California Public Records: A Technical and Legal Reference for the Post-AB 473 Era

Statutes, Portals, APIs, Schemas, and Exemptions

Daniel Ari Friedman

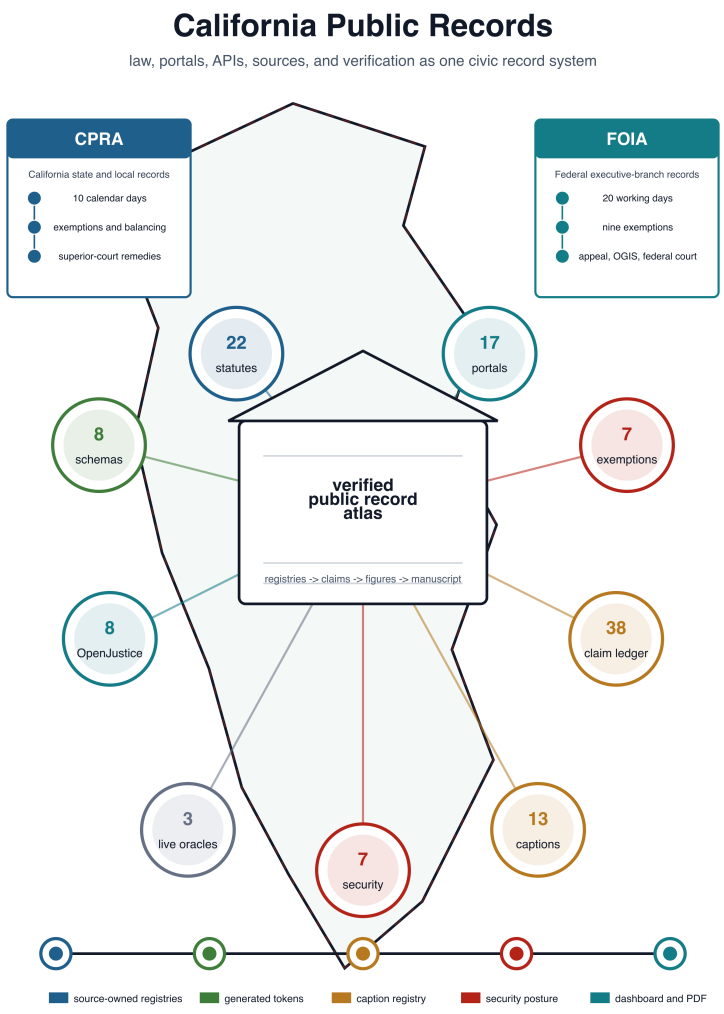
Active Inference Institute, FractAI

daniel@activeinference.institute

ORCID: 0000-0001-6232-9096

DOI: 10.5281/zenodo.20789899

June 21, 2026



Federal FOIA appears as comparator context; CPRA remains the California legal center.

Contents

1 Abstract

California maintains a highly codified public-records ecosystem anchored by the **California Public Records Act (CPRA)**, recodified by Assembly Bill 473 effective January 2023 to Government Code §§ 7920.000 et seq., and extended in practice through state and local open-data portals, request platforms, API frameworks, metadata schemas, intergovernmental data-sharing surfaces, and exemption rules that determine what must be disclosed and in what form. This reference compiles that ecosystem as a machine-readable and reproducible artifact: 22 registered CPRA statute sections across 5 structural categories; 17 open-data and request portals across 7 hosting platforms and 10 subject-matter domains; 7 exemption clusters, including 1 balancing-test and 6 categorical clusters; a 8-dataset OpenJustice taxonomy; standard-library clients for programmatic API surfaces; and a Federal FOIA comparator that clarifies where California state and local access law differs from federal executive-branch disclosure, reporting, appeal, and FOIA.gov API infrastructure. Every registry-derived number in the prose is generated from the source registries, every non-token factual claim is tied to the claim ledger or a cited primary source, every figure caption is emitted from the caption registry, and the defensive security layer maps source poisoning, citation laundering, dependency compromise, build provenance, artifact tampering, live-source volatility, and secret-handling risk to explicit local controls and target posture. The result is both a technical reference for requesters, researchers, journalists, civic technologists, and public agencies, and a reproducibility contract: the same version-controlled inputs regenerate the inventories, validation reports, analytical figures, dashboard, manuscript variables, title-page cover art, and paper outputs while preserving explicit caveats around legal authority, portal completeness, live-source volatility, security posture, and remaining verification residuals.

2 Introduction

California's public-records infrastructure is the product of a five-decade legal arc that began with the California Public Records Act of 1968 — passed by the California Legislature for state and local governments and associated with Assemblyman William T. "Bill" Bagley [California Correctional Health Care Services, 2026, San Francisco Chronicle, 2024] — and now sits atop a federated open-data architecture coordinated by GovOps and the California Department of Technology. The goal of this document is to make that infrastructure legible — to researchers writing CPRA requests, to developers building against the state's APIs, and to civic-technology operators stewarding shared data assets.

2.1 Why a registry-first reference

A typical CPRA "primer" mixes prose summaries of statutory text with screenshots of portal landing pages. Both rot quickly: section numbers were renumbered wholesale by AB 473 in 2023, and portal endpoints migrate as agencies retire on-premises CKAN deployments in favour of managed Socrata, ArcGIS Hub, or custom React-based front-ends. This reference inverts that pattern: every section number, portal URL, schema field, and dataset cited in the prose comes from a Python registry under `src/`, and every count in the abstract — "22 statutes", "17 portals", "8 OpenJustice datasets" — is a double-brace token resolved at build time by `src.manuscript_variables.generate_variables`.

The discipline this enforces is identical to the `template_code_project` reproducibility model: configuration drift, deleted result, or out-of-sync narrative cannot reach a green PDF without the manuscript-token closure test (`tests/test_manuscript_variables.py::test_all_manuscript_tokens_are_generated`) flipping red first.

2.2 Scope

This reference covers:

1. **The statutory framework** — CPRA general access, the 10-day determination deadline, the public-interest balancing test, the recodified exemption clusters, and the SB 272 enterprise systems catalog requirement (sec. 3).
2. **The portal ecosystem** — the federated "portal of portals" model; the operating agencies and platforms behind each portal (sec. 4).
3. **The API patterns** — CKAN Action API, Socrata SoQL, ArcGIS GeoServices REST, CIMIS REST, OpenJustice CSV downloads, and LegiScan bulk-data endpoints, each with a working Python client in `src/clients/` (sec. 5).
4. **The metadata schemas** — DCAT (with California extensions), the CKAN package shape, Dublin Core (as used by CHHS), and the RIPA stop-data field set (sec. 7).
5. **Domain-specific portals** — health, water, justice, environment, finance, business, elections (sec. 8).
6. **The exemption taxonomy** — the 7 structural clusters that govern when an agency may withhold a record (sec. 9).
7. **The package itself** — its architecture as an inputs → methods → outputs data-flow, the input registry/validator/client composition, and the produced artifact set, so the machinery is as auditable as the data (sec. 6).
8. **Cognitive-security implications** — how a registry-first, machine-readable disclosure record functions as information-ecosystem infrastructure, and where open data, source provenance, and build artifacts become an attack surface (sec. 11).

The figures throughout are regenerated from the same registries: the legislative timeline (fig. 1), the statute category and cross-reference views (fig. 2, fig. 3), the citation-provenance breakdown (fig. 5), and the portal ecosystem by platform, domain, and API surface (fig. 6, fig. 7, fig. 9). The package's own structure is shown as a data-flow pipeline (fig. 10) with its inputs (fig. 11), produced artifacts (fig. 12), and defensive security posture (fig. 13).

3 Legal and Statutory Framework

3.1 The CPRA in its current form

The California Public Records Act was originally enacted in 1968 (Stats. 1968, ch. 1473), signed by Governor Ronald Reagan and modeled closely on the federal Freedom of Information Act (5 U.S.C. § 552), whose exemption taxonomy the CPRA's categories still echo [Wikipedia, 1968, U.S. Department of Justice, Office of Information Policy, 1966, California Correctional Health Care Services, 2026]. **Assembly Bill 473**, signed in late 2021, recodified the Act effective January 1, 2023, moving it from Government Code §§ 6250–6276.48 into the new Division 10 beginning at Government Code § 7920.000 [Lozano Smith, 2023, Liebert Cassidy Whitmore, 2022, California Law Revision Commission, 2019]. The reorganization made no substantive changes to disclosure rights but split the formerly monolithic exemption list into multiple independent code sections, improving readability and navigation; the California Law Revision Commission disposition table is the crosswalk used here to keep former and current citations distinct. The full arc of California public-records legislation is shown in fig. 1.

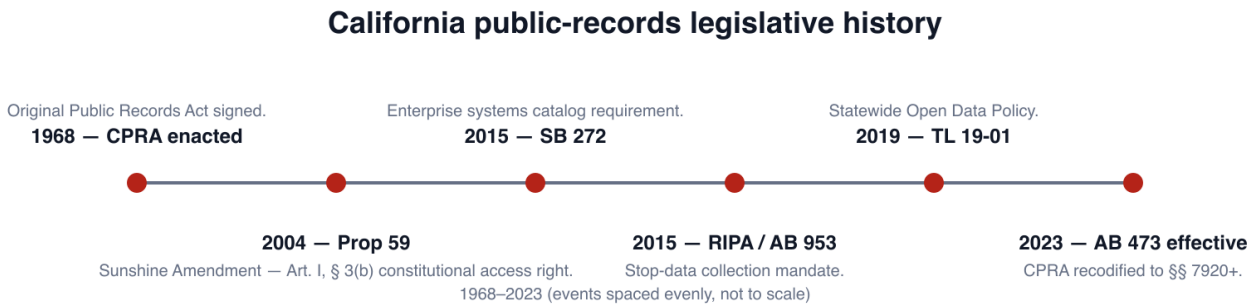


Figure 1: Legislative timeline of California public-records law, from the 1968 CPRA enactment through Proposition 59 and the AB 473 recodification effective January 1, 2023. Provenance: `src/legislative_history.py` and the statutory bibliography. Caveat: the figure is a selected public-records chronology, not a complete history of every transparency statute.

The Act is cited as the California Public Records Act at Gov. Code § 7920.000; the operative general right of access is stated at Gov. Code § 7922.525: every person may inspect and obtain copies of public records maintained by any state or local agency unless the record is exempt by law [Justia, 2025, First Amendment Coalition, 2024]. The definition of a "public record" appears at Gov. Code § 7920.530 as any *writing* containing information relating to the conduct of the public's business prepared, owned, used, or retained by any agency. That reach is not confined to records held on government systems: in *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608, the California Supreme Court held that communications about the public's business sent or received on officials' *personal* accounts or devices are public records subject to disclosure [Supreme Court of California, 2017] — a holding that is load-bearing for any digital-records audit.

The access right is not purely statutory. In 2004 California voters adopted **Proposition 59**, the "Sunshine Amendment," adding **Article I, § 3(b)** to the state Constitution: the people have a right of access to information concerning the conduct of the people's business, and every statute, court rule, or other authority must be *broadly* construed if it furthers that right and *narrowly* construed if it limits it [California Secretary of State, 2004, Legislative Analyst's Office, 2004]. That constitutional canon — not merely the CPRA's own purpose clause — is the source of the rule that the burden of justifying secrecy falls on the agency and that access is the default.

3.2 Statutory registry

The full registry of 22 statute sections currently encoded by this project, across 5 categories, is shown below. fig. 2 summarizes the category distribution, and fig. 3 shows which sections cross-reference external statutory authority.

