code, § 1798.14.

[108] See Civ. Code, § 1798.3, subd. (a).

[109] See *United States v. California* (9th Cir. 2019) 921 F.3d 865, 891; *City & Cnty. of San Francisco v. Garland* (9th Cir. 2022) 42 F.4th 1078, 1085 ("We have rejected DOJ's interpretation of Section 1373 repeatedly… . Section 1373 only covers immigration-status information—*i.e.*, 'what one's immigration status is.'") (quoting *U.S. v. California*, 921 F.3d at 891); *Steinle v. City & Cnty. of San Francisco* (9th Cir. 2019) 919 F.3d 1154, 1164 ("The statutory text … includes only 'information regarding' 'immigration status,' and nothing in §§ 1373(a) or 1644 addresses information concerning an inmate's *release date*.") (emphasis in original). See also, discussion of Privacy and Confidentiality, *supra* p. 20.

[110] Gov. Code, § 12532.5, subd. (b).

[111] Francis, *Data Minimization's Substantive Turn Key: Questions & Operational Challenges Posed by New State Privacy Legislation* (June 2025) Future of Privacy Forum U.S. Legislation White Paper [as of June 5, 2026].

[112] See Gov. Code, § 11019.9; see also *Frequently Asked Questions (FAQs)* California Privacy Protection Agency [as of June 5, 2026]; *Protecting Personal Information: A Guide for Business* Federal Trade Commission [as of June 5, 2026]; *Data Minimization* Washington Technology Solutions [as of June 5, 2026].

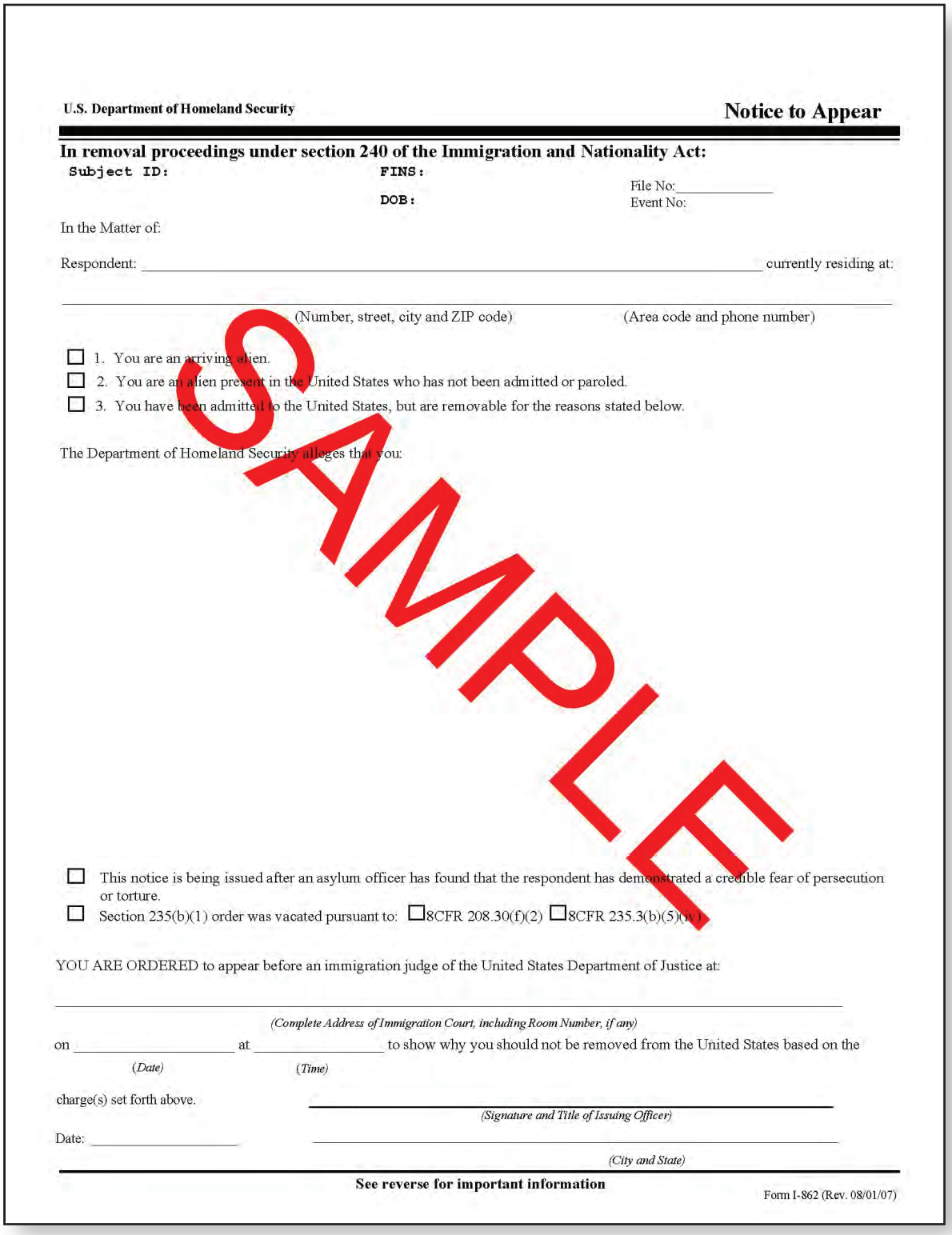
[113] See *Immigration, DOGE and Data Privacy* (May 9, 2025) Center for Democracy & Technology and The Leadership Conference's Center for Civil Rights and Technology [as of June 5, 2026].

