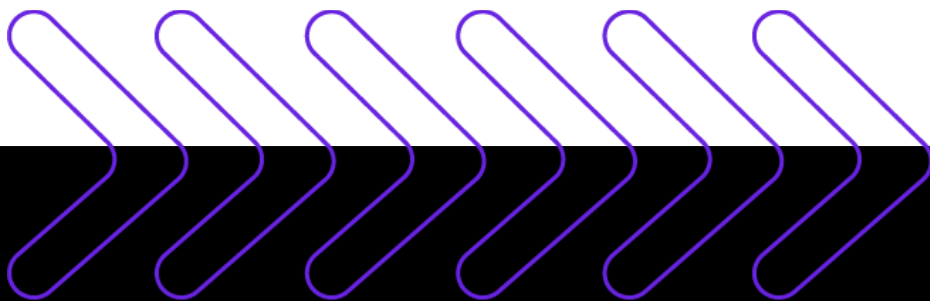


Advancing Transparency and Accountability: A Framework for a Law Enforcement Officer Accountability Database

November 2022



About CEOARE

CEO Action for Racial Equity (CEOARE) is a fellowship of over 100 companies that mobilizes a community of business leaders with diverse expertise across multiple industries and geographies to advance public policy in four key areas — healthcare, education, economic empowerment, and public safety. Its mission is to identify, develop and promote scalable and sustainable public policies and corporate engagement strategies that will address systemic racism, social injustice and improve societal well-being. Its focus is to improve the quality of life for the 47M+ Black Americans through advocacy and advancement of solutions that seek to end systemic racism.

Acknowledgements

This paper (the Report) was written by CEOARE Fellows Lisa Levin, Daniel Garcia, and Avery Joshua with contributions by Zachary Malitz, Chanel Cureton, Martha Voigt and Jamie Campbell. The authors would like to thank the following individuals and organizations for their review of and/or contributions to the Report:

Roslyn Brooks, Policy Lead, CEOARE

Marie Grant, Government Relations Consultant, CEOARE

Julia Sessoms, Government Relations Consultant, CEOARE

Michael Belitzky, Government Relations Consultant, CEOARE

Various CEO Action for Diversity & Inclusion Signatory Organizations

Joe Belitzky, Career defense attorney for law enforcement and correctional officers

Christine Caputo Granich, Associate General Counsel, New York State Law Enforcement Officers Union, Council 82, AFSCME, AFL-CIO

Julie Ciccolini, Director, Full Disclosure Project, National Association of Criminal Defense Lawyers

John Cooper, Executive Director, Safe & Just Michigan

Brandon Hicks, Government Affairs Lead, HP Inc.

Rachel Moran, Associate Professor, University of St. Thomas School of Law

David Riggs, Former Public Safety Director, Denver, Colorado and Former Public Safety Director and Chief of Police, Indianapolis, Indiana

Table of Contents

1. Executive summary.....	4
2. Introduction.....	6
The Issue: Law Enforcement Officer (LEO) Misconduct.....	6
Purpose and Objectives.....	8
Overview of Law Enforcement Officer Accountability Databases.....	8
Policy Landscape.....	10
Database Landscape.....	14
3. Law Enforcement Officer Accountability Database Design Framework.....	15
Analysis Methodology.....	16
Definitions.....	17
4. Design Element Analysis.....	19
Complaint Status.....	19
Misconduct Definition.....	23
Record Details.....	26
Access Rights.....	30
Audit and Compliance.....	33
Record Retention.....	35
Reporting Frequency.....	37
5. Conclusions/Recommendations.....	39
A Working Model for a Law Enforcement Officer Accountability Database.....	40
Future law enforcement reform.....	44
6. Appendix A: Law Enforcement Officer Accountability Database Matrix.....	46
7. Appendix B: Database Analyses.....	51
Introduction.....	51
Active Databases.....	55
Recently Authorized Databases Under Development.....	85

Executive summary

Over the past several years, the American public has witnessed many high-profile incidents of law enforcement officer (LEO) misconduct, with many involving officers' interactions with Black Americans. Misconduct ranges from minor administrative infractions to serious policy violations that can result in significant bodily injury or fatalities for community members. Ultimately, misconduct reduces a community's trust in its law enforcement and makes it harder for officers to perform their jobs. The cornerstone to a well-functioning, effective public safety system is accountability and transparency. A culture of accountability helps to build trust between officers and the community, and it fosters integrity and professionalism among law enforcement officers. Because of a lack of transparency into misconduct records, officers who routinely engage in misconduct often retain their jobs, gain promotions and sometimes move from department to department, inflicting harm on new communities and resulting in costly misconduct settlements that drain resources from cities and states.

At the local, state and federal levels, LEO accountability databases (also known as "misconduct databases") have emerged as a solution to address these issues by increasing transparency and accountability in policing. For purposes of our research, we define a LEO accountability database as a centrally stored collection of officer misconduct records and/or the outcome of misconduct proceedings. The definition also requires that the records be accessible on demand and be reported at the individual officer level.

In this Report, we provide an overview of the policy landscape for accountability databases. In addition, we introduce a novel framework for analyzing the data management and data governance practices of existing accountability databases and others under consideration or development. To demonstrate the utility of the framework, we analyzed 15 databases, administered by governments or independent organizations, to understand how each addressed the design elements of our framework (Appendix B) and showcased almost 50 additional databases maintained by governments or independent organizations (Appendix A).

Based on our analysis and the goal of advancing transparency and accountability, we offer a recommendation on each element of the framework. Collectively, we regard the recommendations as a working model ("Working Model"), that is intended to serve as a starting point for further discussion among stakeholders. Within each element, we welcome additional perspectives and acknowledge the need to continue refining and developing key terms and definitions. Finally, we ask that the Working Model be viewed in the aggregate, giving due consideration to the interconnectedness of the design elements and their holistic impact. We recommend our Working Model, outlined here, as a starting point to advance the policy discussions:

Data Management

1. Complaint Status: Include complaints involving allegations that have been Substantiated, Pending Investigation, and Cleared/Exonerated, with levels of tiered access provided to any records that have not been substantiated
2. Misconduct Definition: Include mandatory submitted records based on a standardized definition of misconduct involving 1) actions taken on an officer's certification/license including decertification and suspension; and 2) other matters of serious misconduct.
3. Record Details: Report a minimum of six data fields to enable quality and efficient analytics

Data Governance

1. Access Rights: Provide levels of tiered access, allowing some stakeholders increased access to select information
2. Audit and Compliance: Conduct regular audits of the records, and provide adequate incentives for compliance by the law enforcement agencies
3. Record Retention: Establish a definitive period for retaining records in the database
4. Reporting Frequency: Require regularly scheduled reporting at a minimum interval of every three to six months

Advancing accountability databases is just one type of policy change that can help improve law enforcement transparency and accountability. We acknowledge that there are other important public safety reforms such as training on de-escalation and the duty to intervene, implementing use-of-force standards, community relationship building, and mandating the use of body cameras. But here we concentrate on the role databases can play in reducing incidents of misconduct and protecting the lives and well-being of our citizens, especially Black Americans. There is broad support for LEO accountability databases across the political spectrum, and this Report is intended to support the policy discussion and help advance databases from theory into practice on a nationwide level. CEOARE looks forward to engaging with policymakers, law enforcement, and the community at large on our seven-point framework for a LEO accountability database. We urge finding common ground so that together we can help rebuild trust between law enforcement and the communities that they serve.

Disclaimer: *The analysis of individual databases was based on publicly available information obtained through online sources. Where information was not available or could not be clearly discerned, we documented the matter with a question mark (?).*

Engage with Us: *We are releasing the database analysis as a working draft for the public's review. In addition, we appreciate any feedback regarding our proposed framework and recommendations in the hopes that future iterations will incorporate more comprehensive input from all stakeholders. Share your comments, questions or interest in collaboration by reaching out to leta@ceoactionracialequity.com.*

Introduction

The Issue: Law Enforcement Officer (LEO) Misconduct

George Floyd was detained by Minneapolis police in May 2020 after trying to use a counterfeit \$20 bill in a convenience store. In a case that became known around the world, police officer Derek Chauvin was captured on video kneeling on Floyd's neck and killing him. Floyd's death and the deaths of many unarmed Black men and boys at the hands of law enforcement, including Tamir Rice and Michael Brown, underscores how officer misconduct can continue for years without public awareness or oversight. Officer Chauvin had been the subject of at least 17 complaints over his almost two-decade career.¹

After Officer Timothy Loehmann shot and killed 12-year-old Tamir Rice, who had been playing with a toy gun, the fact that he had lied on his job application to the Cleveland Police Department came to light. Loehmann claimed he left his prior position for "personal reasons,"² but personnel records, which the Cleveland Police Department did not access, told another story. As a patrol officer in Independence, Ohio, Loehmann was determined unfit to serve and found to have "an inability to emotionally function."³ Officer Darren Wilson shot and killed Michael Brown, an unarmed 18-year old walking down the street in Ferguson, Missouri.⁴ Officer Wilson's work history included working as a police officer in Jennings, Missouri, where tensions between Black and white residents became so tense that the city council fired all the officers. That did not prevent Wilson from getting hired in nearby Ferguson.⁵

A study reported in the Yale Law Journal found that law enforcement executives are at risk for hiring "wandering officers," those who get fired by one agency and find work at another agency.⁶

¹ Derek Hawkins, "Officer Charged in George Floyd's Death Used Fatal Force Before and Had History of Complaints," *The Washington Post*, May 29, 2020, <https://www.washingtonpost.com/nation/2020/05/29/officer-charged-george-floyds-death-used-fatal-force-before-had-history-complaints/>.