Citation	Short Title	Category
Gov. Code § 7920.000	CPRA name and citation	definition
Gov. Code § 7920.510	Definition of local agency	definition
Gov. Code § 7920.530	Definition of public records	definition

Citation	Short Title	Category
Gov. Code § 7920.545	Definition of writing	definition
Gov. Code § 7922.000	Public-interest balancing test	procedure
Gov. Code § 7922.525	General right of access and segregability	procedure
Gov. Code § 7922.535	Ten-day determination deadline	procedure
Gov. Code § 7922.570	Electronic-format production	procedure
Gov. Code § 7922.575	Direct cost of duplicating an electronic record	procedure
Gov. Code § 7922.600	Agency duty to assist requesters	procedure
Gov. Code § 7923.600	Law enforcement complaints and investigations exemption	exemption
Gov. Code § 7924.000	Voter registration information confidentiality	exemption
Gov. Code § 7927.200	Pending litigation and tort-claim records exemption	exemption
Gov. Code § 7927.410	Public-utility customer data confidentiality	exemption
Gov. Code § 7927.500	Preliminary drafts and interagency memoranda exemption	exemption
Gov. Code § 7927.700	Personnel, medical, and similar files privacy exemption	exemption
Gov. Code § 7928.200	Online-service liability shield (elected-official info)	exemption
Penal Code § 832.7	Peace-officer personnel-record disclosure list	exemption
Gov. Code § 7923.000	Enforcement remedy — injunctive, declarative, mandate	enforcement
Gov. Code § 7923.115	Attorneys' fees and costs	enforcement
Gov. Code § 6253.10	Statutory open-data definition for local agencies	open_data
Gov. Code § 6270.5	SB 272 enterprise systems catalog	open_data

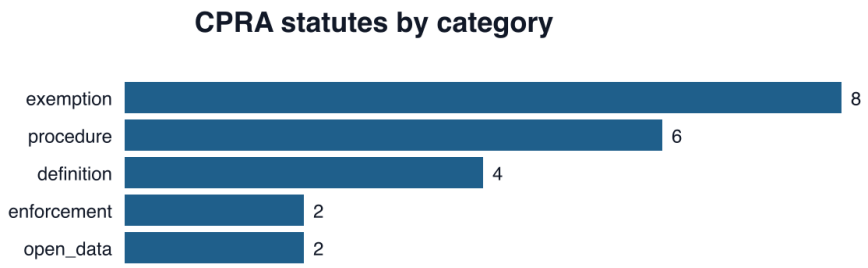


Figure 2: The 22 registered statute sections grouped into 5 structural categories. Provenance: `src/statutes.py` via `src.metrics.compute()`. Caveat: counts describe the project registry, not every California disclosure statute outside the CPRA/open-data scope.

3.3 Procedural posture

Under Gov. Code § 7922.535, agencies must respond within **10 calendar days** of receipt with a determination as to whether the request will be honoured [California State Legislature, 2026, California Department of Justice, Office of the Attorney General, 2026b, California Commission on Peace Officer Standards and Training, 2024, San Diego Law Library, 2024]. The 10-day window is a *determination* deadline, not a production deadline; unusual circumstances may support a written extension, but the statute caps that extension at 14 days. Requests may be submitted orally or in writing, in person, by phone, by mail, by email, or through digital portals. Where a record is held electronically, the agency must

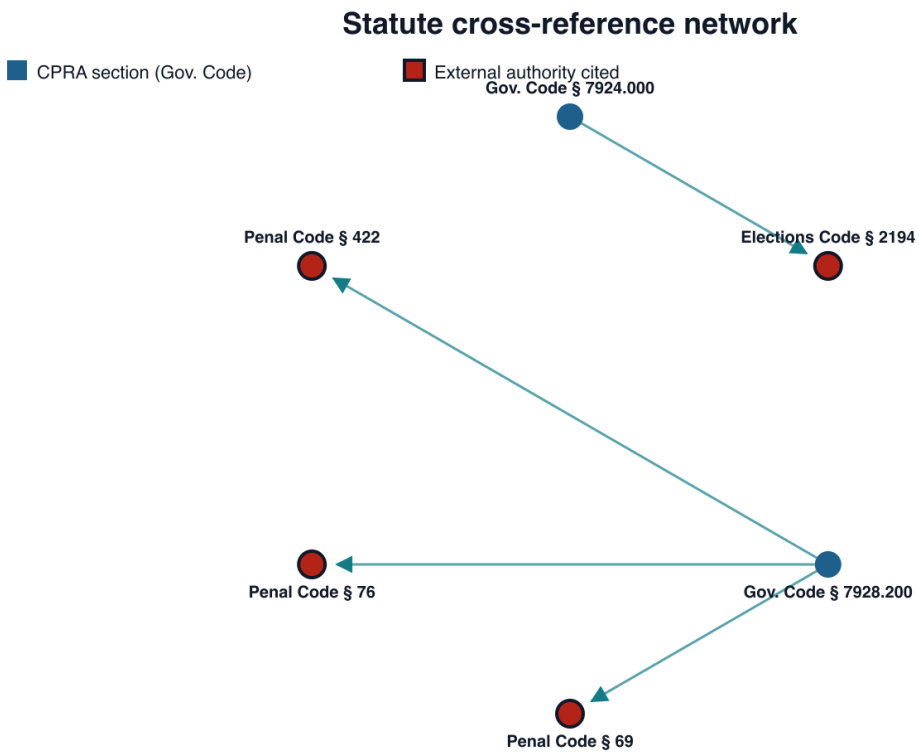


Figure 3: Cross-reference network for registered statute sections that cite external statutory authority. Arrows run from the registered CPRA section to the cited authority; solid nodes are Government Code sections and ringed nodes are external authorities. Provenance: the `cross_references` fields in `src/statutes.py`. Caveat: no edge is inferred from prose; absent edges mean the registry does not encode a cross-reference.

produce it in any electronic format in which it holds the information — the electronic-format mandate at Gov. Code § 7922.570, the recodified successor to former § 6253.9, which makes machine-readable production a statutory entitlement rather than a courtesy [California State Legislature, 2023].

Under AB 1819, requesters who inspect records on agency premises may use their own reproduction equipment at no charge [Best Best & Krieger, 2024]. Per the California Supreme Court's narrowing of cost-recovery provisions in *National Lawyers Guild v. City of Hayward* (2020) 9 Cal.5th 488, agencies may not charge for the time spent searching folders or redacting exempt material; only direct duplication and genuine data-extraction costs are recoverable [Supreme Court of California, 2020, Dannis Woliver Kelley, 2022].

3.4 Federal FOIA comparison boundary

Federal FOIA is the closest national comparator for the CPRA, but it is not a California authority. NARA summarizes FOIA as a right to request records of the **executive branch** of the U.S. Government, subject to nine exemptions, and notes that FOIA does not apply to records of Congress, the Supreme Court, or archival legislative and judicial branch records [National Archives and Records Administration, 2026]. OGIS states the same boundary more operationally for requesters: FOIA covers executive-branch records, not the legislative or judicial branches [Office of Government Information Services, National Archives and Records Administration, 2023]. That jurisdiction line is the main reason this manuscript treats FOIA as comparison and API context rather than as part of the California registry.

The deadline posture also differs. CPRA uses the 10-calendar-day determination window above; Federal FOIA requires an agency determination within 20 days excluding Saturdays, Sundays, and legal public holidays, includes appeal and dispute-resolution notice rights, and allows an unusual-circumstances extension that generally cannot exceed 10 working days [FOIA.gov, U.S. Department of Justice, 2026a, U.S. Department of Justice, Office of Information Policy, 2026]. Federal FOIA also has a stronger statutory reporting/data layer: records requested three or more times can trigger electronic reading-room treatment, and agencies publish annual reporting data that FOIA.gov exposes through downloadable and API-oriented surfaces. fig. 4 visualizes the CPRA/FOIA comparison without merging their legal regimes.

3.5 The public-interest balancing test

The catch-all balancing test of Gov. Code § 7922.000 allows withholding only when the agency demonstrates the public interest in nondisclosure *clearly outweighs* the public interest in disclosure. The standard is high: the burden is the agency's and the default is access — a posture the *Times Mirror* line of cases applies even to deliberative-process claims, which are weighed under this test rather than treated as an automatic bar [Supreme Court of California, 1991, 1986].

3.6 Open-data statutes

Two statutes establish the open-data backbone for local agencies.

- Gov. Code § 6253.10 is the only place California statute speaks to "open data" at all — and even there it supplies a *format standard* rather than a general definition: when a local agency *voluntarily* publishes data it labels "open data," that publication must be platform-independent, machine-readable, freely accessible, and must preserve the data's compiled-form definitions and structure [California State Legislature, 2021a, California State Library, 2018].
- Gov. Code § 6270.5 (SB 272, Stats. 2015, ch. 795, chaptered October 2015 with first catalogs due July 1, 2016) requires each local agency (except local education agencies) to publish a catalog of *enterprise systems* serving as original data sources, updated annually [California State Legislature, 2015b, Santa Cruz County, 2016, Rancho Cordova School District, 2016].

Both open-data statutes retain their pre-recodification (former Division-7) section numbers; fig. 5 classifies every registry citation by its recodification provenance and makes that honesty machine-visible.

The corresponding statewide administrative framework is California Department of Technology **Technology Letter 19-01** (March 2019), which created State Administrative Manual §§ 5160 / 5160.1 / 5160.2 and updated § 4819.2, establishing `data.ca.gov` as the centralized statewide portal [California Department of Technology, 2019, California Department of General Services, 2019].

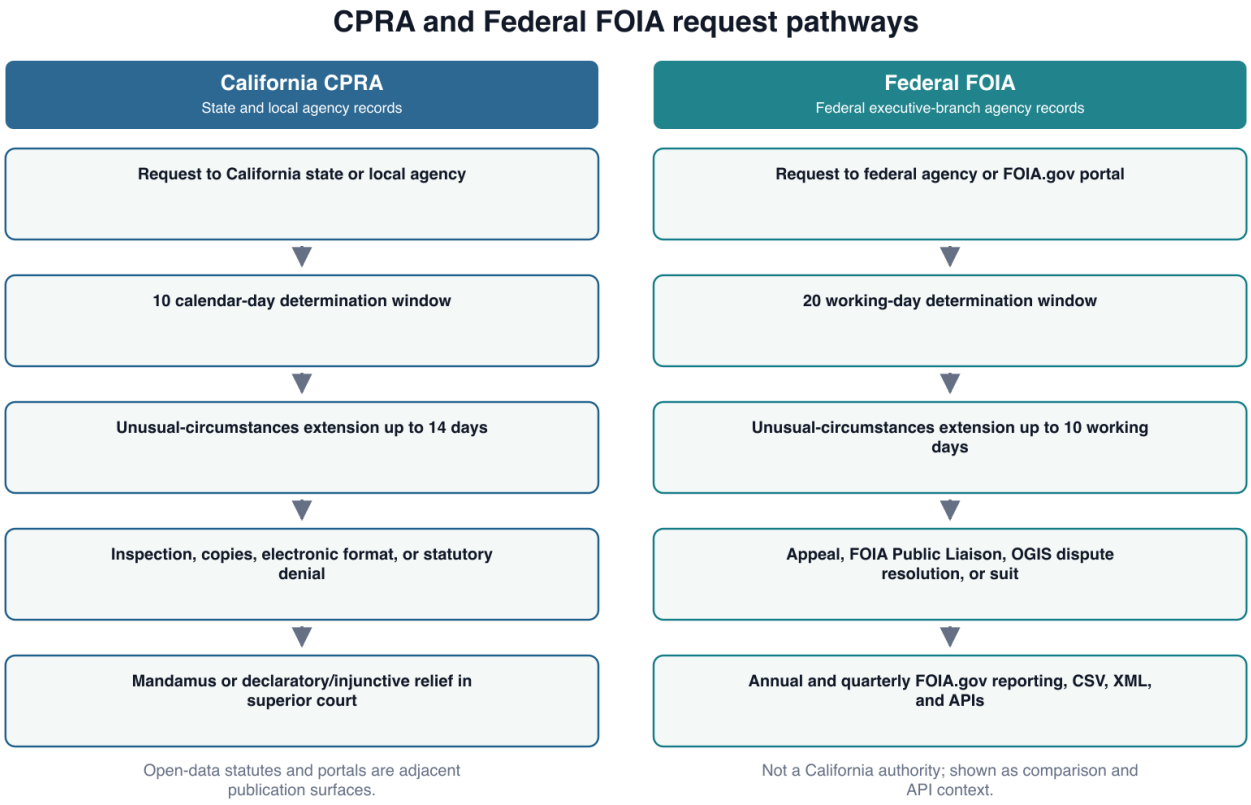


Figure 4: Side-by-side comparison of the California CPRA and Federal FOIA request pathways. CPRA governs California state and local agency records and uses a 10-calendar-day determination window; Federal FOIA governs federal executive-branch agency records, excludes Congress and the federal courts, and uses a 20-working-day determination window with appeal, liaison, OGIS, and judicial review paths. Provenance: `src/figure_bundle.py`, `src/figure_captions.py`, and FOIA/CPRA sources in `manuscript/references.bib`. Caveat: the Federal FOIA lane is comparative context and does not create California agency duties.