[114] Cascio, Lewis, and Zhang, *How Good Are Proxies For Legal Status Evidence From The Legalization Of Two Million Mexicans* (Sept. 2024) National Bureau of Economic Research [as of June 19, 2026].

[115] See Chapter 1: Legal Framework

[116] For information about who may represent individuals in immigration proceedings, see U.S. Dept. of Justice, *Can Someone Represent You Before EOIR?* [as of June 19, 2026].

Appendix A
Notice to Appear (Form I-862)



U.S. Department of Homeland Security — **Notice to Appear**

In removal proceedings under section 240 of the Immigration and Nationality Act:

Subject ID: FINS: DOB:

File No:_____
Event No:

In the Matter of:

Respondent: _____ currently residing at:

_____
(Number, street, city and ZIP code) (Area code and phone number)

☐ 1. You are an arriving alien.
☐ 2. You are an alien present in the United States who has not been admitted or paroled.
☐ 3. You have been admitted to the United States, but are removable for the reasons stated below.

The Department of Homeland Security alleges that you:

SAMPLE

☐ This notice is being issued after an asylum officer has found that the respondent has demonstrated a credible fear of persecution or torture.
☐ Section 235(b)(1) order was vacated pursuant to: ☐8CFR 208.30(f)(2) ☐8CFR 235.3(b)(5)(iv)

YOU ARE ORDERED to appear before an immigration judge of the United States Department of Justice at:

_____
(Complete Address of Immigration Court, including Room Number, if any)

on _____ at _____ to show why you should not be removed from the United States based on the
(Date) *(Time)*

charge(s) set forth above.

_____
(Signature and Title of Issuing Officer)

Date: _____

_____
(City and State)

See reverse for important information

Form I-862 (Rev. 08/01/07)

Appendix B

ICE (Immigrations and Customs Enforcement) "Arrest Warrant" (Form I-200)

U.S. DEPARTMENT OF HOMELAND SECURITY **Warrant for Arrest of Alien**

File No. _____

Date: _____

To: **Any immigration officer authorized pursuant to sections 236 and 287 of the Immigration and Nationality Act and part 287 of title 8, Code of Federal Regulations, to serve warrants of arrest for immigration violations**

I have determined that there is probable cause to believe that _____ is removable from the United States. This determination is based upon:

☐ the execution of a charging document to initiate removal proceedings against the subject;

☐ the pendency of ongoing removal proceedings against the subject;

☐ the failure to establish admissibility subsequent to deferred inspection;

☐ biometric confirmation of the subject's identity and a records check of federal databases that affirmatively indicate, by themselves or in addition to other reliable information, that the subject either lacks immigration status or notwithstanding such status is removable under U.S. immigration law; and/or

☐ statements made voluntarily by the subject to an immigration officer and/or other reliable evidence that affirmatively indicate the subject either lacks immigration status or notwithstanding such status is removable under U.S. immigration law.

YOU ARE COMMANDED to arrest and take into custody for removal proceedings under the Immigration and Nationality Act, the above-named alien.

_____
(Signature of Authorized Immigration Officer)

_____
(Printed Name and Title of Authorized Immigration Officer)

Certificate of Service

I hereby certify that the Warrant for Arrest of Alien was served by me at _____ (Location)

on _____ (Name of Alien) on _____ (Date of Service), and the contents of this notice were read to him or her in the _____ (Language) language.