² "City of Independence Public Records Request - Timothy Loehmann" (Taft Stettinius & Hollister LLP, December 3, 2014), <https://s3.documentcloud.org/documents/1374587/independence-timothy-loehmann-response-to.pdf>, 7.

³ *Ibid.*, 59.

⁴ Memorandum, U.S. Department of Justice Report Regarding the Criminal Investigation Into the Shooting Death of Michael Brown by Ferguson Missouri Police Officer Darren Wilson, March 4, 2015, 4, https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/doj_report_on_shooting_of_michael_brown_1.pdf,

⁵ *Ibid.*

⁶ Ben Grunwald and John Rappaport, "The Wandering Officer," *The Yale Law Journal* 129, no.6 (April 30, 2020), <https://ssrn.com/abstract=3589544>, 1676, 1682.

One study found that wandering officers who had found new jobs were fired for misconduct approximately **50% more often** than officers who had never been fired.⁷

State laws restrict or close off public access to officer misconduct records⁷, leaving community members and, in some cases, hiring officials without the resources to track down applicant personnel records and with little to no data on the applicants' misconduct histories. The current system — replete with its lack of transparency and timely access to complete officer personnel records — creates a public safety risk to community members who are powerless to access information but often subject to policing by the very officers that are known to have patterns of and/or been disciplined for serious misconduct.

The financial cost of officer misconduct is staggering too, yet largely unknown to the public. Payments made to settle misconduct lawsuits are not easily accessible and are often not tracked by cities and towns. Taxpayers are kept in the dark. In March 2022, The Washington Post “collected data on nearly 40,000 payments at 25 of the nation’s largest police and sheriff’s departments... documenting more than \$3.2 billion spent to settle claims” during the period from 2010-2020.⁸ It is repetitive misconduct involving the same officers that drives settlement costs. The Washington Post found that “officers whose conduct was at issue in more than one payment accounted for... nearly half of the money spent by the departments to resolve allegations.”⁹ The Washington Post went on to say that “even when payments are covered by insurance claims, taxpayers ultimately still pay as those claims drive up the cost of insurance.”¹⁰

\$3.2 billion

was paid by 25 of the largest police and sheriff’s departments in the nation during the period 2010-2020.⁹

- In New York City of the \$1.779 billion paid out, 46% involved officers named in multiple payments
- In Detroit, of the \$48 million paid out, 59% involved officers named in multiple payments
- In Boston, of the \$17 million paid out, 38% involved officers named in multiple payments
- In Chicago, of the \$528 million paid out, 72% involved officers named in multiple payments

Source: *The Washington Post*, excerpted from the table titled “Explore the data”.¹¹

⁷ Kallie Cox and William Freivogel, “Police Misconduct Records Secret, Difficult to Access,” Associated Press, January 24, 2022, <https://pulitzercenter.org/stories/police-misconduct-records-secret-difficult-access>.

⁸ Keith L. Alexander, Steven Rich and Hannah Thacker, “The Hidden Billion-Dollar Cost of Repeated Police Misconduct,” *The Washington Post*, March 9, 2022, <https://www.washingtonpost.com/investigations/interactive/2022/police-misconduct-repeated-settlements/>.

⁹ Ibid.

¹⁰ Ibid.




¹¹ Ibid.

Not only are the claims payments kept under wraps, but so are the names of the officers involved. Of the 25 cities reported by The Washington Post, only four indicated tracking payment information.¹² A few cities recorded payments by officers' name or badge number.

Lastly, officer misconduct records are often shielded due in part to a lack of centralized, accessible data. With better access to and analysis of misconduct data, law enforcement agencies would be better able to evaluate the effectiveness of existing training programs, discipline processes and incentive structures. It is well known that cops do not “tell” on other cops and that officers who speak out against illegal or unethical actions by fellow officers are pushed out of their departments and “branded traitors by fellow officers.”¹³ This protects officers accused of wrongdoing and punishes the whistleblowers, creating a culture of retaliation against victims and officers who want to step up and do the right thing. With better access to and use of misconduct data, law enforcement agencies can begin to establish an environment where accountability and improvement are the norm and where safer, healthier, and stronger communities are the goal.

Purpose and Objectives

The purpose of this Report is to:

 <p>Educate and create awareness about the current state of LEO accountability databases</p> <p>Provide an overview of how accountability databases and state freedom of information laws can support access to officer disciplinary records.</p>	 <p>Establish a framework to analyze existing practices for LEO accountability databases</p> <p>Analyze seven key design elements for 15 databases using a comprehensive methodology.</p>	 <p>Propose a working model for LEO accountability database for use on the federal, state, or local level</p> <p>Recommend positions on each of the seven key design elements for use by policymakers in drafting legislation and regulations.</p>
---	---	--

Overview of Law Enforcement Officer Accountability Databases

Law enforcement officer accountability databases have emerged as a solution to the issues of wandering officers and as a tool to identify officers who pose a threat to the communities in which they work.

For purposes of the Report, a LEO accountability database is defined as having four attributes:

1. A centrally stored collection of records.
2. Accessible on demand.

¹² Ibid.

¹³ Nicole Carroll, “USA TODAY Investigation Finds Widespread Retaliation Against Police Whistleblowers,” *USA TODAY*, November 12, 2021, <https://www.usatoday.com/story/opinion/2021/11/12/usa-today-investigation-shows-how-law-enforcement-punishes-whistleblowers/6373652001/>.

3. Containing Substantiated Misconduct, Cleared/Exonerated, and Pending Officer Misconduct and/or the outcome of misconduct proceedings.
4. Reported on an individual officer level.

This definition excludes databases that do not meet all the above criteria. For example, the voluntary FBI Use of Force database¹⁴ does not meet this definition. While it is a centrally stored collection of records reported on an individual officer level that is accessible on demand, it doesn't contain a collection of misconduct records. The incidents included in the database have not been assessed for whether the officers committed any violation of department policy or federal/state/local law.¹⁵

LEO accountability databases come in several forms and vary not just in what data is presented but also in how it's presented. The data in a database can range from information on policing activities, including complaints, disciplinary actions, terminations and decertifications, to information about lawsuits and settlements related to officer conduct. Databases can provide access to primary source documents and case files, have tools that allow users to find data related to individual officers or incidents, or allow users to export data for offline analysis.

While LEO accountability databases are relatively new, disciplinary databases already exist for other professions. The data collection practices for these databases vary considerably.¹⁶ The National Practitioner Data Bank (NPDB), for instance, was established by Congress in 1986 and contains data on "medical malpractice payments and certain adverse actions related to healthcare practitioners, providers and suppliers."¹⁷ The Federation of State Medical Boards has its own database, which collects some information that the NPDB does not.¹⁸ State professional licensing boards that oversee physician discipline for criminal convictions, medical malpractice and other wrongdoing also maintain discipline databases.¹⁹ Similarly, state bar associations and other state agencies maintain databases that allow residents to search for attorneys licensed to practice in that state and access disciplinary histories.²⁰

Ultimately, a nationwide LEO accountability database, requiring participation by federal, state and local law enforcement agencies, would serve as a holistic database. Beyond providing access to the records of officers guilty of misconduct and identify those who "wander" to other departments, it would bring added professionalism to law enforcement as a career. A nationwide database would also allow stakeholders to see patterns in misconduct that might act as an early warning system, identifying officers in need of reassignment or retraining before more serious misconduct occurs.

¹⁴ "Use of Force," FBI (FBI, September 14, 2018), <https://www.fbi.gov/services/cjis/ucr/use-of-force>.

¹⁵ Ibid.

¹⁶ Matt Wynn and John Fauber, "NPDB Records Often Ignored in Docs' Licensing," Milwaukee Journal Sentinel, March 7, 2018, <https://www.medpagetoday.com/special-reports/states-of-disgrace/71600>.

¹⁷ "About Us," The NPDB (U.S. Department of Health & Human Services), accessed April 27, 2022, <https://www.npdb.hrsa.gov/topNavigation/aboutUs.jsp>.

¹⁸ Wynn and Fauber, "NPDB Records."

¹⁹ Charles Ornstein and Annie Waldman, Princess Ojiaku, "Our Doctor Might Have a Disciplinary Record. Here's How to Find Out," *ProPublica*, Published January 8, 2015, last updated December 11, 2019, <https://projects.propublica.org/graphics/investigating-doctors>. For example, see medical license databases in Florida, California, and Washington, DC as examples.

²⁰ See the attorney databases in [Texas](#), [Michigan](#), and [New York](#)

Policy Landscape

National

Following Floyd's death, federal lawmakers from both sides of the aisle set out to create policies to improve policing practices in this country and strengthen relationships between law enforcement agencies and community members. In March 2021, the House of Representatives passed a sweeping federal policing bill, the George Floyd Justice in Policing Act of 2021, H.R. 1280, to establish transparency, accountability and national standards in policing. One proposed reform included creating a national police misconduct registry to track and aggregate misconduct complaints, discipline records, termination records and legal settlements across the 18,000 law enforcement agencies in the country.²¹ Ultimately, bipartisan negotiations over the legislation collapsed, and the George Floyd Bill stalled in the Senate, including the measure to create a national misconduct registry.²²

Absent Congressional action on police reform, President Biden issued an executive order titled "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety" in May 2022, on the second anniversary of Floyd's death.²³ Among other reforms, the order establishes a federally mandatory National Law Enforcement Accountability Database.²⁴ The accountability database is an important first step to advancing transparency and accountability in policing, but its scope is limited due to the president's authority to regulate only federal law enforcement agencies. The executive order encourages state, tribal, local, and territorial participation in the federal database and offers guidance and technical assistance, but nothing is mandated.²⁵

On the federal level, the accountability database requires collection of federal officers' misconduct records including convictions, termination, decertifications, civil judgments, resignations and retirements while under investigation for serious misconduct and sustained complaints or information on discipline for serious misconduct — in addition to recognitions and awards.²⁶ The Attorney General still needs to determine what information will be made available to the public, taking into consideration the public need for transparency and accountability weighed against the safety and privacy of law enforcement officers.²⁷

²¹ Carrie Mihalcik, "Police Reform Bill Would Create a National Registry on Misconduct," *CNET*, June 8, 2020, <https://www.cnet.com/news/police-reform-bill-would-create-a-national-registry-on-misconduct/>.