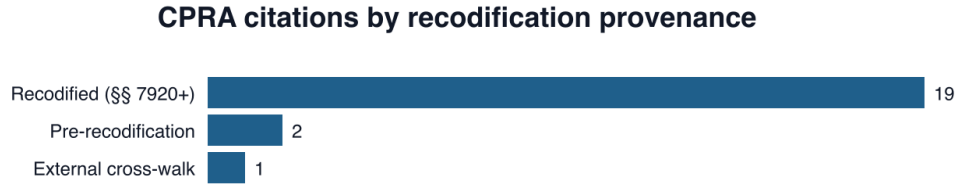


Figure 5: Every registered statute citation classified by recodification provenance: recodified-current sections, pre-recodification open-data sections retained under former Division 7, and external cross-walk authority. Provenance: `src/provenance.py` and `src/statutes.py`; methodology is documented by the project verification contract. Caveat: this is citation honesty, not an independent legal-concordance opinion.

4 The Portal Ecosystem

4.1 The "portal of portals" model

California's open-data infrastructure operates as a federation. The state runs `data.ca.gov` as a centralized catalog whose entries point into individual agency portals. Technology officials describe the architecture as a *portal of portals* — a central discovery layer that reduces the need to scrape individual agency websites [StateScoop, 2021, California Open Data Portal, 2024a].

This project's registry currently tracks 17 portals across 7 hosting platforms and 10 subject-matter domains (fig. 6). The headline counts:

- **4** portals run on CKAN (`data.ca.gov`, CalHHS, CNRA, the CDT Open Data Lab).
- **2** portals run on ArcGIS Hub (`gis.data.ca.gov`, OEHHA CalEnviroScreen).
- **1** portal runs on Socrata SODA at the local-government layer (DataSF).
- **2** portals are CPRA-request platforms running on NextRequest (LA, San Francisco).

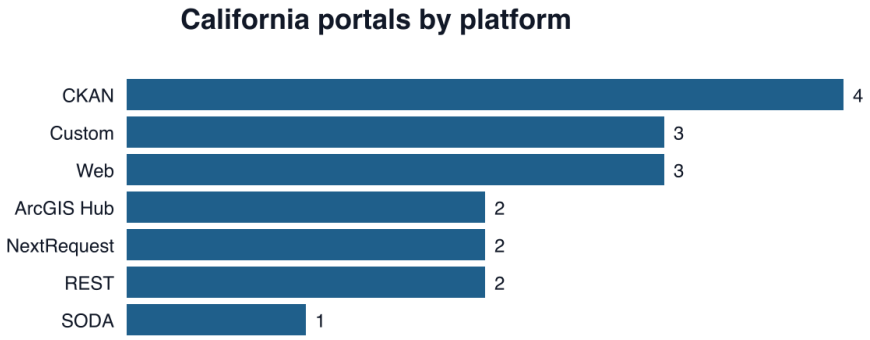


Figure 6: The 17 registered portals grouped across 7 hosting platforms. Provenance: `src/portals.py` via `src.metrics.compute()`. Caveat: platform labels describe the observed publication surface in the registry, and mixed or custom portals are intentionally normalized for comparison.

4.2 Domain distribution

The same 17 portals partition across the data domains they serve (fig. 7):

- Health: **1**
- Water: **2**
- Environment: **2**
- Justice: **1**
- Finance: **1**
- Business: **1**
- CPRA requests: **2**

The interaction between domain and hosting platform is shown in fig. 8.

4.3 Full portal registry

Portal	URL	Platform	Operator	Domain
California Open Data Portal	`https://data.ca.gov`	CKAN	California Department of Technology / GovOps	general
CalHHS Open Data Portal	`https://data.chhs.ca.gov`	CKAN	California Health and Human Services Agency	health
CNRA Open Data Platform	`https://data.cnra.ca.gov`	CKAN	California Natural Resources Agency	environment

Portal	URL	Platform	Operator	Domain
California State Geoportal	https://gis.data.ca.gov	ArcGIS Hub	GovOps / California Department of Technology	general
OEHHA CalEnviroScreen	https://oehha.ca.gov/calenviroscreen	ArcGIS Hub	Office of Environmental Health Hazard Assessment	environment
OpenJustice Data Portal	https://openjustice.doj.ca.gov/data	Custom	California Department of Justice	justice
Open FI$Cal	https://open.fiscal.ca.gov	Custom	California Department of Finance / FI$Cal	finance
CIMIS Web API	https://et.water.ca.gov/api/data	REST	California Department of Water Resources	water
California Data Exchange Center	https://cdec.water.ca.gov	Web	California Department of Water Resources	water
Secretary of State BizFile Online	https://bizfileonline.sos.ca.gov	Web	California Secretary of State	business
DataSF	https://data.sfgov.org	SODA	City and County of San Francisco	general
California Open Data Lab	https://lab.data.ca.gov	CKAN	California Department of Technology Open Data Lab	general
Los Angeles Public Records Portal	https://recordsrequest.lacity.org	NextRequest	City of Los Angeles	requests
San Francisco Public Records Portal	https://sanfrancisco.nextrequest.com	NextRequest	City and County of San Francisco	requests
California Legislative Information	https://leginfo.legislature.ca.gov	Web	Office of Legislative Counsel	legislative
LegiScan California Bulk Legislative Data	https://legiscan.com/CA	REST	LegiScan (third-party aggregator of CA legislative data)	legislative
CAL-ACCESS Raw Data (Campaign Finance & Lobbying)	https://www.sos.ca.gov/campaign-lobbying/cal-access-resources/raw-data-campaign-finance-and-lobbying-activity	Custom	California Secretary of State	elections

The registry is the single source of truth for portal metadata in this project. Every cross-reference in subsequent sections resolves against an entry above.

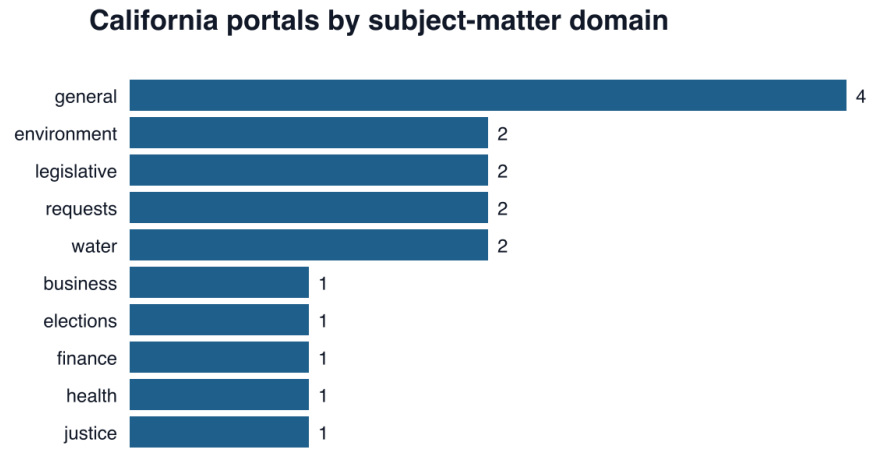


Figure 7: The same 17 registered portals partitioned across 10 subject-matter domains. Provenance: `src/portals.py` domain tags. Caveat: domain is a reader-facing classification; multi-purpose portals are assigned to their dominant role in this registry.

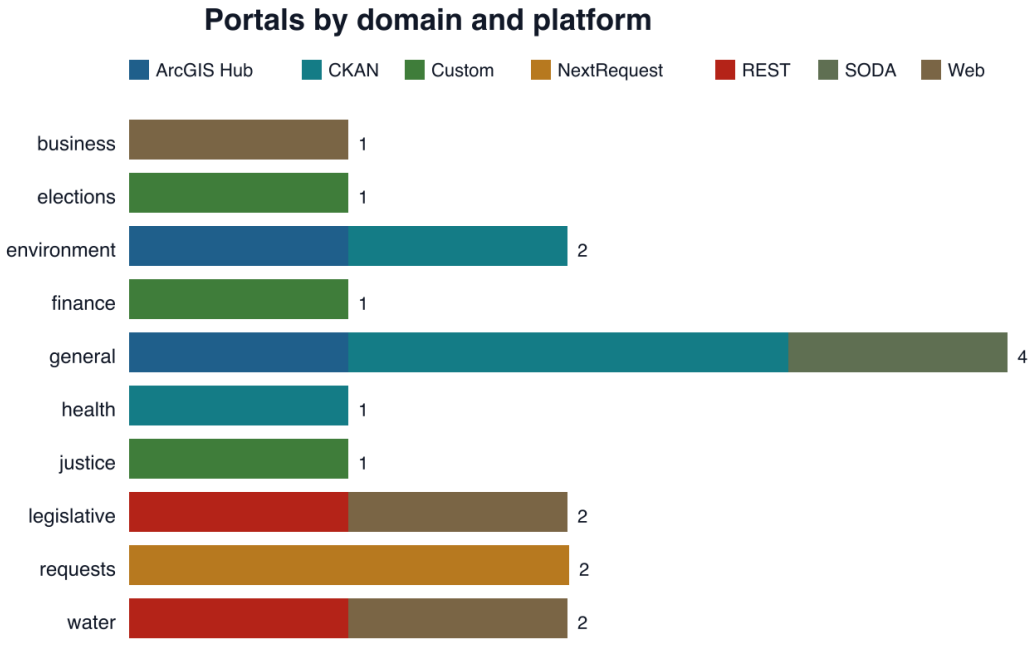


Figure 8: Cross-cut of registered portals by subject-matter domain and hosting platform. Provenance: `src.metrics.portals_domain_x_platform_matrix()`. Caveat: the chart compares registry classifications and should not be read as usage volume, dataset volume, or statutory importance.

5 API Patterns and Reference Clients

This section catalogs the distinct API surfaces in active production use across the California open-data ecosystem and the Python clients in `src/clients/` that implement each one. The registry spans 7 API surfaces (fig. 9); 6 of them expose a programmatic API and each has a client in `src/clients/` that uses only the Python standard library, so the project carries no third-party HTTP dependency. The remaining surface is download-only and needs no client.

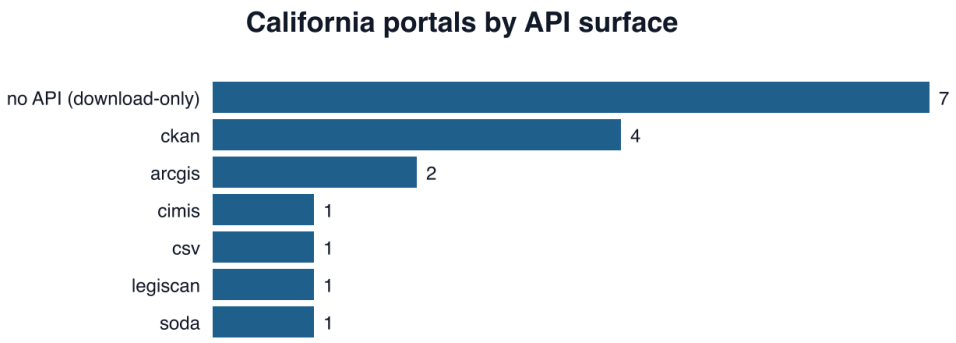


Figure 9: Registered portals grouped by API surface. Of the 7 API surfaces shown, 6 expose a programmatic API with a standard-library client in `src/clients/`; the remaining surface is download-only. Provenance: `src/portals.py` API-kind tags and `src/clients/`. Caveat: this is an endpoint-shape inventory, not an uptime or completeness guarantee.

Federal FOIA.gov is not part of the California portal registry, but it is a useful benchmark for mature public-records data plumbing. FOIA.gov exposes annual agency FOIA statistics and quarterly request/backlog statistics as charts and CSV downloads, while its developer documentation describes an API-keyed public API, an agency-component endpoint, an annual-report XML schema, and a draft RESTful HTTPS specification for agencies that receive requests from the portal through case-management integrations [FOIA.gov, U.S. Department of Justice, 2026d,c,b]. The comparison matters here because California's open-data portals are mostly dataset catalogs and bulk-download/API endpoints, whereas FOIA.gov combines request intake, administrative reporting, and machine-readable federal FOIA performance data. This project documents that federal pattern for comparison only; no FOIA.gov API-key client is added to the California reference package.

5.1 CKAN Action API

The CKAN Action API is the most frequent API pattern in this project's state-portal registry: it powers `data.ca.gov`, `data.cnra.ca.gov`, and `data.chhs.ca.gov` (the 4 CKAN portals enumerated in sec. 4) [CKAN, 2024b, California Natural Resources Agency, 2024a, California Open Data Portal, 2024b,c, CKAN, 2024a, California Natural Resources Agency, 2024d]. The canonical contract for `package_list`, `package_show`, `package_search`, and `datastore_search` — and for the `success`/`result` envelope the client wraps — is the official CKAN Action API reference [CKAN, 2024b].