_____ Name and Signature of Officer

_____ Name or Number of Interpreter (if applicable)

Form I-200 (Rev. 09/16)

Appendix B

ICE (Immigrations and Customs Enforcement) "Removal Warrant" (Form I-205)

DEPARTMENT OF HOMELAND SECURITY
U.S. Immigration and Customs Enforcement

WARRANT OF REMOVAL/DEPORTATION

File No: _____

Date: _____

To any immigration officer of the United States Department of Homeland Security:

_____
(Full name of alien)

who entered the United States at _____ on _____
(Place of entry) (Date of entry)

is subject to removal/deportation from the United States, based upon a final order by:

- ☐ an immigration judge in exclusion, deportation, or removal proceedings
- ☐ a designated official
- ☐ the Board of Immigration Appeals
- ☐ a United States District or Magistrate Court Judge

and pursuant to the following provisions of the Immigration and Nationality Act:

I, the undersigned officer of the United States, by virtue of the power and authority vested in the Secretary of Homeland Security under the laws of the United States and by his or her direction, command you to take into custody and remove from the United States the above-named alien, pursuant to law, at the expense of:

_____
(Signature of immigration officer)

_____
(Title of immigration officer)

_____
(Date and office location)

Appendix C

Federal Search and Seizure Warrant (Form AO 93)

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

) Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

YOU ARE COMMANDED to execute this warrant on or before _____ *(not to exceed 14 days)*
❒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: _____ _____
Judge's signature

City and state: _____ _____
Printed name and title

Appendix D

Federal Arrest Warrant (Form AO 442)

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

United States of America
v.

Case No.

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) _____ ,

who is accused of an offense or violation based on the following document filed with the court:

❒ Indictment ❒ Superseding Indictment ❒ Information ❒ Superseding Information ❒ Complaint

❒ Probation Violation Petition ❒ Supervised Release Violation Petition ❒ Violation Notice ❒ Order of the Court

This offense is briefly described as follows:

Date: _____

_____
Issuing officer's signature

City and state: _____

_____
Printed name and title

Return

This warrant was received on *(date)* _____ , and the person was arrested on *(date)* _____

at *(city and state)* _____ .

Date: _____

_____
Arresting officer's signature

_____
Printed name and title

Appendix E

DHS Immigration Enforcement Subpoena (Form I-138)

1. To (Name, Address, City, State, Zip Code)	DEPARTMENT OF HOMELAND SECURITY **IMMIGRATION ENFORCEMENT SUBPOENA** **to Appear and/or Produce Records** 8 U.S.C. § 1225(d), 8 C.F.R. § 287.4
Subpoena Number	
2. In Reference To (Title of Proceeding) (File Number, if Applicable)	

By the service of this subpoena upon you, **YOU ARE HEREBY SUMMONED AND REQUIRED TO:**

(A) ☐ **APPEAR** before the U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), or U.S. Citizenship and Immigration Services (USCIS) Official named in Block 3 at the place, date, and time specified, to testify and give information relating to the matter indicated in Block 2.

(B) ☒ **PRODUCE** the records (books, papers, or other documents) indicated in Block 4, to the CBP, ICE, or USCIS Official named in Block 3 at the place, date, and time specified.

Your testimony and/or production of the indicated records is required in connection with an investigation or inquiry relating to the enforcement of U.S. immigration laws. Failure to comply with this subpoena may subject you to an order of contempt by a federal District Court, as provided by 8 U.S.C. § 1225(d)(4)(B).

3. (A) CBP, ICE or USCIS Official before whom you are required to appear Name Title Address Telephone Number	(B) Date (C) Time ☒ a.m. ☐ p.m.
4. Records required to be produced for inspection	

If you have any questions regarding this subpoena, contact the CBP, ICE, or USCIS Official identified in Block 3.

5. Authorized Official

(Signature)

(Printed Name)

(Title)

(Date)

DHS Form I-138 (6/09)

Appendix F

Federal Judicial Subpoena (Form AO 88B)

AO 88B (Rev. 02/14) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT

for the

_____)
Plaintiff)
v.) Civil Action No.
_____)
Defendant)

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To:

_____
(Name of person to whom this subpoena is directed)

❒ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material:

Place:	Date and Time:

❒ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: _____

CLERK OF COURT

OR

_____ _____
Signature of Clerk or Deputy Clerk *Attorney's signature*

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* _____
_____, who issues or requests this subpoena, are:

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Appendix G

Reference Guide — Immigration Enforcement Documents Description of Legal Documents Presented by Immigration Enforcement

This document provides a brief overview of the types of documents that an immigration enforcement officer may present when seeking to enter a public facility, whether to conduct a search or an arrest or when requesting records. Not all documents authorize immigration enforcement to enter a facility or to obtain records. Samples of each document are found in the appendix to this guide.

When an immigration enforcement agent asks for permission to enter a nonpublic area of a state or local agency facility or for information about a state or local agency client, staff should first ask the immigration enforcement agent to present credentials. Staff should immediately notify designated personnel, a supervisor, or agency legal counsel of the request. Staff should also collect any documents presented by the immigration enforcement officer that purport to require compliance with the officer's request. Designated staff or legal counsel should review the sufficiency of any documents presented by the immigration enforcement officer before complying with a request.