²² Joan E. Greve, "Sweeping George Floyd Police Reform Bill Stalls as Talks Collapse," *The Guardian*, September 22, 2021, <https://www.theguardian.com/us-news/2021/sep/22/us-police-reform-bill-congress-bipartisan-talks>.

²³ Executive Order 14074 of May 25, 2022, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, 87 FR 32945, <https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and>.

²⁴ Executive Order on Policing, Section 5.

²⁵ Executive Order on Policing, Section 5(f).

²⁶ Executive Order on Policing, Section 5(a), 5(b)(ii), (iii).

²⁷ Executive Order on Policing, Section 5(g)(ii).

State/Local/Independent

While federal police reform has languished in Congress, some states, municipalities, and independent entities have stepped up to advance transparency and accountability in policing. Many agree that if there is to be impactful work, it will happen on the state and local level.

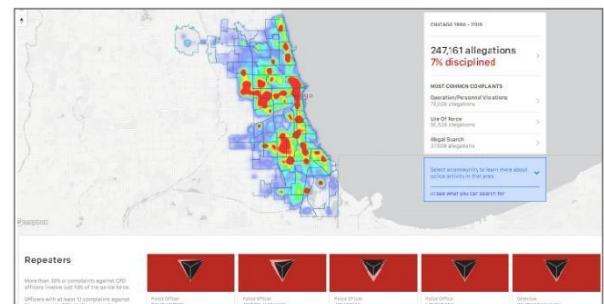
One area where momentum is taking hold is with the creation of LEO misconduct and accountability databases. What has evolved are databases across various jurisdictions that are administered by both government and independent entities. Over the past five years, multiple accountability databases have been developed as the result of policies enacted at the state or local level or through independent efforts by journalists and advocacy organizations.²⁸

Because policing is local, each department has its own rules, responsibilities, and authority regarding officer discipline. Many of the departments do not collect the same kinds of information, and that presents challenges to creating a standardized database. The result is a patchwork of different databases across the country each with different data management and data governance practices.

Although limited in scope, these databases still enable users to start identifying patterns in misconduct across a police department or for specific officers, allowing law enforcement executives to act early before more serious incidents occur.

One particularly interesting example of existing databases is the Invisible Institute's Citizens Police Data Project (CPDP), a collaborative effort between the Invisible Institute and the University of Chicago Law School's Mandel Legal Aid Clinic. Initially acquired through public records requests, the database includes records of misconduct allegations against Chicago Police Department officers.²⁹ In addition to attorneys, law enforcement investigators and the public, "even individual police officers in Chicago are accessing the records [in the CPDP]. Rajiv Sinclair, the CPDP director, [said that] police officers have anonymously told his team that they use the database 'in order to avoid getting partnered up with someone who they don't want to get,' out of concern that they will be caught up in misconduct."³⁰

Last Name	First Name	Rank	Command	Incident Date	Complaint Category	Allegation	CORB Finding	NYPD Finding	Penalty	Officer Race	Race of Impacted Person	District/Location
MEDCO	Taylor	Talko	11N-100	2019-03-18	Alarms Of Jurisprudence	Trial of Law	Indicated	NA	NA	White	Hispanic	14C-01
MEDINA	Nelson	Talko	18-1132	2019-01-11	Force	Physical Abuse	Order - Pending Litigation	NA	NA	Hispanic	Black	14C-01
PARK	Esteban	Officer	11N-100	2019-01-11	Force	Physical Abuse	Order - Pending Litigation	NA	NA	White	Black	14C-01



Criminal Justice

Home > Criminal Justice > DPSST Professional Standards/Economic Sanctions Database

DPSST Professional Standards/Economic Sanctions Database

Below is a searchable database of DPSST Professional Standards Cases and agency police officer discipline that include economic sanctions as required to be reported per ORS 181A.004.

For a detailed explanation of the fields, please scroll to the bottom of this page. NOTE: Records with a Status of Under Review indicates that DPSST has opened a professional standards case due to the receipt of information indicating that an officer may have engaged in behavior that violates an established certification standard. An open case that is under review is not proof that a public safety professional engaged in misconduct.

Figure 1: Screenshots of the publicly available NYPD Misconduct Complaint Database, Citizens Police Data Project, and Oregon DPSST Sanctions Database, respectively

²⁸ Taylor Avery, "Biden Wants More Transparency for Police Disciplinary Records. Experts Say It's Harder Than it Sounds," *USA Today*, July 31, 2021, <https://www.usatoday.com/story/news/2021/07/31/biden-wants-openness-police-disciplinary-files-thats-hard-do/5422091001/>.

²⁹ "Citizens Police Data Project," Invisible Institute, accessed March 24, 2022, <https://invisible.institute/police-data/>.

³⁰ Stephanie Wykstra, "In Response to Police Misconduct, a Flourishing of Online Databases," *Undark Magazine*, June 5, 2019 (quoting Rajiv Sinclair, Director of the Citizens Police Data Project) <https://undark.org/2019/06/05/police-conduct-databases-eric-garner/>.

“Police officers have anonymously [stated] that they use the database ‘in order to avoid getting partnered up with someone who they don’t want to get,’ out of concern that they will be caught up in misconduct.”³¹

Rajiv Sinclair, Director,
Citizens Police Data Project

The New York Civil Liberties Union also created a publicly searchable database, the New York City Police Department (NYPD) Misconduct Complaint Database, that includes public complaints made to the New York City Civilian Complaint Review Board (excludes complaints made directly to the NYPD).³¹ The state of Oregon established the Department of Public Safety Standards & Training, Professional Standards/Economic Sanctions Database, a publicly searchable database of the names of officers whose licenses have been denied, suspended, or revoked due to misconduct.³² Community members need to submit a public records request to access the complete file on the circumstances of the misconduct. These examples illustrate the vast differences in how misconduct records are sourced and maintained as well as who has access to the information.

Additionally, recent law enforcement reform legislation in North Carolina³³ and Massachusetts³⁴ has created state-level requirements for law enforcement agencies to check the National Decertification Index (NDI) prior to hiring any candidates.³⁵

Public Records Requests/Freedom of Information Act

Federal and state freedom of information act (FOIA) laws provide another way to access government information. The purpose of FOIA laws is to open the workings of government to the public. However, that is not always the case with law enforcement agencies. Officer disciplinary histories remain secret or at least difficult to access in at least 32 states.³⁶ Depending on the jurisdiction, officer misconduct records or limited portions of them may be available by making a written request to the agency, but agencies often deny the requests based on exemptions in the law that allow withholding information for reasons like personal privacy, confidentiality of personnel records or pending investigations.³⁷ Some states — California, New York, Illinois, Colorado, Massachusetts and Maryland — have opened access by reforming FOIA exemptions or through court cases compelling disclosure of the records.³⁸

³¹ “NYPD Misconduct Complaint Database,” New York Civil Liberties Union, May 18, 2021, <https://www.nyclu.org/en/campaigns/nypd-misconduct-database>.

³² “DPSST Professional Standards/Economic Sanctions Database,” Department of Public Safety Standards & Training (Oregon.gov), accessed May 5, 2022, <https://www.oregon.gov/dpsst/cj/pages/cases.aspx>.

³³ “House Bill 547 (2021-2022 Session),” North Carolina General Assembly, April 13, 2021, <https://www.ncleg.gov/Sessions/2021/Bills/House/PDF/H547v0.pdf>, Section 1(a)(21).

³⁴ “An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth,” The General Court of the Commonwealth of Massachusetts, accessed April 13, 2022, <https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter253>, Section 4(d).

³⁵ The National Decertification Index is currently being expanded pursuant to President Trump’s June 2020 Safe Policing for Safe Communities Executive Order. “NDI Expansion Project,” IADLEST (IADLEST), accessed July 7, 2022, <https://www.iadlest.org/our-services/ndi/about-ndi>.

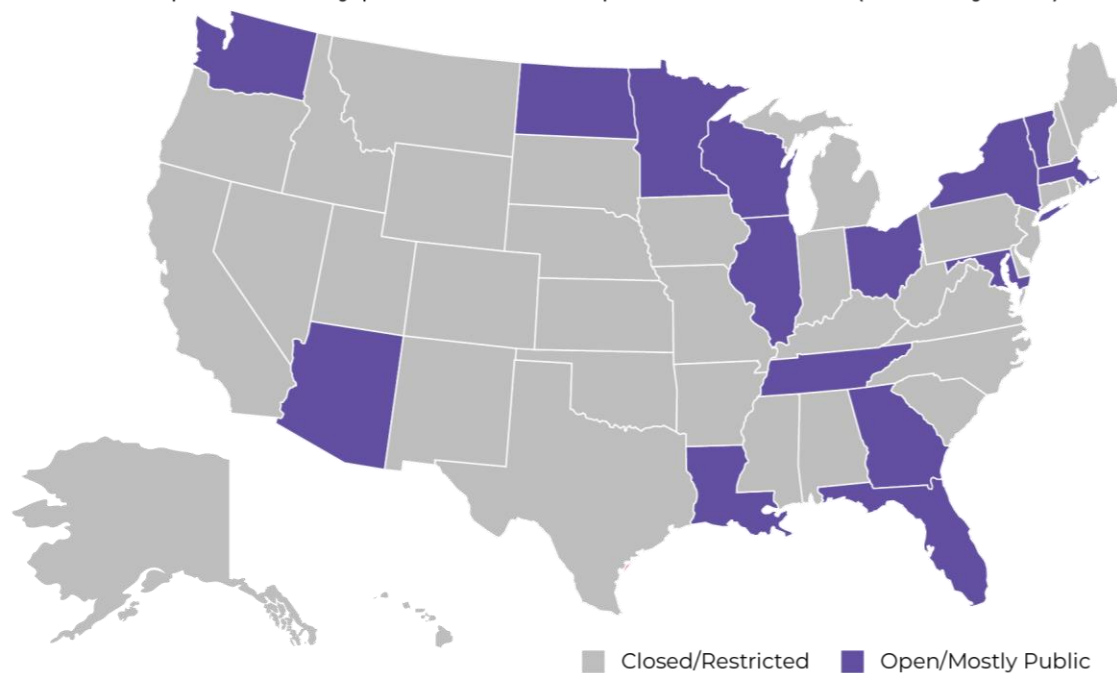
³⁶ Kallie Cox and William Freivogel, “Police Misconduct Records Secret, Difficult to Access.”