Base pattern:

`https://<portal-domain>/api/3/action/<action_function>`

The client `src.clients.ckan.CkanClient` exposes:

- `package_list()` — catalog of dataset slugs.
- `package_show(id)` — full metadata for one dataset.
- `package_search(q, rows)` — full-text search.
- `datastore_search(resource_id, limit, q)` — tabular row queries.

Every method wraps the CKAN action envelope (`success` flag plus `result`) and raises `ApiError` on `success=False` or shape mismatches.

5.2 Socrata Open Data API (SODA)

San Francisco's `data.sfgov.org`, and many other California county and city portals, run on Socrata (now Tyler Technologies) with the SODA query language [DataSF, 2024a, Socrata / Tyler Technologies, 2024a, DataSF, 2024b].

Endpoint pattern: `/resource/<xxxx-xxxx>.json` with `$select`, `$where`, `$order`, `$group`, `$limit`, `$offset`, and `$q` parameters.

The client `src.clients.soda.SodaClient` validates the Socrata 4×4 dataset identifier and the `SoqlQuery` builder enforces positive `limit` and non-negative `offset`. Optional `X-App-Token` header carries the Socrata application token when provided [Socrata, 2024, Socrata / Tyler Technologies, 2024b]. The client targets the legacy SODA 2.x `/resource/<4x4>.json` pattern documented in the SoQL reference; the forthcoming SODA 3 revision moves queries to an `/api/v3/.../query.json` surface and tightens token/authentication requirements, so the endpoint shape here is expected to migrate [Socrata / Tyler Technologies, 2024b].

5.3 ArcGIS GeoServices REST

The California State Geoportal `gis.data.ca.gov` aggregates 25+ state agencies' geospatial data on ArcGIS Online Hub [Esri, 2020]. Individual layers — including the OEHHA CalEnviroScreen 4.0 results layer and the California Protected Areas Database (CPAD) — are exposed as FeatureServer endpoints with a SQL-style `where` clause and a controlled vocabulary of response formats (`json`, `geojson`, `pbf`) [Esri Developer, 2024, Esri, 2024]. The normative parameter set for the `query` operation — `where`, `f`, `resultOffset`, and `maxRecordCount` — is the Esri ArcGIS REST API *Query (Feature Service/Layer)* reference [Esri, 2024].

The client `src.clients.arcgis.ArcGisClient` implements the `query` operation with parameter validation on layer index, record count, offset, and format.

5.4 CIMIS REST

The California Irrigation Management Information System provides agricultural and meteorological data via `https://et.water.ca.gov/api/data` [California Department of Water Resources, 2024b,c]. Access requires a free application key registered at `cimis.water.ca.gov`.

The client `src.clients.cimis.CimisClient` validates the unit-of-measure choice (`M` or `E`) and the data-item vocabulary against the documented CIMIS list. Targets may be station IDs, zip codes, lat/long pairs, or street addresses [California Department of Water Resources, 2024a].

5.5 DOJ OpenJustice CSV datasets

The DOJ does not expose a query API: instead it publishes raw CSV bulk downloads under `openjustice.doj.ca.gov/data` [California Department of Justice, 2024]. The 8-dataset taxonomy is encoded in `src.clients.openjustice` along with a streaming CSV loader that validates the header against the expected schema column list.

Slug	Title	Columns
`arrests`	Arrests by demographics, county, and offense class	10
`arrest_dispositions`	Arrest dispositions by demographic and county	7
`complaints`	Citizen complaints against peace officers	4
`crimes_clearances`	Reported crimes and clearances	6
`ripa_stop`	RIPA Act stop data (officer-perceived demographics)	10
`lea_cjp`	Law Enforcement and Criminal Justice Personnel	4
`leoka`	Law Enforcement Officers Killed or Assaulted	4
`deaths_in_custody`	Deaths in custody (including arrest-related)	6

5.6 LegiScan California legislative data

LegiScan (`api.legiscan.com`) provides structured California legislative data — bill text, roll calls, amendments, supplemental documents — under a CC BY 4.0 bulk-data license [LegiScan, 2024b,a]. An open-source alternative, **Open States v3**, exposes a unified national schema for California bills, legislators, committees, votes, and events [Open States,

2024]. A community-maintained third-party REST shim for the California codes themselves is also available [Pearson, Tyler, 2024].

The client `src.clients.legiscan.LegiScanClient` validates the operation name against a closed enumeration, surfaces `status: ERROR` responses as `ApiError`, and provides typed wrappers for `getMasterList`, `getBill`, and `getSessionList`.

5.7 Schema field counts

Across the four metadata-schema validators in `src/schemas/`, the field counts are:

- DCAT: **6** required fields, **9** optional.
- CKAN: **7** required dataset fields and **4** required per-resource fields.
- RIPA: **15** required fields, **5** optional.
- CHHS Dublin Core: **11** required fields.

6 Package Architecture and Reproducibility

The figures in the preceding sections visualize the California public-records *domain*. This section visualizes the *package itself* — what it consumes, the methods it runs, and what it produces — so a reader can audit not just the data but the machinery that generates it. The structure is a strict left-to-right data-flow from inputs through pure methods to outputs (fig. 10).

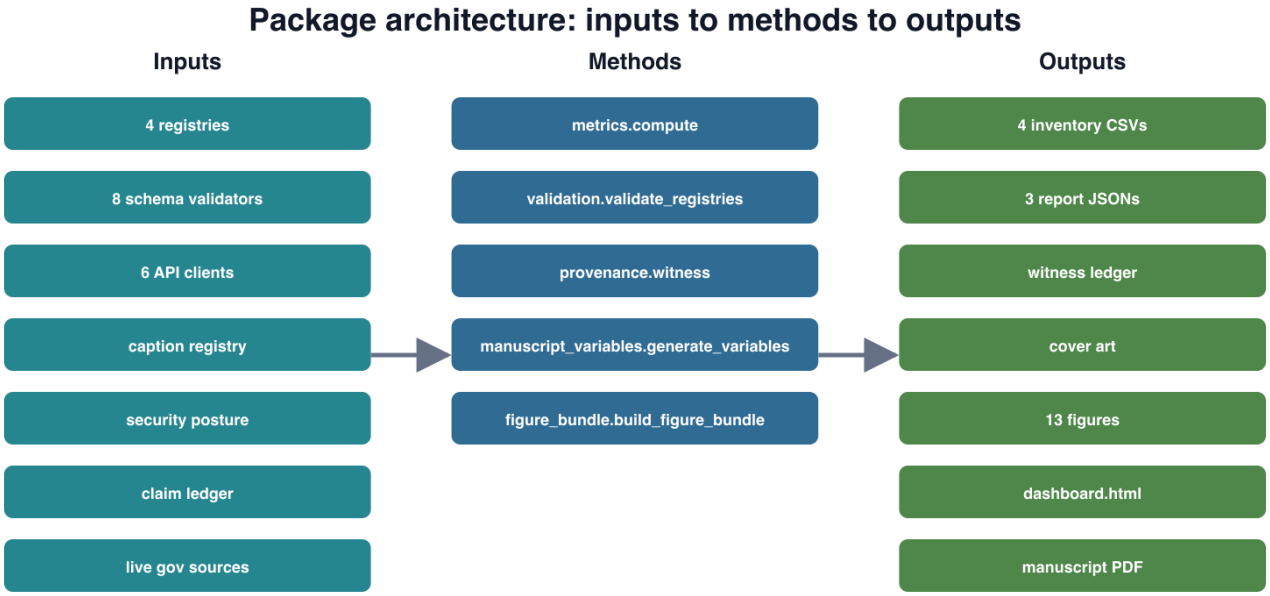


Figure 10: Package data flow from source-owned inputs through pure generator methods to reproducible outputs. Inputs include 4 registries, 8 schema validators, 6 standard-library HTTP clients, 13 caption records, the claim ledger, and live government sources; outputs include inventories, JSON reports, figures, dashboard HTML, and the rendered manuscript. Provenance: `src/package_map.py`. Caveat: the diagram describes the local build pipeline, not publication readiness.

6.1 Inputs

The package consumes 4 source-of-truth registries (statutes, exemptions, portals, and OpenJustice datasets), validates upstream payloads against 8 metadata-schema validators, reaches live endpoints through 6 standard-library HTTP clients, pins every prose statistic that is not registry-derived in the claim ledger, carries 7 defensive security-control records, and re-checks the most volatile source claims against real government pages through 3 live source oracles. fig. 11 counts each input kind.

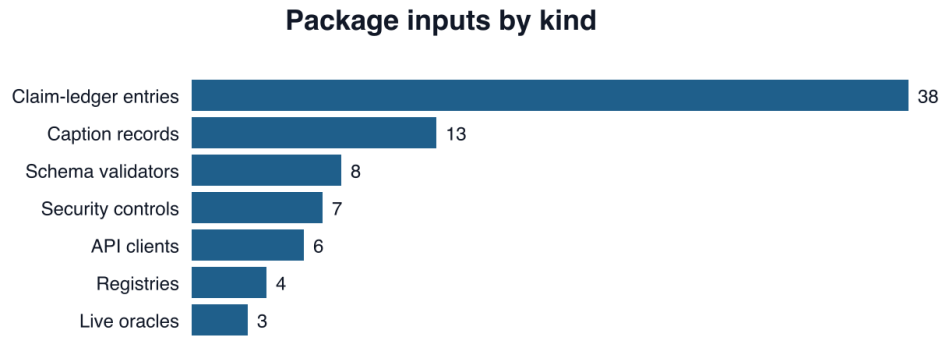


Figure 11: Package inputs by kind: 4 source registries, 8 schema validators, 6 HTTP clients, 13 source-owned caption records, 7 defensive security controls, claim-ledger entries, and 3 live source oracles. Provenance: `src/package_map.input_counts()`. Caveat: claim-ledger and caption counts are build metadata; they are not public-records ecosystem counts.

6.2 Methods

The 5 methods that turn those inputs into artifacts — `metrics.compute`, the validation aggregator, the provenance witness, the manuscript-variable generator, and the figure-bundle renderer — are **pure functions of the registries**: no clock, randomness, or network state feeds a computed value. Re-running any of them yields byte-identical output except a single provenance timestamp, a property enforced by `tests/test_idempotency.py` and described by the project architecture contract.

6.3 Outputs

From those inputs and methods the package emits 4 inventory CSVs, 3 machine-readable report JSONs (ecosystem metrics, validation, and the manuscript-variable set), the witness evidence ledger, and 13 rendered figures — every one of which appears in this manuscript or its companion dashboard. fig. 12 counts each produced artifact kind.

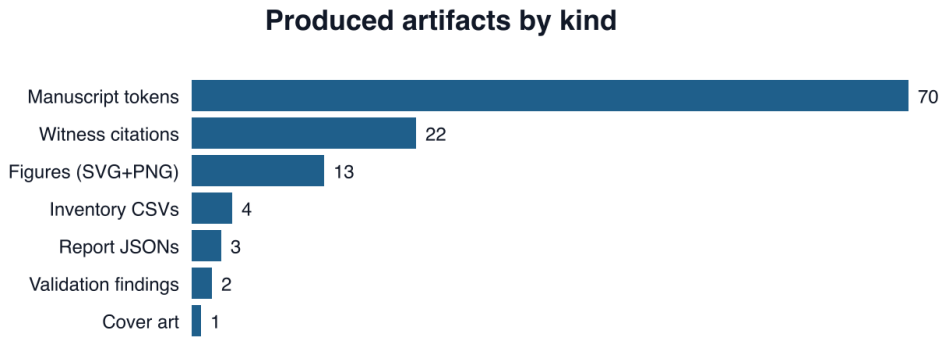


Figure 12: Produced artifacts by kind: 4 inventory CSVs, 3 report JSON files, 13 analytical figure pairs, 1 title-page cover asset, generated manuscript tokens, validation findings, and witness citations. Provenance: `src/package_map.output_counts()`. Caveat: validation findings count all severities, including informational provenance notices.

6.4 Defensive Security Posture

The publication pipeline is also a target surface. A nation-state-capable actor does not need to defeat the CPRA to damage a public-records reference; it can poison source pages, launder citations through plausible prose, compromise a dependency or build step, alter generated artifacts after review, force schema drift that breaks downstream clients, or induce secret leakage through API-keyed integrations. This project already carries local defenses against some of those failures: source-owned registries, claim-ledger quote checks, caption tokens, no third-party HTTP runtime client, deterministic generators, offline and live gates, and explicit handling of access-policy skips versus real source drift. fig. 13 separates that current local posture from target hardening such as signed provenance, transparency-log records, formal vulnerability triage, monitored source drift, and release-path secret controls [National Institute of Standards and Technology, 2020, 2022b,a, 2024, The MITRE Corporation, 2026, SLSA, 2026, Sigstore, 2026a,b, Cybersecurity and Infrastructure Security Agency, 2026].