ICE Administrative "Warrant"

An ICE administrative "warrant" is issued by certain immigration enforcement officers at ICE or other agencies within DHS (see Appendix B). The "warrant" authorizes the officer to arrest a person suspected of violating immigration laws, but it is not a warrant within the meaning of the Fourth Amendment to the U.S. Constitution.

When presented with an ICE administrative "warrant," personnel are not required to cooperate with the officer's request(s), including helping apprehend the person named in the "warrant" or consenting to an officer's search. Subject to a few exceptions, an agency cannot voluntarily consent to an officer seeking access to a nonpublic area. However, staff should not physically interfere with an officer in the performance of their duties.

Notice to Appear

A notice to appear (NTA) is issued by ICE, CBP, or the USCIS to commence formal removal proceedings against an individual before an immigration court (see Appendix A). An NTA notifies an individual that they are expected to appear before an immigration judge on a certain date, but it does not authorize authorities to arrest the individual.

When presented with an NTA, staff are not required to take any action or cooperate with requests from authorities, including authorizing access to nonpublic areas of an agency or allowing authorities to search agency records.

Federal Search or Arrest Warrant

A federal court warrant is issued by a district judge or a magistrate of a U.S. District Court based on a finding of probable cause. A search warrant authorizes the search or seizure of property, entry into a nonpublic area to arrest a named person while an arrest warrant authorizes the arrest of a named person.

Staff should carefully review the federal court warrants, which come in two types: (1) a federal search-and-seizure warrant allows an officer to conduct a search authorized by the warrant (see Appendix C), and (2) a federal arrest warrant allows an officer to arrest the individual named in the warrant (see Appendix D).

The warrant should include a judge's signature and identifying details about the place to be searched (e.g., address). While it typically specifies the exact area an officer is authorized to search, the warrant may not grant permission to search the entire shelter. When presented with a valid federal court warrant, prompt compliance is typically required. Where feasible, designated staff or legal counsel should review before an agency responds.

Administrative Subpoena

An administrative subpoena is issued by an immigration enforcement officer to request the production of records (see Appendix E). The subpoena will contain the file number, subpoena number, mailing address, list of applicable regulations, request for information, and signature(s) of the officer(s).

When presented with an administrative subpoena, staff generally need not comply immediately. If the officer arrives with a pre-designated subpoena, agency staff may decline to produce records and challenge the subpoena before a federal judge in a U.S. District Court. Therefore, agency staff should immediately contact designated staff, a supervisor, or legal counsel upon receipt of the subpoena.

Federal Judicial Subpoena

A federal judicial subpoena requests the production of records. It does not require staff to grant access to a particular place or person. The subpoena will identify a federal court and the name of the issuing judge or magistrate (see Appendix F).

When presented with a federal judicial subpoena, staff generally are not required to comply immediately. A subpoenaed agency may challenge the subpoena before the issuing court. Therefore, agency staff should immediately contact designated staff or legal counsel upon receipt of the subpoena.

Court Order

A court order is a directive signed by a judge that requires a person or organization to do something or stop doing something. Whoever it is directed at must comply. If an immigration enforcement officer arrives with a court order, a designated staff or legal counsel should review the order and respond consistent with the scope of the order.

Type of Legal Document	Issued By	Action(s) Required	Immediate Compliance Necessary?
ICE Administrative "Warrant"	Immigration enforcement officer (not always ICE)	No action required on the part of the state or local agency. The "warrant" only authorizes the officer to arrest an individual suspected of violating immigration laws.	No
Notice to Appear (NTA)	Immigration enforcement agencies (usually ICE, CBP, or USCIS)	No action required on the part of the state or local agency. The NTA only notifies an individual that they are expected to appear before an immigration judge for a formal removal proceeding.	No
Federal Court Arrest or Search Warrant	Federal judge (district court judge or magistrate judge)	A judicial search warrant authorizes a search of a specific location for evidence; a federal arrest warrant authorizes the arrest of a specific person.	Yes, but the scope of the warrant determines the extent of compliance
Administrative Subpoena	Immigration enforcement officer	No action required. Under California law, a notice to consumer may be required before any information or documents about the consumer are produced.	No
Federal Judicial Subpoena	Federal judge or magistrate	If valid, the production of records but immediately compliance is not required. Agency served with a subpoena may petition a court to squash or limit the scope of the subpoena.	No
Court Order	Judge or magistrate	A designated administrator or legal counsel should review the order and respond accordingly.	Yes
Public Records Act Request	Requestor	Before complying with the request, determine if it is in the public interest to withhold the information or if exemptions or privileges apply. If agency decides to produce a record, agency should first determine if redaction of non-disclosable information under state law or agency policy is required. Under California, a notice to consumer may be required before any information or documents about the consumer are produced.	No