³⁷ Ibid.

³⁸ Ibid.

Police misconduct record availability

15 states have open or mostly public records for police misconduct (as of May 2021)



While the trend of increasing disclosure at the state level is positive, FOIA remains an inadequate method to provide meaningful transparency into officer misconduct records. First, FOIA provides access to a fragmented set of records and requesters must navigate a patchwork of state confidentiality laws. The process can be burdensome and protracted with FOIA litigation taking years, such as the Invisible Institute’s work in Chicago to create the CPDP. Some states may not collect the data, have “shoddy record-keeping” practices or lack the administrative resources to maintain or produce the information.³⁹ News outlets in West Virginia, for example, have shed light on law enforcement agencies’ inconsistent recordkeeping and poor response to open record laws requests.⁴⁰ And just because data may be accessible by the public, agencies can impose hefty fees for each request.⁴¹ As journalists and media sources have explained, “the challenges we encountered in collecting and analyzing data on [misconduct] settlements are indicative of broader problems and complications in police accountability: lack of standardization, a dearth of transparency and incomplete or missing data.”⁴²

³⁹ Amelia Thomson-Devaux, Laura Bronner and Damini Sharma, “Police Misconduct Costs Cities Millions Every Year. But That’s Where The Accountability Ends,” The Marshall Project, February 22, 2021, <https://www.themarshallproject.org/2021/02/22/police-misconduct-costs-cities-millions-every-year-but-that-s-where-the-accountability-ends>.

⁴⁰ American Civil Liberties Union West Virginia, “Police Misconduct Report 2020,” October 29, 2020, https://www.acluww.org/sites/default/files/field_documents/2020_police_misconduct_report_aclu-ww.pdf, 5-6.

⁴¹ Jessie Gomez, “What’s the Costliest Public Records Request Fee in Your State?,” MuckRock, September 19, 2018, <https://www.muckrock.com/news/archives/2018/sep/19/high-fees-map/>.

⁴² Thomson-Devaux, Bronner, and Sharma “Police Misconduct Costs Cities Millions Every Year. But That’s Where The Accountability Ends.”

Database Landscape

To understand the breadth and complexity of LEO accountability databases, we conducted a review of existing database practices and proposals on two levels.

Appendix A, the Law Enforcement Officer Accountability Database matrix, identifies close to 50 accountability databases that are either in operation or under construction. The databases are categorized along the matrix identifying the:

1. *Jurisdiction*, whether the database's reported incidents of misconduct are at the federal, state or local law enforcement level.
2. *Administrator*, whether the database is managed by a governmental or independent entity.

Appendix B selects a cross section of databases from the matrix for a deeper analysis. Fifteen databases are analyzed for each of the following elements in the Design Framework.

1. Complaint Status
2. Misconduct Definition
3. Record Details
4. Access Rights
5. Audit and Compliance
6. Record Retention
7. Reporting Frequency

Finally, we discuss key takeaways on existing practices and recommendations to advance the principles of accountability and transparency in policing.

Law Enforcement Officer Accountability Database Design Framework

A key purpose of this Report is to provide a framework for understanding and analyzing key elements of LEO accountability databases across the United States (US). The Design Framework consists of seven elements explored in detail in the analysis section that follows. Each design element falls into either the data management or data governance category.

The collection, storage and management of data are at the center of an accountability database. **Data management** refers to “the practice of collecting, keeping and using data securely, efficiently and cost-effectively.”⁴³ Law enforcement, policymakers, journalists, and other stakeholders should be able to make sense of the data collected and rely on its accuracy and completeness for hiring decisions, research, and other public safety uses. Like businesses, law enforcement agencies should have a strategy to manage data on officer misconduct and discipline. The elements outlined below — Complaint Status, the definition of misconduct and the details of each misconduct record — are key to developing a meaningful and agile data management system.

Data governance is also a critical concept for effective databases. Businesses describe data governance as “the policies and procedures that are implemented to ensure an organization’s data is accurate ... and handled properly while being input, stored, manipulated, accessed and deleted.”⁴⁴ There are various policies to help confirm the reliability and integrity of data reported to the database, including audits of the reported information, Record Retention, schedules for Reporting Frequency and penalties for noncompliance.

⁴³ OCI, “Data Management Defined,” <https://www.oracle.com/database/what-is-data-management/>.

⁴⁴ SAP, “What is Data Governance?” <https://www.sap.com/insights/what-is-data-governance.html>.

Design Elements

Data Management



1. Complaint Status: at which stage of an investigative process is a misconduct complaint eligible to be included in the database?



2. Misconduct Definition: Is there a standardized definition for misconduct, are records submitted voluntarily or through a mandate, and does the scope include only licensing actions?



3. Record Details: what information is included for each record in the database?

Data Governance



4. Access Rights: who has access to the information in the database?



5. Audit and Compliance: are records audited by an internal and/or independent auditor and are there penalties or other incentives to support compliance with the terms and conditions of the database?



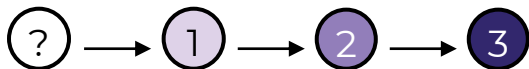
6. Record Retention: does the database have a record retention policy?



7. Reporting Frequency: are records reported on a regular basis to the database?

Analysis Methodology

In the analysis of individual databases (see Appendix B), we use a consistent scale to assess how that database approaches each of the design elements. The analysis of individual databases was based on publicly available information obtained through online sources. Where information was not available or could not be clearly discerned, we documented the matter with a question mark (?).



A “?” indicates that there is either no information or there is insufficient information available to understand how a database addresses a specific design element. Using the Reporting Frequency design element as an example, a database would be assessed as a “?” if there was no public information about how often records were added to or updated in the database. Levels 1 through 3 are defined for each design element in the following section of this Report.

Our goal is to analyze each database under a common framework that can be applied for consistent analysis. It is not to rank or judge the database's effectiveness. We recognize that each database is designed with certain end goals in mind and within certain regulatory and legal environments. These factors need to be considered in reviewing the analyses. This framework is a tool for understanding databases, but it's not intended to identify which databases are “leading” examples. Readers, based on their individual needs, will be able to use the framework to identify elements among databases that are of most interest to them and help to ground policy discussions with a diverse set of stakeholders.

Definitions

The following represents definitions of key terms used in the Report:

Term	Definition
Complaint	A written grievance filed with a federal, state, or local law enforcement agency or a law enforcement oversight body alleging misconduct.
Cleared/ Exonerated	Where an investigation determines that an officer did not do what was alleged or was exonerated of wrongdoing
Database Administrator	The agency or organization responsible for administering and managing the accountability database.
Data Management	Practices for collecting and organizing data to support data analytics and decision-making for stakeholders.
Data Governance	Policies and procedures to confirm the accuracy, usability and reliability of the data collected, along with oversight of Access Rights and compliance with the data reporting policy.
Design Element	An element of database design in either the data management (e.g., Misconduct Definition) or data governance (e.g., audit policy) category.
Design Framework	A framework consisting of the seven design elements to be used for understanding and analyzing accountability databases.
Law Enforcement Officer Accountability Database	Also known as a misconduct database, accountability database, police misconduct registry or discipline database, in this Report, a LEO accountability database must meet each of the four criteria below: <ol style="list-style-type: none"> 1. A centrally stored collection of records. 2. Accessible on demand. 3. Containing substantiated misconduct, pending investigation misconduct and/or the outcome of misconduct proceedings including cleared or exonerated finding. 4. Reported on an individual officer level.
Misconduct	Any violation of any federal, state, or local law, regulation, executive order, or department policy committed by a law enforcement officer.
Officer	A federal, state, or local law enforcement officer including those employed by local or state police departments, sheriff's offices, transportation departments or correctional facilities.
Pending Investigation	An investigation by the applicable federal, state, local law enforcement or other relevant agency into the status of a misconduct complaint or allegations that has not yet been completed
Record Retention	The time period that records are retained in a database.
Releasing Agency	Agencies/departments that release misconduct information in response to a public request for information.

Reporting Agency	Agencies/departments that submit misconduct information to a database.
Substantiated Misconduct	An allegation or complaint of misconduct that was investigated and a finding of misconduct was made by the applicable federal, state, local law enforcement or other relevant agency or court of law.
Unfounded	An allegation or complaint of misconduct where there is credible evidence that the misconduct did not occur.