Because every output is a deterministic function of the version-controlled inputs, a reviewer can regenerate the entire artifact set from a clean checkout and confirm by `git diff` that nothing drifted — the reproducibility guarantee that lets this reference be trusted on first encounter.

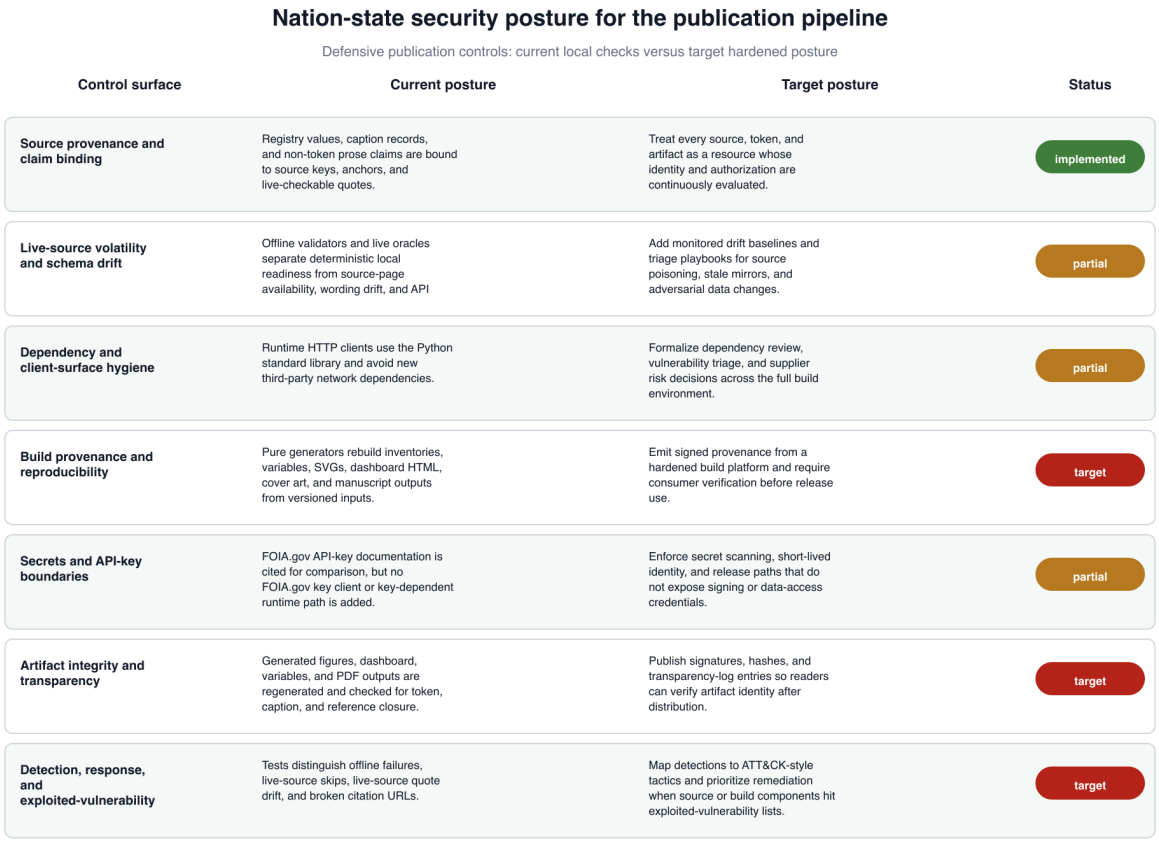


Figure 13: Defensive posture matrix for the publication pipeline, comparing current local controls with a harder target posture for source provenance, live-source volatility, dependency hygiene, build provenance, secret handling, artifact integrity, and detection readiness. Provenance: the source-owned security-posture registry and official NIST, MITRE ATT&CK, SLSA, Sigstore, and CISA sources. Caveat: the figure documents manuscript and build-pipeline controls; it is not a claim of production deployment, signed release enforcement, or external compliance status.

7 Metadata Schemas

Four schema validators live under `src/schemas/`. Each accepts a Python `Mapping` and returns a `ValidationReport` with `ok`, `missing`, and `warnings` fields.

7.1 DCAT (with California extensions)

DCAT (Data Catalog Vocabulary) is the cross-portal interoperability layer that makes California datasets discoverable from federal `data.gov` aggregators [World Wide Web Consortium (W3C), 2024, California Natural Resources Agency, 2024a,c]. The normative vocabulary is the W3C DCAT Recommendation (DCAT-3, 2024) [World Wide Web Consortium (W3C), 2024]; the specific profile California must emit to contribute to `data.gov` is DCAT-US, and the federal mandate that makes `data.gov` a statutory aggregator at all is the OPEN Government Data Act of 2018 (Title II of the Foundations for Evidence-Based Policymaking Act, 44 U.S.C. § 3506 et seq.) [U.S. General Services Administration, 2024, 2018]. California portals extend DCAT with several program-specific fields documented by CNRA and CHHS:

- `Public Access Level` — controlled vocabulary: public, restricted, non-public.
- `Frequency` — Daily, Weekly, Monthly, Quarterly, Annually, Irregular, Continuous.
- `Program Contact Name` / `Program Contact Email`.
- `DCAT Issued Date` / `DCAT Modified Date` — ISO 8601 strings.
- `Spatial Coverage` and `Temporal Coverage`.

The 6-field required core plus 9 optional fields are validated by `src.schemas.dcat.validate`.

7.2 CKAN package shape

CKAN models a dataset as a *package* containing one or more *resources* (file URLs plus their metadata) [California Natural Resources Agency, 2024a]. A valid package supplies 7 required top-level fields and every resource supplies 4 required fields. The validator flags missing fields and emits warnings for non-slug `name` values, organisations without titles, and zero-resource packages.

7.3 RIPA stop-data schema

The Racial and Identity Profiling Act of 2015 (AB 953, Stats. 2015, ch. 466, codified at Penal Code §§ 13012 and 13519.4) requires covered California law-enforcement agencies to submit detailed stop data to the DOJ for covered officer-initiated or call-for-service stops [California State Legislature, 2015a, City of Mill Valley, 2024, Los Angeles County Sheriff's Department, 2024]. The reportable data elements and their controlled vocabularies are fixed by the DOJ's stop-data regulations — definitions at **11 CCR § 999.224** and the data elements to be reported at **§ 999.226** (the series runs §§ 999.224–999.229) — so reporting agencies cannot redefine them locally [California Department of Justice, 2020, College of Marin, 2024].

The schema records officer-*perceived* demographics (race, gender, age, LGBT status, English fluency, disability), procedural posture (stop type, reason, duration, location), actions (orders out of vehicle, handcuffing, searches), the search basis, contraband-found status, and the disposition. Officer metadata (officer ID, years of experience, assignment) is included for accountability.

The validator enforces 15 required fields with controlled-vocabulary warnings on race, gender, stop type, and stop result. 5 optional fields cover the supplementary RIPA elements.

7.4 CHHS Dublin Core

The CHHS Open Data Handbook (`chhsdata.github.io/opendatahandbook`) is the canonical California reference for Dublin Core-based publication standards and is the basis for the statewide handbook at `handbook.data.ca.gov` [California Health and Human Services Agency, 2024d,c, California Department of Technology, 2024, California Health and Human Services Agency, 2024f]. The underlying vocabulary is defined normatively by the DCMI Metadata Terms and standardized as ISO 15836-1; the classic Dublin Core element set has 15 elements, so the 11 required CHHS fields are best read as a *profile* of that set rather than a separate schema [Dublin Core Metadata Initiative, 2020, International Organization for Standardization, 2017].

CHHS datasets must supply the 11 Dublin Core fields. The format field is validated against the CHHS-standard format set (CSV, JSON, XML, XLSX, Shapefile, KML, KMZ, GeoJSON, GeoPackage, PDF, HTML).

8 Domain-Specific Portals

8.1 Health and Human Services

The **CalHHS Open Data Portal** at `data.chhs.ca.gov` (1 of the 1 health portals) hosts hundreds of datasets covering public health, healthcare delivery, Medi-Cal, social services, and epidemiology; its live CKAN `package_search` endpoint returned 481 public datasets on June 21, 2026 [California Health and Human Services Agency, 2024e,b, 2026]. Notable artifacts include the Provider Suspended and Ineligible List, the Enrolled Medi-Cal Fee-for-Service Provider directory, the SUD Recovery Treatment Facilities dataset, the Licensed DUI Provider Directory, and the daily Death Profiles by County [California Health and Human Services Agency, 2024a].

8.2 Environmental Justice

CalEnviroScreen (produced by OEHHA) scores California census tracts for pollution burden and population vulnerability. CalEPA released an updated version in October 2021, and its mapping tool supports results by indicator or by individual census tract [California Environmental Protection Agency, 2021]. OEHHA released the Draft CalEnviroScreen 5.0 update on January 28, 2026; the official draft page says it uses the most recent census geography and data and introduces Diabetes Prevalence and Small Air Toxic Sites as new indicators, while the official comment page records a public-comment window through April 1, 2026 [Office of Environmental Health Hazard Assessment, 2026c,a,b]. Data is exposed as XLSX with a data dictionary, ArcGIS Feature Service REST API, Shapefile, GDB, CSV, GeoJSON, KML, and GeoPackage [UC Riverside Sustainability, 2024].

8.3 Water Resources

CDEC (`cdec.water.ca.gov`), the California Data Exchange Center, hosts real-time and historical hydrologic data drawn from NOAA NWS, USACE, USBR, USGS, CDFW, DWR, SMUD, PG&E, and EBMUD [Drought.gov, 2024]. **CIMIS** at `et.water.ca.gov` (1 of the 2 water portals) provides the REST API surface documented in sec. 5, [California Department of Water Resources, 2024b,c]. **CNRA CPAD** (California Protected Areas Database) covers lands owned in fee and protected for open space by over 1,000 public agencies or non-profit organizations, via multiple ArcGIS REST API endpoints [California Natural Resources Agency, 2024b].

8.4 Criminal Justice

OpenJustice is the 1-portal foothold of the California DOJ in the open-data ecosystem; the White House Police Data Initiative described CA DOJ as the first state agency to participate after launching OpenJustice [The White House (Obama Administration), 2015, GovTech, 2024a,b, San Diego Regional Data Library, 2024]. It publishes the 8 CSV datasets cataloged in `src/clients/openjustice.py`, including the RIPA stop data, arrests, arrest dispositions, citizen complaints, crimes and clearances, LEA/CJP personnel, LEOKA, and deaths in custody.

The Racial and Identity Profiling Advisory Board's 2026 report, released January 30, 2026, analyzed approximately 5.1 million police and pedestrian stops conducted by 533 state and local law-enforcement agencies in 2024 [California Department of Justice, Office of the Attorney General, 2026c]. OAG's AB 953 page also anchors the operating model: the Board analyzes stop and complaint data annually, issues annual reports, and directs users to OpenJustice for interactive stop-data comparisons [California Department of Justice, Office of the Attorney General, 2026a].

Disclosure of peace-officer personnel records is governed by **Penal Code § 832.7**, which compels disclosure in enumerated categories: use of force resulting in death or great bodily injury, discharge of firearm at persons, sustained findings of dishonesty or sexual assault, sustained findings of unlawful arrests or illegal searches, sustained findings of unreasonable or excessive force, failure to intervene, and findings of prejudice or discrimination [California State Legislature, 2022, 2018, 2021b, Civica Law Group, 2023]. The original categories — use of force causing death or great bodily injury, discharge of a firearm at a person, and sustained findings of dishonesty or sexual assault — were created by SB 1421 (operative 2019); SB 16 (operative 2022) added the remainder — sustained unlawful arrests or illegal searches, sustained unreasonable or excessive force, failure to intervene, and findings of prejudice or discrimination — so the list above is the post-SB-16 set. The earlier scaffolding of this project incorrectly placed § 7928.200 as a CPRA companion to § 832.7; § 7928.200 in fact governs liability shields for online-service providers re: posting elected-official information.

8.5 Business Entities

The California Secretary of State maintains **BizFile Online** (`bizfileonline.sos.ca.gov`) providing free access to over 17 million corporate, LLC, and limited-partnership images/records [California Secretary of State, 2024b,a, secretaryofs-

tate.com, 2024]. Programmatic verification is available through the SOS API Developer Portal and third-party REST wrappers [Cobalt Intelligence, 2024a,b].