Design Element Analysis

Complaint Status



Description

For purposes of this analysis, a database is assessed based on the following criteria:

LEVEL ?	LEVEL 1	LEVEL 2	LEVEL 3
No information or insufficient information available to understand how the database addresses the design element.	Includes records for Substantiated Misconduct.	Includes records for Substantiated Misconduct AND Pending Investigations OR Cleared/ Exonerated Misconduct.	Includes records for Substantiated Misconduct, Pending Investigation, AND Cleared/ Exonerated Misconduct.

A threshold issue in the design of databases is what types of records should be collected. We analyzed databases based on three categories of records. Complaints: 1) involving allegations that have been substantiated by the applicable agency or a court (Substantiated Misconduct); 2) that are pending review (Pending Investigation); and 3) involving findings, by the applicable reviewing agency or a court, that the officer did not commit the alleged wrongdoing or misconduct (Cleared/Exonerated).⁴⁵ Within the categories, we recognize that there are additional levels that could be considered including complaints that are deemed unfounded or complaints that are substantiated but where no discipline has been imposed. We welcome more discussion around other levels for consideration and how such terms should be defined. But for purposes of this initial Report, we applied the three broad categories described above. Understanding the stages of complaint processing is an important driver to advancing transparency and accountability in law enforcement generally, but particularly into the investigative and discipline process. Finding agreement on language will help stakeholders find common ground to determine the types of records that should be included in databases.

⁴⁵ Josefa Velasquez, Greg B. Smith, and Reuven Blau. "The Complaint Files NYPD Unions Don't Want You to See." *THE CITY*, July 31, 2020, <https://www.thecity.nyc/2020/7/31/21350186/nypd-complaint-files-unions-police-new-york-city>.

Advocacy organizations have raised several questions about law enforcement agency investigation practices.⁴⁶ Is there enough rigor around the complaint review process? What evidence is there that an investigation was thorough and complete? Was a fair and appropriate outcome assigned after the evaluation of the complaint? Information about an agency's internal investigative practices or the records themselves are not always forthcoming, clear or disclosed in a timely manner.⁴⁷ For these questions, among others, advocates have sought to have visibility into all complaints to allow for their own analysis to determine whether outcomes fit the complaint or to seek additional explanation.

Conversely, law enforcement stakeholders have claimed⁴⁸ that including complaints that are pending investigation or those in which an officer has been exonerated, in any database, regardless of who can access those complaints, can expose officers to potentially harmful outcomes and may disqualify that officer from future employment within or outside of law enforcement. Law enforcement unions have also argued that including such complaints may encourage more frivolous and unwarranted claims by stakeholders seeking to endanger an officer.⁴⁹

⁴⁶ "Shielded from Justice: Police Brutality and Accountability in the United States - Investigation and Discipline," Human Rights Watch, June 1998, accessed April 7, 2022. <https://www.hrw.org/legacy/reports98/police/uspo08.htm>.

⁴⁷ Dusty Christensen and Greta Jochem, "A Test of Transparency: Public Records Requests Yield Mixed Results from Area Police Departments," *Daily Hampshire Gazette* (Concord Monitor), December 17, 2021, <https://www.gazettenet.com/How-transparent-are-police-departments-internal-affair-records-39655379>.

⁴⁸ Bill Cummings, "Policing the Police: Secretive System Rarely Leads to Serious Punishment for CT Police," *Connecticut Post*, June 23, 2021, <https://www.ctpost.com/projects/2021/police-misconduct/>.

⁴⁹ Kayla Regan, "Bill That Would Criminalize False Complaints against Cops Stalled," *Police1*, March 20, 2014, <https://www.police1.com/investigations/articles/bill-that-would-criminalize-false-complaints-against-cops-stalled-2oCJC7CHSXHTZa9J/>.

Advocates for including complaints of Pending Investigation and Cleared/Exonerated argue that if databases are limited to substantiated complaints only, "... disciplinary outcomes are

Stakeholder Perspective:

“Council 82 supports legitimate measures that strengthen the public’s trust in law enforcement, but cannot support an “accountability” database which includes allegations, unfounded or unsubstantiated complaints of misconduct, or any matter concerning misconduct for which an officer has been exonerated and does not include a protocol for officers to clear their names, preserve their reputations, and compensate them for damages when they are wrongfully included in that database.”

- Christine Caputo Granich, Associate General Counsel, New York State Law Enforcement Officers Union, Council 82, AFSCME, AFL-CIO.

going to be simply left unsubstantiated so that [the officers] won’t be able to face public scrutiny.”⁵⁰ Accountability databases can be designed to include as much data as possible so that stakeholders can filter for the content that is relevant and appropriate for their consideration. Stakeholders who are interested only in complaints that have been reviewed, investigated, and adjudicated, for example, would filter out pending claims. However, there is also the risk that those who have access to complaints that have not been substantiated might not fully understand the investigation process and may consider such data as being representative of an officer’s character and performance.

The percentage of complaints that are ultimately substantiated varies greatly depending on the jurisdiction (2.4% of Chicago Police Department complaints are substantiated⁵¹ compared to 7% for the New York City Civilian Complaint Review Board⁵² and more than 70% for certain smaller Connecticut agencies⁵³). After a complaint is substantiated, an outcome or discipline designation helps stakeholders understand an applicant’s history and determine the extent to which the outcome provides the appropriate accountability for the complaint.

⁵⁰ Rachel Sawicki, “Amended Delaware police-records bill aims to create transparency for public,” *Bay to Bay News*, March 22, 2022, accessed April 26, 2022, <https://baytobaynews.com/delaware/stories/amended-delaware-police-records-bill-aimed-to-create-incredible-opaqueness,74192>.

⁵¹ Citizens Police Data Project, accessed March 22, 2022, <https://data.cpdp.co/data/AG6Ple/citizens-police-data-project>.

⁵² Simon McCormack and Jesse Barber, “Cop Out: Analyzing 20 Years of Records Proving Impunity,” NYCLU ACLU of New York, December 14, 2021, https://www.nyclu.org/sites/default/files/field_documents/nyclu-2021-ccrbdata-report.pdf, 11.

⁵³ Bill Cummings, “Policing the Police.”



What we Found

The databases we analyzed included a wide range of Complaint Statuses. Eight of the 15 databases (including the NDI, NJ Major Discipline Report, and the USA Today Decertified Officer Database) include only instances of substantiated misconduct. A couple of the evaluated databases, specifically the Colorado Peace Officer Standards and Training (POST) and NYPD Member of Service History databases provided insight into the investigations process by publishing those records pending investigation. For example, in Colorado, although the vast majority of records are related to substantiated misconduct, some records are related to ongoing criminal investigations of misconduct that have not been deemed substantiated. In the case of Oregon’s Professional Standards Cases

Database, records of ongoing investigations provide transparency into the disciplinary process.

There are several databases that include not only records of substantiated misconduct, and pending investigations, but also instances where an officer has been cleared or exonerated. For example, the San Francisco CopMonitor database’s inclusion of records of officers who were exonerated from any wrongdoing provides insight into the investigation process and context for why certain actions by officers are in line with department policy.

Misconduct Definition



Description

In this analysis, a database is assessed based on the following criteria:

LEVEL ?	LEVEL 1	LEVEL 2	LEVEL 3
No information or insufficient information available to understand how the database addresses the design element.	Includes voluntary submission by Reporting Agencies that may have differing definitions of misconduct.	Includes mandatory submission by Reporting Agency, or Administrator's reporting, based on a standardized definition of misconduct, of ONLY actions against an officer's license/certification.	Includes mandatory submission by Reporting Agency, or Administrator's reporting, based on a standardized definition of misconduct, of actions against an officer's license/certification and/or records of misconduct that do not result in a license/certification action.

The Misconduct Definition design element refers to how misconduct is defined for the records within a database, whether that definition is consistent for all records included in the database, and whether submission is voluntary or mandatory. In the US, the Department of Justice (DOJ) enforces certain civil and criminal federal misconduct laws that apply to all LEOs, whether employed by a state, county, or local law enforcement agency.⁵⁴ However, the over 18,000 law enforcement agencies in the country are also governed by separate state, local and/or department level laws and policies that further specify what is or is not considered to be misconduct. These laws and policies also determine what discipline is administered for different types of misconduct. For example, regarding officer decertification, Ben Grunwald and John Rappaport found that “all states with decertification authority... can decertify for felony convictions, but only 61% can decertify for failure to meet training or qualification requirements, 57% for general misconduct, 39% for termination for cause, and

⁵⁴ “Addressing Police Misconduct Laws Enforced by the Department of Justice,” The United States Department of Justice, October 13, 2020, <https://www.justice.gov/crt/addressing-police-misconduct-laws-enforced-department-justice>.

11% for any misdemeanor conviction.”⁵⁵ A consistent definition of misconduct for the records within a database helps the user better understand the context around individual records.

All states with decertification authority... can decertify for felony convictions, but only...



For databases that rely on law enforcement agencies submitting records to the database, a consistent definition would also be key to confirming that they know what to submit and what not to submit. Clear parameters are important for both Reporting Agencies and users of the database.

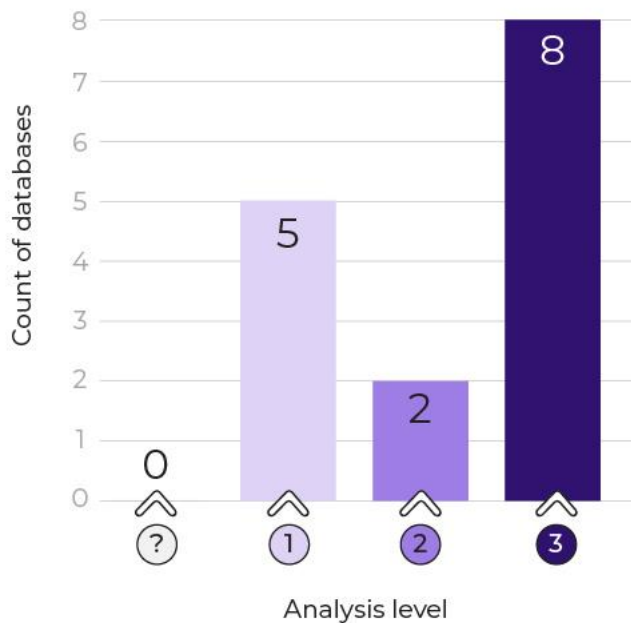
Mandatory reporting is also critical to the standardization of databases. For our analysis, if Reporting Agencies are not required by law to report misconduct to the Administrator of the database, it is considered a “voluntary” database. Where Administrators have to aggregate or collect misconduct records through open records requests or other publicly available sources, we considered such databases as “voluntary.” Voluntary databases risk compromising the integrity and completeness of the data set. Voluntary reporting will likely result in representation of select areas, only. This causes gaps in data coverage and limits users of the database to gain insights and identify trends and patterns in misconduct. Voluntary reporting also requires the Database Administrator to expend resources on open records requests in order to fill in the gaps in coverage and because the data is coming from a third-party, there may be no known controls to verify the accuracy of the reported information.

The Misconduct Definition can also influence the scope of the records collected in the database. Some Administrators only include records that involve an action against an officer’s licensing or certification status within the jurisdiction. Other databases collect a broader set of information including discipline for misconduct that did not result in any action on the officer’s license or certification.

The combination of these three components: standardization of definition, voluntary vs. mandatory submission, and limiting records to licensing and certification actions (or not), drive the transparency and opportunity for accountability within this design element.

⁵⁵ Grunwald and Rappaport, “The Wandering Officer,” 1694.

Misconduct Definition



What we Found

Our analysis of existing databases revealed that the definitions of misconduct are derived from many sources including the Database Administrator’s rules, state Peace Officer Standards and Training (POST) regulations, local law enforcement agencies’ policies and procedures and/or state FOIA laws.

We also found that databases that covered multiple jurisdictions resulted in a less consistent definition of misconduct. For example, the University of Southern California (USC) Police Misconduct Registry (PMR) aggregates records from multiple agencies with differing definitions of misconduct. In the case of the NDI, states voluntarily submit the records. Generally speaking, independently administered databases should be considered “voluntary,” as there

is no government mandate that Reporting Agencies submit records to the administrator. Consequently, there is a strong likelihood for inconsistent definitions of misconduct within the database records. This pattern is to be expected based on the way law enforcement agencies are governed in the US. There will generally be a tradeoff between a broad scope of data and a consistent definition of misconduct. However, even among the databases covering a single law enforcement agency, we found that there is no reliable way to compare data across those databases. This is important as jurisdictions will need to find compromise in how they interpret misconduct data if they are to contribute to a multi-jurisdictional database. For example, when completed, Alabama’s database will include only substantiated complaints that resulted in formal corrective actions related to use of force, while the NYPD Member of Service Histories Database includes any closed complaint under the jurisdiction of the Civilian Complaint Review Board (CCRB).

We identified state-run accountability databases that achieved consistent definitions by limiting the scope of records included in the database. Oregon’s Professional Standards Cases Database, for instance, does not include all complaints of officer misconduct but instead includes only professional standards cases which are all initiated and adjudicated by the state Oregon Department of Public Safety Standards & Training. Users can have confidence that the records in that database are based on consistent rules and policies. However, there is an inherent temptation to find the “lowest common denominator” and exclude important, albeit unique, misconduct data from one or more departments for the benefit of creating a database with a common baseline definition of misconduct.

Regarding the final component of our definition, as to whether the records only are associated with actions against an officer’s license/ certification, we found there to be several databases that use this criteria as the principle driver in what records are included. For

example, the NJ Major Discipline Report only includes records where an officer has been terminated or has had a reduction in rank or grade, and/or suspension of more than five days.

Record Details



Description

For purposes of this analysis, a database is assessed based on the following criteria:

LEVEL	LEVEL	LEVEL	LEVEL
?	1	2	3
No information or insufficient information available to understand how the database addresses the design element.	Records include five or fewer of the 11 identified data fields.	Records include six or more of the 11 identified data fields.	Records include six or more of the 11 identified data fields with primary source documents attached.

Each misconduct record within a database can have data in a wide spectrum of fields. These fields provide stakeholders with information about each individual misconduct record, allowing them to conduct independent analyses. The more fields made available for each record, the more transparency a stakeholder has into the circumstances and outcomes of an individual complaint. While each record will have its own details, Database Administrators can choose to aggregate data for reporting purposes (by misconduct category, agency, outcome, etc.) or to help users navigate the database.

When designing a database, Database Administrators decide whether to include a unique identifier for individual misconduct records and/or for the officers represented in those records. One of the most debated identifiers is an officer's name. Proponents for the inclusion of an officer's name in a misconduct database argue that true accountability cannot be had without visibility into which officers have been the subject of complaints.⁵⁶ This information helps law enforcement hiring agencies (or even employers outside of law enforcement) make informed decisions when evaluating an officer's candidacy.⁵⁷ Attorneys can also use officer names to learn of potentially abusive or unreliable officers (i.e., Brady lists⁵⁸).

⁵⁶ "Promoting Accountability," *Transforming the System*, accessed May 2, 2022, <https://transformingthesystem.org/criminal-justice-policy-solutions/create-fair-and-effective-policing-practices/promoting-accountability/>.

⁵⁷ Stephanie Wykstra, "In Response to Police Misconduct, a Flourishing of Online Databases," *Undark Magazine*, June 5, 2019, <https://undark.org/2019/06/05/police-conduct-databases-eric-garner/>.

⁵⁸ "The Brady List", accessed May 2, 2022, <https://giglio-bradylis.com/brady-offenses>.

Stakeholder Perspective:

“Including officer names in an accountability database could change future behavior, knowing misconduct could be disclosed to future hiring agencies.”

- **Joe Belitzky**, career defense attorney for law enforcement and correctional officers

Conversely, law enforcement unions have argued that exposing officer names in a database can open them up to physical or other harm and are in breach of existing union contracts to shield officer misconduct from public disclosure.⁵⁹ Rather than including officer names, some have recommended using a trackable, unique identifier for each officer (department IDs, badge numbers, etc.).⁶⁰

Other key data fields for misconduct records include the complaint or incident description, category of misconduct, demographic information for both the complainant and officer, outcome of the investigation, and any documentation that provides visibility into both the complaint and outcome.

The collection of demographic data, such as race/ ethnicity, often relies on self-reporting.⁶¹

Data on an officer or complainant’s race, age, gender, and other such data can highlight trends that can indicate bias or discriminatory behavior, a useful finding for any hiring agency or POST board. However, demographic data should not include sensitive information such as addresses, Social Security numbers or phone numbers. It’s also important that demographic data is self-reported and not based on impressions or subjective determinations.

⁵⁹ “Research Basis.” *Nix The Six, a project by Campaign Zero*, accessed April 8, 2022, <https://nixthe6.org/research-basis/>.

⁶⁰ “Fighting Police Abuse: A Community Action Manual,” *American Civil Liberties Union*, accessed April 8, 2022, <https://www.aclu.org/other/fighting-police-abuse-community-action-manual>.

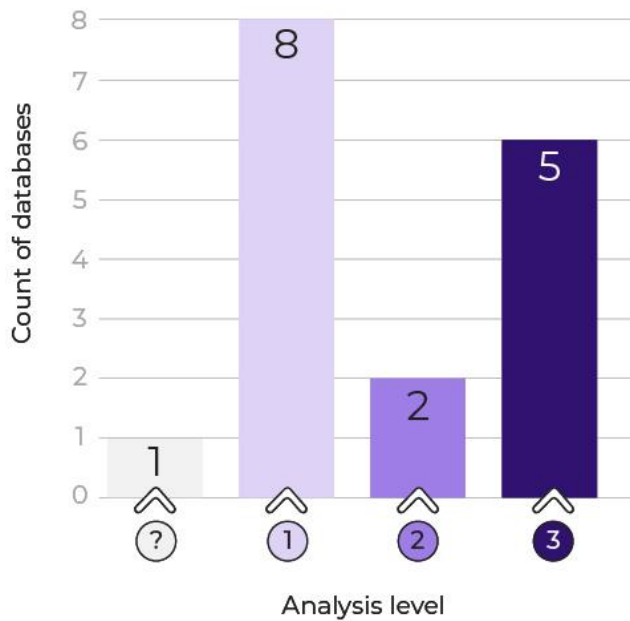
⁶¹ “NYPD Misconduct Complaint Database,” *New York Civil Liberties Union*, May 18, 2021, <https://www.nyclu.org/en/campaigns/nypd-misconduct-database>.

The following data fields are those that are commonly included in accountability databases or included in discussions about officer misconduct. Some databases also attach supporting primary source documents to individual records.

#	Data Field	Purpose
1	Officer name/unique ID	To identify officers with histories of misconduct. In absence of a unique ID, combine officer name with hire date.
2	One or more dates (incident, outcome, case closure, etc.)	To demonstrate the timeliness of investigations
3	Incident category	To identify the type of misconduct that took place
4	Detailed description of incident	To understand what specific misconduct took place
5	Disciplinary outcome/ investigation status	To identify what discipline, if any, was applied for the misconduct or the status of the investigation
6	Agency name	To identify the law enforcement agency a hiring agency or other stakeholder can contact for additional information about that officer
7	Incident location	To identify where misconduct is happening most frequently
8	Complainant demographics (gender, race, age, etc.)	To understand how different community members are impacted by officer misconduct
9	Officer demographics (gender, race, age, etc.)	To understand how different officers are engaging in misconduct
10	Officer rank/role	To understand how misconduct histories affect law enforcement leadership
11	Legal settlement amounts	To identify the cost of officer misconduct for individual jurisdictions and to highlight multiple settlements involving the same officers



Record Details



What we Found

The databases we analyzed did not include a consistent set of data fields for each record. Our definition of an accountability database requires the inclusion of either officer names or unique ID and all the databases in our analysis included names. However, besides officer names and incident categorization, records in different databases generally include different information.