8.6 Elections

The Secretary of State maintains the statewide voter-registration database. Voter information is available only for statutorily authorized requesters and uses, including election, scholarly, journalistic, political, and governmental purposes via a formal Voter Registration Information File Request; it is not a bulk open-data download, and confidential registration records are excluded even for authorized purchasers [California Secretary of State, 2026, 2024d].

8.7 State Finances

Open FI$Cal (`open.fiscal.ca.gov`) publishes expenditure data for 151 departments (188 business units) representing roughly 79% of state expenditures, sourced from the statewide Financial Information System for California (FI$Cal) [California Department of Finance, 2024, FI$Cal Newsletter, 2024]. A beta API exposes the data dimensions (fiscal year, department, fund, budget reference, object/subobject, vendor, appropriation) to downstream applications [California Open Data Portal, 2024d].

Transparent California (`transparentcalifornia.com`) is a third-party aggregation of CPRA-obtained public-employee salary and pension data. A May 2024 report on its 2022 compensation-data collection stated that it hosted a cumulative total of roughly 42 million records spanning about a decade; that collection wave added 2.7 million employee records obtained from 2,518 agencies [Transparent California, 2024]. The California State Controller's **Government Compensation** site is the official complement [California Policy Center, 2024].

8.8 Courts

California courts have a separate access boundary from executive-branch CPRA practice. Rule of Court 10.500 governs judicial administrative records and expressly leaves adjudicative case-record access to separate law; Rule 2.550 supplies the presumption of openness for court records unless sealing standards are met [Judicial Council of California, 2026, Plumas County Superior Court, 2024, Judicial Council of California, 2024]. Superior-court access is per-court: the Judicial Branch states that each of California's 58 superior courts keeps its own records and that requesters must contact the individual court, while remote electronic access depends on case type and court capability [Judicial Branch of California, 2026b,a]. There is no unified statewide case-record API; access remains per-court (Sacramento County [Sacramento County, 2024], Orange County [Orange County Superior Court, 2024], etc.).

8.9 Local CPRA-request platforms

NextRequest is a widely used CPRA request-management platform in California; this registry tracks local and state deployments rather than asserting a statewide adoption count [Regional Center of the East Bay, 2024]. Major deployments include Los Angeles City ([City of Los Angeles, 2024]), San Francisco ([City and County of San Francisco, 2024]), Mountain View ([City of Mountain View, 2024]), Richmond ([City of Richmond, 2024]), the CA High-Speed Rail Authority ([California High-Speed Rail Authority, 2024]), and Sonoma County ([County of Sonoma, 2024]). Agency-specific portals are run by POST [California Commission on Peace Officer Standards and Training, 2024], the Secretary of State [California Secretary of State, 2024c], FTB [California Franchise Tax Board, 2024], and the Attorney General's office [California Department of Justice, Office of the Attorney General, 2026b].

9 Exemption Taxonomy

The post-AB 473 recodified CPRA organises exemptions into **7** structural clusters, of which **1** are governed by the public-interest balancing test of Gov. Code § 7922.000 and **6** operate as categorical bars on disclosure [Civica Law Group, 2023, City of Eureka, 2024, Justia, 2005, 2010].

Cluster	Code Range	Protects	Balancing?
General balancing test	Gov. Code § 7922.000	agency-asserted public interest in nondisclosure	Yes
Personnel, medical, similar files	Gov. Code § 7927.700	employee privacy	No
Law-enforcement complaints and investigations	Gov. Code § 7923.600	active investigative interests, intelligence, and security procedures	No
Preliminary drafts and interagency memoranda	Gov. Code § 7927.500	deliberative-process integrity	No
Pending litigation and tort claims	Gov. Code § 7927.200	litigation strategy until adjudication or settlement	No
Voter registration information	Gov. Code § 7924.000	voter privacy and identity-document confidentiality	No
Peace officer personnel records	Penal Code § 832.7	officer privacy outside enumerated disclosure categories	No

The "catch-all" balancing test of Gov. Code § 7922.000 bears its own weight: the agency must demonstrate the public interest in nondisclosure *clearly outweighs* the public interest in disclosure [First Amendment Coalition, 2024, Justia, 2025]. The public's interest in monitoring the conduct of government supplies the disclosure side of that scale [Supreme Court of California, 1986]. The burden is high; courts have repeatedly held that vague invocations of "deliberative process" or "privacy" cannot satisfy it without a concrete record-by-record showing — the deliberative-process privilege itself is read through the same balancing test rather than as a categorical bar [Supreme Court of California, 1991].

The Penal Code § 832.7 categorical-disclosure list for peace-officer records, shown as its own cluster in the taxonomy above, is a major boundary between confidentiality and affirmative disclosure; the enumerated categories were created by SB 1421 (operative 2019) and expanded by SB 16 (operative 2022) [California State Legislature, 2022, 2018, 2021b, Civica Law Group, 2023]. Records of use of force resulting in death or great bodily injury, discharge of firearm at a person, sustained findings of dishonesty or sexual assault, sustained findings of unlawful arrests or illegal searches, sustained findings of unreasonable or excessive force, failure to intervene, and findings of prejudice or discrimination *must* be disclosed; other peace-officer personnel records remain categorically exempt. The earlier scaffolding of this project incorrectly placed Gov. Code § 7928.200 as the CPRA companion to § 832.7; § 7928.200 actually governs liability shields for online-service providers re: posting elected-official information, and Penal Code § 832.7 stands on its own as the operative peace-officer-disclosure mandate.

9.1 Cost recovery and enforcement

In *National Lawyers Guild v. City of Hayward* (2020) 9 Cal.5th 488, the California Supreme Court held that the statutory "data extraction" an agency may bill for does *not* include the cost of redacting exempt material from electronic records; agencies bear their own search-staff and redaction time and may recover only the direct duplication cost [Supreme Court of California, 2020, Dannis Woliver Kelley, 2022]. Where genuine data *compilation, extraction, or programming* is necessary to produce responsive records from a database in a new form, those extraction costs remain recoverable.

Prevailing CPRA requesters are entitled to a mandatory award of court costs and reasonable attorney's fees under Gov. Code § 7923.115; enforcement is by writ petition to the superior court under Gov. Code § 7923.000, and an agency that disobeys a disclosure order may be held in contempt. The CPRA itself imposes no flat per-violation civil penalty; the per-violation civil-penalty figures often attributed to "CPRA" online belong to the separately abbreviated California *Privacy Rights* Act, not the Public Records Act.

9.2 Statutory enterprise-system disclosure

SB 272 (Stats. 2015, ch. 795, codified at Gov. Code § 6270.5) operates as a *positive* obligation rather than an exemption. Each local agency (except local education agencies) must publish a catalog of enterprise systems serving as original data sources, with current vendor, product, system purpose, data categories collected, custodial department, and collection frequency [California State Legislature, 2015b, City of Downey, 2024, Tulare County Employees' Retirement Association, 2024]. The catalog is the metadata anchor against which CPRA requests for the underlying records can be drafted.

10 Conclusion

10.1 Top-line verdict

CERTIFY-WITH-RESIDUALS. The registries, clients, schemas, and closure tests in `src/` and `tests/` are validated by an offline no-mocks suite against a real local HTTP server, plus optional live checks against California open-data endpoints (`data.ca.gov`, `data.chhs.ca.gov`, `data.cnra.ca.gov`, OEHHA ArcGIS). The CI-enforced `src/` coverage floor applies across 22 statute entries, 17 portal entries, 7 exemption clusters, and 8 OpenJustice datasets. The registry's statute citations are source-verified with documented residuals: original authoring used `leginfo.legislature.ca.gov`, and a later cross-vendor audit re-confirmed selected citations against Justia and FindLaw where leginfo was network-blocked; citations that could not be independently verified were removed rather than carried as conjectures. The verification methodology preserves recodification-crosswalk confidence labels and residuals instead of hiding them. **Residuals:** four CPRA sections cited in the upstream research document (Gov. Code §§ 7922.650, 7923.200, 7927.600 as "library patron records", 7928.200 as "peace officer records") were either misattributed or unverifiable against leginfo's JavaScript-rendered code-section pages and are deliberately omitted; this is a coverage gap, not a fabrication. The peace-officer-disclosure mandate is pinned to **Penal Code § 832.7** without a Gov. Code companion (against the source document's claim).

The same bounded verdict applies to security. The project now documents a defensive posture against source poisoning, citation laundering, build and dependency compromise, artifact tampering, live-source volatility, and secret leakage, but it does not claim continuous monitoring, signed releases, transparency-log publication, hardened-build provenance, or deployed zero-trust infrastructure. Those remain target controls rather than present assurances.

California's public-records ecosystem is technically and legally detailed. The CPRA's 2023 recodification (AB 473) improved statutory legibility while preserving five decades of disclosure rights [Liebert Cassidy Whitmore, 2022, Lozano Smith, 2023]. The 2019 Open Data Policy (TL 19-01) and associated State Administrative Manual sections provide an administrative mandate for proactive publication [California Department of Technology, 2019, California Department of General Services, 2019].

The federated architecture — anchored by `data.ca.gov`, supplemented by the 4 CKAN agency portals, the 2 ArcGIS Hub geospatial portals, the SODA local layer, the CIMIS REST endpoint, the OpenJustice CSV bundles, and the LegiScan bulk-data API — creates a rich API landscape supporting programmatic access at every tier. Metadata standards based on Dublin Core and DCAT ensure cross-portal interoperability [California Health and Human Services Agency, 2024c].

This reference makes those structural facts machine-readable. The registries under `src/` are the system of record, the validators under `src/schemas/` enforce schema conformance, the clients under `src/clients/` exercise the live API surfaces using only the Python standard library, and the manuscript token generator in `src/manuscript_variables.py` binds registry-derived counts in the prose to those registries. The CI gates (`tests/`, >=90% coverage on `src/`, the manuscript-token closure test) are designed to fail when a future contributor updates a registry without updating the prose — or vice versa.

For researchers operating in Active Inference, entomology, cognitive security, or any empirical domain touching California government behavior, this infrastructure provides direct, durable, machine-readable access to criminal justice, environmental, health, legislative, financial, water, and geospatial data — governed by a statutory disclosure regime with enforceable judicial remedies.

10.2 Provenance

- Configuration hash: `ea35b6ca65723acf`
- Generated: `2026-06-22T01:15:03Z`
- Python: `3.12.13` on `Darwin arm64`

11 Cognitive-Security Implications

A public-records ecosystem is also an *information ecosystem*. The same infrastructure that makes the state's data machine-readable also exposes it to cognitive-security pressures — narrative capture, data weaponization, citation laundering, and credibility collapse. This section briefly maps those pressures onto the architectural choices this reference makes.

11.1 Citation laundering and the registry-first model

A pernicious failure mode in public-records reference work is *citation laundering*: a confident-sounding prose claim transmits a section number to a reader who never checks the operative statute. This project rejected one scaffolded example of that failure mode: Gov. Code § 7928.200 was initially treated as a peace-officer personnel-records provision, but the operative text governs liability shields for online service providers that post elected-official information. The peace-officer disclosure mandate is therefore pinned to Penal Code § 832.7 rather than carried as a Government Code companion claim.

The registry-first model is one structural defense: section numbers are Python data structures with documented source-verification residuals (original authoring against leginfo; later cross-vendor re-checks against Justia/FindLaw where leginfo was unavailable) and live keyword checks in `tests/test_live_statutes.py` when leginfo is reachable. Every prose token in the manuscript resolves through `src.manuscript_variables.generate_variables` to registry data, and a closure test (`tests/test_manuscript_variables.py`) fails CI if the prose references a token the generator does not declare.

11.2 Disclosure regimes as information-ecosystem infrastructure

The CPRA disclosure regime is not just a transparency mechanism — it is *cognitive-security infrastructure*. A robust public-records workflow:

1. Surfaces primary records that competing narratives can be tested against.
2. Constrains agency claim-making by enabling external verification.
3. Reduces the asymmetric information advantage that allows narrative capture of regulatory or political processes.
4. Lets researchers, journalists, and civic technologists audit government behaviour without relying on intermediated framings.

The 7-cluster exemption taxonomy is the adversarial surface: each cluster is a structural locus where an agency may assert withholding authority. The public-interest balancing test of Gov. Code § 7922.000 is especially sensitive to overbroad framing because it requires a concrete, record-specific showing that the public interest in nondisclosure clearly outweighs the public interest in disclosure. Vague invocations of "deliberative process" or "privacy" should therefore be treated as claims to test, not as self-validating reasons — a discipline the *Times Mirror* balancing authority and the *CBS v. Block* statement of the public-monitoring interest both support [Supreme Court of California, 1991, 1986].