Officer and complainant demographics were rarely included in the databases we analyzed. Only the CPDP included demographic information. No database included legal settlement amounts. Officer rank and location were also rarely included in the databases in our analysis. Of the databases that did include more than six of the identified data elements, two independently administered databases (CPDP and CopMonitor) and three

government databases (Massachusetts, Washington, and Oregon) also provided primary source documents as part of the database.

Access Rights



Description

In this analysis, a database is assessed based on the following criteria:

LEVEL	LEVEL	LEVEL	LEVEL
?	1	2	3
<p>No information or insufficient information available to understand how the database addresses the design element.</p>	<p>Access provided to a single stakeholder (law enforcement, journalists, etc.).</p>	<p>Access provided on a tiered basis to two or more stakeholders, with some stakeholders having more access to information than others.</p>	<p>Full access provided to the public.</p>

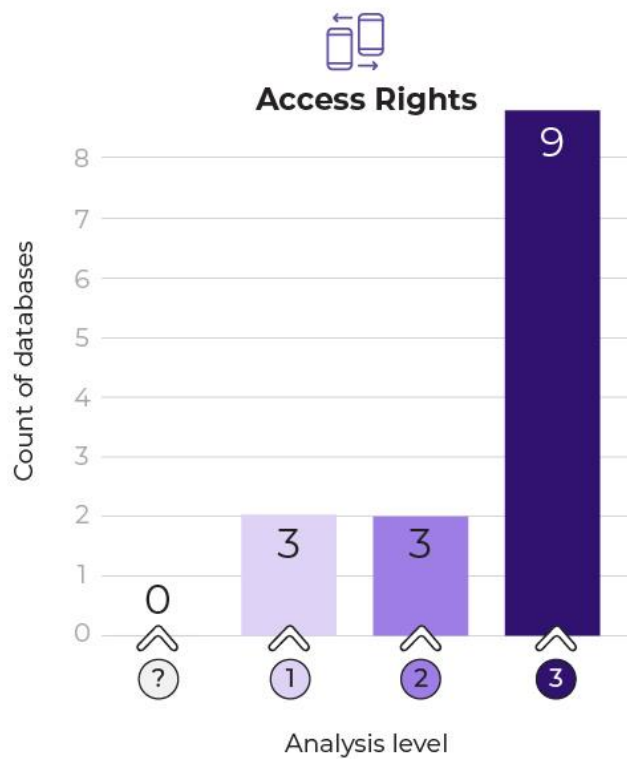
Access to officer misconduct records varies greatly across the US. There is no federal law applying to all 50 states that specifies who can access officer misconduct records. Some states prevent the public from accessing essentially any law enforcement misconduct records, outside of certain litigation contexts. Some states grant the public access to a limited category of misconduct records (e.g., only those involving sustained findings of misconduct) but deny access to most others. As noted, “A minority [of states] make all or a substantial amount of misconduct records presumptively available to anyone who requests them.”⁶² A 2021 Associated Press article revealed that only 15 states have what would be considered public or mostly public law enforcement conduct records. Since the article was published, several states (Colorado’s new rules are set to go into effect in 2023) have modified their record laws to open them up to the public, but the numbers still reveal a general lack of transparency into officer misconduct records.⁶³

⁶² Rachel Moran and Jessica Hodge, “Law Enforcement Perspectives on Public Access to Misconduct Records.” *Cardozo Law Review*, September 28, 2021, 1245.

⁶³ Kallie Cox and William Freivogel, “Police Misconduct Records Secret, Difficult to Access.”

research is necessary to fully understand the implications of misconduct records being accessible to the public.⁶⁶

Accountability databases can exist regardless of a jurisdiction’s laws regarding access to misconduct records. In jurisdictions where misconduct records are not available to the public, accountability databases have been developed with access given only to law enforcement personnel or those specifically tasked with hiring duties. Where misconduct records are available to the public, databases have also been opened to the public, generally through the Administrator’s website. Additionally, Administrators may choose to provide the public access to certain data fields within a database but reserve others for specific stakeholder groups.



What we Found

In our analysis of the 15 LEO accountability databases identified in Appendix B, 12 provide public access to at least some portion of the data. Public access ranges from being limited to certain types of records (e.g., termination or decertification records) to allowing full public access to all complaints. Only the NDI, the Illinois Officer Professional Conduct Database, and the Alabama database limit access to certain law enforcement stakeholders.

Of the databases that do provide some level of public access, there was no single type of database that consistently provided full public access. Both the CPDP and the Oregon Professional Standards Cases Database, for example, provide full public access to the data they collect. The CPDP is an independently administered database covering a single police department while the Oregon database is administered by a

government agency and covers all officers in the state.

⁶⁶ Rachel Moran and Jessica Hodge. “Law Enforcement Perspectives on Public Access to Misconduct Records.”

Audit and Compliance



Description

In this analysis, a database is assessed based on the following criteria:

LEVEL	LEVEL	LEVEL	LEVEL
<p>No information or insufficient information available to understand how the database addresses the design element.</p>	<p>No audits or compliance incentives/disincentives.</p>	<p>Audit <u>or</u> compliance incentives/disincentives.</p>	<p>Audits <u>and</u> compliance incentives/disincentives.</p>

Audits can play a critical role in identifying inaccurate, insufficient, or stale data. As recipients of public money and grants, law enforcement agencies are often audited to confirm that spending complies with the authorized purposes. In the area of law enforcement accountability databases, audits play a critical role in securing accurate and reliable data. For example, with independently administered databases that collect information from multiple sources, such as public record requests, web-scan, there is a possibility of duplicate records. It is incumbent on the administrator and auditor, to ensure that appropriate data validation protocols are applied. Audits also function to evaluate department policies and procedures, performance, and the adequacy of existing controls. In December 2021, a government audit found that although the Oregon Department of Public Safety Standards and Training was responsible for regulating police officers, the state agency had inadequate resources or staff to properly investigate officer conduct and deferred too much to local enforcement agencies.⁶⁷ In San Francisco, the Office of the Controller’s City Services Auditor conducted an audit of how the San Francisco Police Department collected and reported use of force data. The auditor concluded that the department needed “clearer guidance and more proactive governance for better use-of-force data collection and reporting.”⁶⁸

⁶⁷ “Department of Public Safety Standards and Training - Additional Resources Needed to Strengthen Police Training and Accountability” (Oregon Secretary of State, December 2021), <https://www.documentcloud.org/documents/21120922-dpsstaudit>.

⁶⁸ Steve Flaherty and Kat Scoggin, “Use-of-Force Data Audit: the Police Department Needs Clearer Guidance and More Proactive Governance for Better Use-of-Force Data Collection and Reporting,” Office of the Controller, City Services Auditor, October 21, 2020, 1.

Law enforcement agencies also often need incentives (in the form of funding, resources, or other support) to comply with data collection and reporting requirements. Absent adequate financial resources, local and state law enforcement agencies may be unable to secure the technical and infrastructure expertise to report consistent, accurate and reliable information to a central accountability database. A common approach to incentivizing compliance with federal policing mandates is to condition funding under DOJ grant programs, such as the Edward Byrne Memorial Justice Assistance Grant (JAG) or Community Oriented Policing Services (COPS) programs, on a state or local government's compliance with certain standards.⁶⁹

However, the Congressional Research Service raised a concern about the impact of conditioning access to funding from the JAG and COPS programs, when reviewing the compliance components of the proposed George Floyd Justice in Policing Act of 2021: "Depending on the costs of compliance (e.g., whether state and local governments would have to spend money to upgrade their information technology infrastructure or would have to increase staff to process data), there might be a question about whether the JAG program provides enough funding to encourage compliance."⁷⁰

The Congressional Research Service also noted that smaller jurisdictions are particularly at risk for non-compliance with data reporting requirements due to those departments receiving such a small share of the allocated funding from JAG or other federal law enforcement grant programs.

Examples of proposed legislation conditioning federal funding include:

- The George Floyd Justice in Policing Act of 2021, which would require submission of disciplinary data every 180 days to the National Police Misconduct Registry as a condition of receiving JAG funds.⁷¹
- The Cost of Police Misconduct Act of 2021, which would require law enforcement agencies to report information on the costs of judgments or settlements for misconduct claims among other information on allegations of misconduct or be subject to a ten percent reduction of JAG funds.⁷²

⁶⁹ Nathan James, "Policing Reform Legislation: Conditions on Funding and New Authorizations," *Congressional Research Service*, March 11, 2021, 1-2.

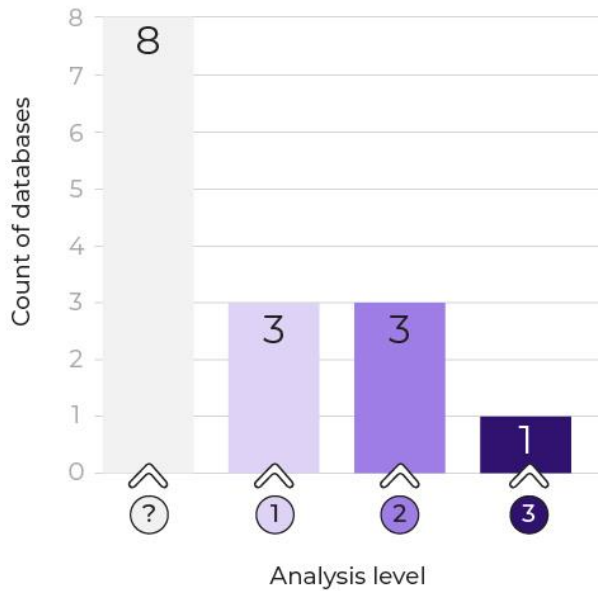
⁷⁰ Nathan James, "Programs to Collect Data on Law Enforcement Activities: Overview and Issues," *Congressional Research Service*, March 11, 2021, 11.