11.3 Open data as an attack surface

When agencies publish machine-readable open data via the 4 CKAN portals or the 2 ArcGIS Hub portals enumerated in sec. 4, they expose four cognitive-security surfaces:

1. **Schema drift** — silent changes to field meanings can break downstream civic-tech tooling. The schema validators in `src/schemas/` are the project's defense against this drift.
2. **Selective publication** — what an agency publishes is itself a choice; what it withholds is the harder signal. The exemption taxonomy in `src/exemptions.py` documents the structural categories under which withholding can occur.
3. **Update cadence opacity** — the DCAT `Frequency` field documents how often the dataset is supposed to refresh; observed cadence should be cross-checked against documented cadence.
4. **Cross-portal incongruity** — when the same fact appears in multiple agency portals with different values, the divergence is itself the finding.

11.4 Nation-state and supply-chain posture

For a high-capability adversary, the publication pipeline around a civic-data reference is part of the target. The relevant threat is not only false content inside the manuscript; it is also source poisoning, citation laundering, build step compromise, stale mirrors, dependency confusion, malicious package or tooling updates, credential exposure, and artifact tampering after a reviewer has trusted a local render. The defensive reading of NIST Zero Trust is that no source page, local artifact, runtime client, or build step should receive implicit trust merely because it sits inside a familiar boundary; NIST SSDF and C-SCRM make the same point for software development and supply-chain acquisition, while CSF 2.0 frames the work

as governance, identification, protection, detection, response, and recovery rather than a one-time checklist [National Institute of Standards and Technology, 2020, 2022b,a, 2024].

This project implements the documentary subset of that posture. It binds numbers to registries, binds non-token claims to source quotes, separates offline gates from live-source volatility, and keeps API clients on the Python standard library. It does not yet publish signed build provenance, public transparency-log entries, a software bill of materials, continuous drift monitoring, or a formal incident-response program. SLSA and Sigstore/Rekor therefore appear here as target architecture for provenance and artifact identity, not as a statement that these paper artifacts are already signed or verified through a hardened release channel [SLSA, 2026, Sigstore, 2026a,b].

MITRE ATT&CK is useful as a vocabulary for the adversary side of this map: credential access, supply-chain compromise, defense evasion, exfiltration, and impact are all plausible around a publication pipeline even when the paper itself is static. CISA's Known Exploited Vulnerabilities catalog is the operational companion: it gives maintainers a way to prioritize remediation when a build tool, platform dependency, or runtime component enters known exploitation. The security-posture figure in sec. 6 uses those frameworks only to bound defensive review; it should not be read as a claim of production deployment or release assurance [The MITRE Corporation, 2026, Cybersecurity and Infrastructure Security Agency, 2026].

11.5 The 8 OpenJustice datasets

The DOJ OpenJustice initiative is a case study in cognitive-security infrastructure: it puts criminal-justice statistics into the public information commons in a form that supports third-party audit. The RIPA stop-data schema enumerated in `src/schemas/ripa.py` (with 15 required fields fixed by the DOJ stop-data regulations — definitions at 11 CCR § 999.224, data elements at § 999.226, under the authority of AB 953) is particularly load-bearing: it constrains the fields that covered California law-enforcement agencies report for covered stops, so reasoning about stop patterns is less vulnerable to local definitional drift.

11.6 The peace-officer disclosure regime

Penal Code § 832.7 — built out by SB 1421 (2019) and SB 16 (2022) — is a major affirmative-disclosure carve-out in California public-records law [California State Legislature, 2022, 2018, 2021b]. Its enumerated categories — use of force causing death or great bodily injury, sustained dishonesty findings, sustained sexual-assault findings, unlawful arrests, illegal searches, unreasonable or excessive force, failure to intervene, and prejudice or discrimination — constrain the narrative space around law-enforcement accountability by making specified underlying records disclosable despite the general confidentiality of peace-officer personnel records.

11.7 Boundary

This section is a threat-modeling lens over the registry, not an independent empirical study of information operations. Its claims are therefore limited to the project's checked statutory, portal, schema, and source-ledger surfaces.

12 References

Bibliography lives in manuscript/references.bib and is resolved by Pandoc at PDF render time via --natbib / --citeproc. Every [@bibtex-key] citation in the preceding prose binds to a @misc / @article entry in the bib file, and the closure test at tests/test_bibliography.py fails CI if the prose cites an undeclared key or if the bib declares a key that the prose never cites.

References

Best Best & Krieger. California public records act new legislation, 2024. URL https://bbklaw.com/resources/california-public-records-act-new-legislation.

California Commission on Peace Officer Standards and Training. California public records act faqs, 2024. URL https://post.ca.gov/California-Public-Records-Act-FAQs.

California Correctional Health Care Services. California public records act, 2026. URL https://cchcs.ca.gov/pra/.

California Department of Finance. State of california expenditures — open fiscal, 2024. URL https://open.fiscal.ca.gov.

California Department of General Services. State administrative manual section 5160: Open data policy introduction, 2019. URL https://www.dgs.ca.gov/Resources/SAM/TOC/5100/5160.

California Department of Justice. California code of regulations, title 11, section 999.224 et seq. (ab 953 stop data regulations), 2020. URL https://oag.ca.gov/ab953/regulations.

California Department of Justice. Data portal — california department of justice openjustice, 2024. URL https://openjustice.doj.ca.gov/data.

California Department of Justice, Office of the Attorney General. Ab 953: The racial and identity profiling act of 2015, 2026a. URL https://oag.ca.gov/ab953.

California Department of Justice, Office of the Attorney General. Public records, 2026b. URL https://oag.ca.gov/consumers/general/pra.

California Department of Justice, Office of the Attorney General. Ripa board reports, 2026c. URL https://oag.ca.gov/ab953/board/reports.

California Department of Technology. Technology letter 19-01: Open data, 2019. URL https://cdt.ca.gov/wp-content/uploads/2019/03/TL-19-01.pdf.

California Department of Technology. Open data handbook — caweb, 2024. URL https://handbook.data.ca.gov.

California Department of Water Resources. Cimis weather station and spatial cimis data — web api, 2024a. URL https://data.ca.gov/dataset/cimis-weather-station-spatial-cimis-data-web-api.

California Department of Water Resources. Cimis — california irrigation management information system, 2024b. URL https://www.cimis.water.ca.gov.

California Department of Water Resources. Cimis web api — rest services, 2024c. URL https://et.water.ca.gov/rest/index.

California Environmental Protection Agency. Press release: Calepa updates groundbreaking environmental justice tool, 2021. URL https://calepa.ca.gov/2021/10/13/press-release-calepa-updates-groundbreaking-environmental-justice-tool/.

California Franchise Tax Board. California public records act — ftb, 2024. URL https://www.ftb.ca.gov/your-rights/california-public-records-act.html.

California Health and Human Services Agency. Calhhs dataset catalog, 2024a. URL https://data.chhs.ca.gov/dataset/dataset-catalog.

California Health and Human Services Agency. Chhs datasets, 2024b. URL https://data.chhs.ca.gov/dataset.

California Health and Human Services Agency. Open data handbook — guidelines, 2024c. URL https://chhsdata.github.io/opendatahandbook/guidelines/.

California Health and Human Services Agency. Open data handbook — california health and human services agency, 2024d. URL https://chhsdata.github.io/opendatahandbook/.

California Health and Human Services Agency. California health and human services open data portal: Welcome, 2024e. URL https://data.chhs.ca.gov.

California Health and Human Services Agency. Open data handbook — use, 2024f. URL https://chhsdata.github.io/opendatahandbook/use/.

California Health and Human Services Agency. Calhhs open data portal ckan package search api, 2026. URL https://data.chhs.ca.gov/api/3/action/package_search?rows=0.

California High-Speed Rail Authority. Faqs for requests — public records act portal, 2024. URL https://hsr-ca.nextrequest.com/faqs.

California Law Revision Commission. Disposition table for government code division 10, access to public records, 2019. URL https://clrc.ca.gov/pub/Printed-Reports/Pub241-G400-Disposition.pdf.

California Natural Resources Agency. Api — california natural resources agency open data, 2024a. URL https://data.cnra.ca.gov/pages/api.

California Natural Resources Agency. California protected areas database, 2024b. URL https://data.cnra.ca.gov/dataset/california-protected-areas-database.

California Natural Resources Agency. Cnra open data platform metadata schema (data.ca.gov), 2024c. URL https://data.ca.gov/dataset/cnra-open-data-platform-metadata-schema.

California Natural Resources Agency. Cnra open data platform metadata schema (data.cnra.ca.gov), 2024d. URL https://data.cnra.ca.gov/dataset/cnra-open-data-platform-metadata-schema.

California Open Data Portal. About california open data, 2024a. URL https://data.ca.gov/about.

California Open Data Portal. Developer tools — california open data, 2024b. URL https://data.ca.gov/pages/developer-tools.

California Open Data Portal. Open data publisher guide contents, 2024c. URL https://data.ca.gov/pages/datacagov-open-data-publisher-guide-contents.

California Open Data Portal. Fi$cal — organizations on california open data, 2024d. URL https://data.ca.gov/organization/about/fiscal.

California Policy Center. Comparing compensation information on transparent california and the state controller's site, 2024. URL https://californiapolicycenter.org/comparing-compensation-information-on-transparent-california-and-state-controllers-site/.

California Secretary of State. California constitution, article i, section 3(b) (proposition 59, the sunshine amendment, adopted november 2, 2004), 2004. URL https://law.justia.com/constitution/california/article-i/section-3/.

California Secretary of State. Bizfile online, 2024a. URL https://bizfileonline.sos.ca.gov.

California Secretary of State. Business entities records request, 2024b. URL https://www.sos.ca.gov/business-programs/business-entities/information-requests.

California Secretary of State. Public records act requests, 2024c. URL https://www.sos.ca.gov/administration/public-records-act-requests.

California Secretary of State. Voter registration information file request, 2024d. URL https://www.sos.ca.gov/elections/voter-registration/voter-registration-information-file-request.

California Secretary of State. Voter registration information file request, 2026. URL https://www.sos.ca.gov/elections/voter-registration/voter-registration-information-file-request.

California State Legislature. Assembly bill 953 (stats. 2015, ch. 466): Racial and identity profiling act of 2015 (codified at penal code sections 13012 and 13519.4), 2015a. URL https://calmatters.digitaldemocracy.org/bills/ca_201520160ab953.

California State Legislature. Senate bill 272 (stats. 2015, ch. 795): Local agency enterprise systems catalog (codified at gov. code section 6270.5), 2015b. URL https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB272.

California State Legislature. Senate bill 1421 (stats. 2018, ch. 988): Peace officers, release of records (amending penal code section 832.7); operative january 1, 2019, 2018. URL https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1421.

California State Legislature. California government code section 6253.10 (open data format standard), 2021a. URL https://law.justia.com/codes/california/2021/code-gov/title-1/division-7/chapter-3-5/article-1/section-6253-10/.

California State Legislature. Senate bill 16 (stats. 2021, ch. 402): Peace officers, release of records (amending penal code section 832.7); operative january 1, 2022, 2021b. URL https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB16.

California State Legislature. California penal code section 832.7 (peace-officer personnel records; categorical disclosure), 2022. URL https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=832.7.

California State Legislature. California government code section 7922.570 (electronic-format production mandate; recodified successor to former section 6253.9), 2023. URL https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=7922.570.

California State Legislature. California government code section 7922.535 (cpra determination deadline and unusual-circumstances extension), 2026. URL https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=7922.535.

California State Library. Making open data work in california's state government, 2018. URL http://castatelibrary.github.io/opendata/07-State-Policies-Open-Data.html.

City and County of San Francisco. Public records request — nextrequest, city of san francisco, 2024. URL https://sanfrancisco.nextrequest.com.

City of Downey. Sb 272 — public agency enterprise systems disclosure, 2024. URL https://www.downeyca.org/our-city/sb-272-public-agency-enterprise-systems-disclosure.

City of Eureka. California public records act faqs, 2024. URL https://www.eurekaca.gov/DocumentCenter/View/6422/Information-on-Government-Code-and-Exemptions-PDF.

City of Los Angeles. Public records request — city of los angeles, 2024. URL https://recordsrequest.lacity.org.

City of Mill Valley. Ripa data — mill valley, 2024. URL https://www.millvalleylibrary.org/906/RIPA-Data.

City of Mountain View. Public records request — nextrequest, city of mountain view, 2024. URL https://cityofmountainviewca.nextrequest.com.

City of Richmond. Public records request — city of richmond, 2024. URL https://www.ci.richmond.ca.us/4331/Public-Records-Request.

Civica Law Group. The recodification of the california public records act (cpra): A quick reference, 2023. URL https://civicalaw.com/2023/06/12/the-recodification-of-the-california-public-records-act-cpra-a-quick-reference-guide-for-code-enforcement-teams.

CKAN. Establishing the metadata fields, 2024a. URL https://groups.google.com/a/ckan.org/g/ckan-dev/c/npYbgM0jqIU.

CKAN. Ckan action api reference, 2024b. URL https://docs.ckan.org/en/latest/api/.

Cobalt Intelligence. California secretary of state api for business entity verification, 2024a. URL https://www.linkedin.com/posts/cobaltintelligence_guide-to-the-california-secretary-of-state-activity-7422292413702025216-oGLS.

Cobalt Intelligence. California secretary of state business search guide 2024, 2024b. URL https://www.youtube.com/watch?v=CjMSA5SQHvM.

College of Marin. Racial identity profiling statistics — campus police, 2024. URL https://police.marin.edu/racial-identity-profiling-statistics.

County of Sonoma. California public records act (cpra) resource, 2024. URL https://sonomacounty.gov/california-public-records-act-(cpra)-resource.

Cybersecurity and Infrastructure Security Agency. Known exploited vulnerabilities catalog, 2026. URL https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

Dannis Woliver Kelley. Public records act's cost recovery provision narrowed by california supreme court, 2022. URL https://www.dwkesq.com/public-records-acts-cost-recovery-provision-narrowed-by-california-supreme-court/.

DataSF. Developers — sf opendata, 2024a. URL https://data.sfgov.org/developers.

DataSF. Datasf tips: Using the open data portal api, 2024b. URL https://datasf.substack.com/p/datasf-tips-using-the-open-data-portal.

Drought.gov. California data exchange center, 2024. URL https://www.drought.gov/data-maps-tools/california-data-exchange-center.

Dublin Core Metadata Initiative. Dcmi metadata terms, 2020. URL https://www.dublincore.org/specifications/dublin-core/dcmi-terms/.

Esri. Arcuser winter 2020: California created a knowledge base with gis, 2020. URL https://www.esri.com/content/dam/esrisites/en-us/newsroom/arcuser/arcuser-winter-2020.pdf.

Esri. Arcgis rest apis — query (feature service/layer), 2024. URL https://developers.arcgis.com/rest/services-reference/enterprise/query-feature-service-layer/.

Esri Developer. Arcgis rest apis documentation, 2024. URL https://developers.arcgis.com/documentation/glossary/arcgis-rest-apis/.

FI$Cal Newsletter. Open fi$cal website continues to improve state's financial transparency, 2024. URL https://fiscal.ca.gov/newsletter/open-fiscal-website-continues-to-improve-states-financial-transparency/.

First Amendment Coalition. California public records act primer, 2024. URL https://firstamendmentcoalition.org/handbook/california-public-records-act/.

FOIA.gov, U.S. Department of Justice. Freedom of information act statute, 2026a. URL https://www.foia.gov/foia-statute.html.

FOIA.gov, U.S. Department of Justice. Foia.gov draft restful https api spec, 2026b. URL https://www.foia.gov/developer/agency-api/.

FOIA.gov, U.S. Department of Justice. Foia.gov developer resources, 2026c. URL https://www.foia.gov/developer/.

FOIA.gov, U.S. Department of Justice. Annual and quarterly foia reports, 2026d. URL https://www.foia.gov/reports.html.

GovTech. White house, california department of justice partner on open data, 2024a. URL https://insider.govtech.com/california/www-techwire-net/white-house-california-department-of-justice-partner-on-open-data.html.

GovTech. California launches data-driven openjustice dashboard, 2024b. URL https://www.govtech.com/data/california-launches-data-driven-openjustice-dashboard.html.

International Organization for Standardization. Iso 15836-1:2017 — information and documentation — the dublin core metadata element set — part 1: Core elements, 2017. URL https://www.iso.org/standard/71339.html.

Judicial Branch of California. Who? where? how? viewing a court's electronic case records, 2026a. URL https://courts.ca.gov/policy-administration/public-records/who-where-how-viewing-courts-electronic-case-records.

Judicial Branch of California. Public records, 2026b. URL https://courts.ca.gov/policy-administration/public-records.

Judicial Council of California. Public records — judicial branch of california, 2024. URL https://courts.ca.gov/policy-administration/public-records.

Judicial Council of California. California rules of court, rule 10.500: Public access to judicial administrative records, 2026. URL https://courts.ca.gov/cms/rules/index/ten/rule10_500.

Justia. California government code sections 6275-6276.48 (2005), 2005. URL https://law.justia.com/codes/california/2005/gov/6275-6276.48.html.

Justia. Other exemptions from disclosure: Government code 6275-6276.48 (2010), 2010. URL https://law.justia.com/codes/california/2010/gov/6275-6276.48.html.

Justia. California government code section 7922.000 (2025), 2025. URL https://law.justia.com/codes/california/code-gov/title-1/division-10/part-2/chapter-3/article-1/section-7922-000/.

LegiScan. Legiscan api, 2024a. URL https://legiscan.com/legiscan.

LegiScan. Array session data archives — california, 2024b. URL https://legiscan.com/CA/dsets.

Legislative Analyst's Office. Proposition 59: Access to government information (ballot analysis), 2004. URL https://lao.ca.gov/ballot/2004/59_11_2004.htm.

Liebert Cassidy Whitmore. Ab 473 reorganizes and recodifies the california public records act, 2022. URL https://www.lcwlegal.com/news/ab-473-reorganizes-and-recodifies-the-california-public-records-act/.

Los Angeles County Sheriff's Department. Racial identity & profiling act (ripa) stop data, 2024. URL https://lasd.org/transparency/ripa/.

Lozano Smith. The california public records act has all new statutory citations, 2023. URL https://www.lozanosmith.com/news-clientnewsbriefdetail.php?news_id=3227.

National Archives and Records Administration. Freedom of information act (foia), 2026. URL https://www.archives.gov/foia.

National Institute of Standards and Technology. Nist sp 800-207: Zero trust architecture, 2020. URL https://csrc.nist.gov/pubs/sp/800/207/final.

National Institute of Standards and Technology. Nist sp 800-161 rev. 1: Cybersecurity supply chain risk management practices for systems and organizations, 2022a. URL https://csrc.nist.gov/pubs/sp/800/161/r1/final.

National Institute of Standards and Technology. Nist sp 800-218: Secure software development framework (ssdf) version 1.1, 2022b. URL https://csrc.nist.gov/pubs/sp/800/218/final.

National Institute of Standards and Technology. The nist cybersecurity framework (csf) 2.0, 2024. URL https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final.

Office of Environmental Health Hazard Assessment. Comment submissions — calenviroscreen 5.0, 2026a. URL https://oehha.ca.gov/calenviroscreen/comments/comment-submissions-calenviroscreen-50.

Office of Environmental Health Hazard Assessment. Summary of public workshops for draft calenviroscreen 5.0, 2026b. URL https://oehha.ca.gov/sites/default/files/media/2026-04/calenviroscreen50workshopcommentsd0406266.pdf.

Office of Environmental Health Hazard Assessment. Draft calenviroscreen 5.0 (official report landing page), 2026c. URL https://oehha.ca.gov/calenviroscreen/report/draft-calenviroscreen-50.

Office of Government Information Services, National Archives and Records Administration. Requester best practices: Things journalists ought to know about foia, 2023. URL https://www.archives.gov/ogis/resources/foia-for-journalists.

Open States. Open states api v3 overview, 2024. URL https://docs.openstates.org/api-v3/.

Orange County Superior Court. Case access — superior court of california, county of orange, 2024. URL https://www.occourts.org/online-services/case-access.

Pearson, Tyler. California laws api, 2024. URL https://github.com/tylerpearson/california-laws-api.

Plumas County Superior Court. Record searches — superior court of california, county of plumas, 2024. URL https://plumas.courts.ca.gov/online-services/record-searches.

Rancho Cordova School District. Sb 272 enterprise system catalog, 2016. URL https://www.rcsd.org/sb-272-enterprise-system-catalog.

Regional Center of the East Bay. Public records act request — rceb, 2024. URL https://rceb.org/about-us/public-records-act-request/.

Sacramento County. Sacramento county public portal, 2024. URL https://prod-portal-sacramento-ca.journaltech.com/public-portal/?q=Home.

San Diego Law Library. Requesting government records: California public records act, 2024. URL https://sdlawlibrary.libguides.com/c.php?g=1290791&p=9477556.

San Diego Regional Data Library. California openjustice datasets — sdrdl data repository, 2024. URL https://data.sandiegodata.org/dataset/openjustice-doj-ca-gov-datasets/.

San Francisco Chronicle. William t. bagley obituary, 2024. URL https://www.legacy.com/us/obituaries/sfgate/name/william-bagley-obituary?id=58663729.

Santa Cruz County. Sb 272 — enterprise systems catalog, 2016. URL https://www.santacruzcountyca.gov/Departments/InformationServices/SB272EnterpriseSystemsCatalog.aspx.

secretaryofstate.com. California business entity search, 2024. URL https://secretaryofstate.com/california/.

Sigstore. Sigstore cosign keyless signing overview, 2026a. URL https://docs.sigstore.dev/cosign/signing/overview/.

Sigstore. Sigstore rekor overview, 2026b. URL https://docs.sigstore.dev/logging/overview/.

SLSA. Slsa version 1.1 security levels, 2026. URL https://slsa.dev/spec/v1.1/levels.

Socrata. Api endpoints — socrata soda, 2024. URL https://dev.socrata.com/docs/endpoints.html.

Socrata / Tyler Technologies. Socrata developers, 2024a. URL https://dev.socrata.com.

Socrata / Tyler Technologies. Soql queries — socrata open data api (soda), 2024b. URL https://dev.socrata.com/docs/queries/.

StateScoop. California is building a portal of portals for its data, 2021. URL https://statescoop.com/california-portal-of-portals-data-sharing/.

Supreme Court of California. Cbs, inc. v. block (1986) 42 cal.3d 646, 1986. URL https://scocal.stanford.edu/opinion/cbs-inc-v-block-28477.

Supreme Court of California. Times mirror co. v. superior court (1991) 53 cal.3d 1325, 1991. URL https://scocal.stanford.edu/opinion/times-mirror-co-v-superior-court-state-california-31297.

Supreme Court of California. City of san jose v. superior court (2017) 2 cal.5th 608 (public business on personal accounts/devices is subject to the cpra), 2017. URL https://law.justia.com/cases/california/supreme-court/2017/s218066.html.

Supreme Court of California. National lawyers guild, san francisco bay area chapter v. city of hayward (2020) 9 cal.5th 488, 2020. URL https://law.justia.com/cases/california/supreme-court/2020/s252445.html.

The MITRE Corporation. Mitre att&ck enterprise matrix, 2026. URL https://attack.mitre.org/matrices/enterprise/.

The White House (Obama Administration). The police data initiative: Five-month update, 2015. URL https://obamawhitehouse.archives.gov/blog/2015/10/27/police-data-initiative-5-month-update.

Transparent California. Transparent california completes annual data collection of public pay and pensions, 2024. URL https://antiochherald.com/2024/05/transparent-california-completes-annual-data-collection-of-public-pay-pensions/.

Tulare County Employees' Retirement Association. Sb 272 — california public records act, 2024. URL https://tcera.org/news-publications/sb-272-california-public-records-act/.

UC Riverside Sustainability. Calenviroscreen 4.0 — ucr sustainability, 2024. URL https://sustainability.ucr.edu/calenviroscreen-40.

U.S. Department of Justice, Office of Information Policy. The freedom of information act, 5 u.s.c. section 552, 1966. URL https://www.justice.gov/oip/freedom-information-act-5-usc-552.

U.S. Department of Justice, Office of Information Policy. The freedom of information act, 5 u.s.c. section 552, 2026. URL https://www.justice.gov/oip/freedom-information-act-5-usc-552.

U.S. General Services Administration. Open government data act (title ii of the foundations for evidence-based policymaking act of 2018, pub. l. 115-435; 44 u.s.c. section 3506 et seq.), 2018. URL https://data.gov/open-gov/.

U.S. General Services Administration. Dcat-us schema (project open data metadata schema), v1.1, 2024. URL https://resources.data.gov/resources/dcat-us/.

Wikipedia. California public records act (original enactment, statutes of 1968, chapter 1473; signed by governor reagan; modeled on the federal foia), 1968. URL https://en.wikipedia.org/wiki/California_Public_Records_Act.

World Wide Web Consortium (W3C). Data catalog vocabulary (dcat) — version 3, w3c recommendation, 2024. URL https://www.w3.org/TR/vocab-dcat-3/.