⁷¹ George Floyd Justice in Policing Act of 2021, H.R. 1280, 117th Cong. (2021), section 201(d), 40.

⁷² Cost of Police Misconduct Act of 2021, H.R. 1481, 117th Cong. (2021), section 2(c)(3), 8.



Audit & Compliance



What we Found

Of the 15 databases in our analysis, only the legislation that created the Alabama database provided for both an Audit and Compliance incentive. The Colorado POST Database has a compliance mechanism, and the Invisible Institute conducts an informal audit of the data received from the City of Chicago for the CPDP. For most of the databases in our analysis (eight of 15), no information about audit or compliance mechanisms was available in our research.

Databases administered by independent organizations are generally unable to provide compliance incentives or disincentives since participation is either voluntary (as in the case of the NDI) or the records in the database are gathered through public record requests (as with the CPDP).

Record Retention

Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit and Compliance	Record Retention	Reporting Frequency

Description

In this analysis, a database is assessed based on the following criteria:

LEVEL 	LEVEL 	LEVEL 	LEVEL
No information or insufficient information available to understand how the database addresses the design element.	Ambiguity on what the policy is regarding retaining records in the database.	Definitive period established for retaining records in the database.	Permanent retention of records within the database.

The Record Retention design element refers to how long data is maintained in an accountability database. Individual law enforcement agencies or states generally have policies for how long personnel records (including records of misconduct) are retained, but this design element is specifically about how long records are available in an accountability database. For example, an agency may retain personnel records for ten years but make misconduct records available for only five.



What we Found

Record Retention is a design element that many of the databases in our analysis failed to address in a holistic manner. Of the 15 databases, only the CPDP permanently retained records. Eleven of the 15 databases had ambiguous/ unclear Record Retention policies and Oregon's, Washington's, and Alabama's databases at least provided definitive periods for Record Retention.

Reporting Frequency



Description

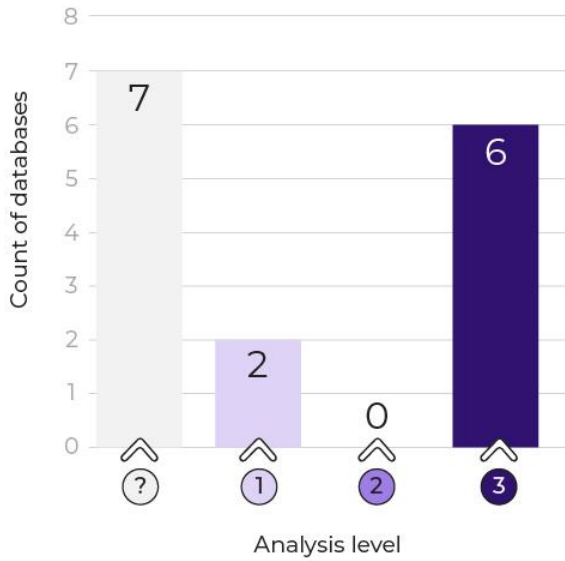
In this analysis, a database is assessed based on the following criteria:

LEVEL	LEVEL	LEVEL	LEVEL
No information or insufficient information available to understand how the database addresses the design element.	Periodic reporting is not done at least semi-annually (>6 months).	Periodic reporting is done at least semi-annually (3-6 months).	Periodic reporting is done at least quarterly (<3 months).

The Reporting Frequency design element refers to how frequently records in a LEO accountability database are added or updated. Updates to a record may come in the form of edits or deletions and can be managed manually or through an automated process such as an application programming interface, where one system queries another system for responses and updates. More frequent record additions and updates may be more administratively burdensome but provide users with confidence that the information in the database is timely and relevant.



Reporting Frequency



What we Found

Similar to Record Retention, very few of the databases in our analysis specify a required Reporting Frequency. The databases in Colorado, Oregon, Alabama, Washington and Massachusetts require the most frequent updates/additions. In our analysis, Reporting Frequency ranges from reporting within two days of receiving a complaint (Massachusetts) to annual reporting (New Jersey Major Discipline Report). Many of the other databases make no mention about how often records are added to or updated in the database. For the databases where a clear Reporting Frequency is identified, the Database Administrator, or in some cases the legislature, sets the guidelines for Reporting Frequency.

Conclusions/Recommendations

Throughout this Report, several trends emerged and stakeholders may glean different insights based on their goals and objectives. Academics, for example, may find more value in the aggregation of existing database practices, while policymakers may seek to identify leading practices from similar size jurisdictions. Additionally, law enforcement officials may recognize the training and hiring value of aggregating and tracking officer misconduct data. Regardless of a particular stakeholder's interests, it's clear that the evaluation of database design elements yields important conclusions that can be leveraged to increase transparency.

Stakeholder Perspective:

“Complete and publicly available data are key to creating meaningful police misconduct registries. Communities have a right to know whether officers, entrusted with protecting the public, have been terminated, resigned for any reason or have a pending investigation against them.

Transparency is the path to building trust and accountability in policing.”

- **David “Troy” Riggs**, Former Public Safety Director, Denver, CO and Former Public Safety Director & Chief of Police, Indianapolis, IN

Databases should collect and report data that would meaningfully inform future evidence-based policymaking on transparency and accountability in policing.

We believe that a meaningful database could be achieved by leveraging leading practices that are already implemented throughout the United States and by taking a pragmatic view on how to effectively reduce harm against community members. We utilized our design element analysis to inform a working model for accountability databases at a national, state or local level.

It should be noted that user experience, training, change management, data security, and other factors can also significantly impact the effectiveness of a database. Each jurisdiction should be prepared to appropriate sufficient funding and lead buy-in efforts across reporting agencies, including considering the assistance of dedicated third parties, for a successful launch and continued operation of the database. Still, we recognize that resource capacity, technical maturity, and prioritization of these considerations may differ across jurisdictions. This Report sets aside such considerations and focuses solely on the

design of a database and the quality of the data collected and maintained.

What follows are our recommendations on each design element and the corresponding assessment level from our analysis methodology.

A Working Model for a Law Enforcement Officer Accountability Database



Complaint Status: Our “Working Model” would include complaints involving allegations that have been Substantiated, Pending Investigation, and Cleared/Exonerated, with levels of tiered access provided to any records not Substantiated. **3**

To provide as much transparency as possible into patterns of officer misconduct reported by law enforcement agencies and citizens, we recommend including all complaints, lawsuits, officer arrests, or records, whether substantiated or not. Given the significant number of misconduct allegations that are not substantiated, or for which investigations are not completed, stakeholders would benefit from understanding the patterns around claims under investigation or where an officer has been cleared or exonerated of misconduct. Data from New York City, for example, shows that the vast majority of complaints have not resulted in Substantiated Misconduct and that most substantiated complaints do not result in any discipline.⁷³ Where discipline is imposed by the oversight agency, the local law enforcement agency may reject the recommendation.⁷⁴ Other New York City data shows that Black officers are more likely to receive serious discipline than white officers.⁷⁵ Available complaints that have not been substantiated can reveal disturbing trends about particular officers, and provide insights on the need for additional training and education. The complaint data can lead to the development of solutions for officer training, discipline, and oversight, along with helping improve a community’s interactions with law enforcement.

Allowing public access to complaints pending investigation or when an officer has been cleared or exonerated of misconduct, however, presents concerns for officers. Officers could face reputational risk by opening access to such complaints. But law enforcement executives and other hiring personnel would benefit from a complete and accurate summary of an applicant’s personnel record. For that reason, our Working Model would provide tiered access to records of Pending Investigation and Cleared/Exonerated cases, enabling law enforcement only to review such records.



Misconduct Definition: Our Working Model would include mandatory submitted records based on a standardized definition of misconduct involving 1) actions taken on an officer’s certification/license including decertification and suspension; and 2) other matters of serious misconduct. **3**

As described in our analysis, the consistency of the definitions of misconduct that apply to records in accountability databases vary widely and depend largely on the jurisdiction covered by the database. A standardized definition of misconduct would help Database Administrators aggregate a consistent data set, enabling law enforcement, policymakers, and other stakeholders to analyze the data and make informed decisions.

While there is a need to find commonality on what constitutes misconduct in order to establish databases across states or at the national level, establishing a common definition across 18,000 law enforcement agencies would be a daunting task. General policing powers are left to the states, with local agencies often setting their own policies and procedures. While definitions may vary, the generalized notion of misconduct means unauthorized or

⁷³ Simon McCormack and Jesse Barber, "Cop Out: Analyzing 20 Years of Records Proving Impunity," 9-10.

⁷⁴ Simon McCormack and Jesse Barber, "Cop Out: Analyzing 20 Years of Records Proving Impunity," 7-8, 10.

⁷⁵ Simon McCormack and Jesse Barber, "Cop Out: Analyzing 20 Years of Records Proving Impunity," 9-10.

inappropriate conduct by an officer against another officer or member of the public while the officer is performing his/her official duties. At the same time, the facts and circumstances that lead to a finding of “inappropriate” or “unauthorized” conduct also vary considerably based on the local agency (and its various oversight structures) making these determinations.

We urge maximizing the utility of a database. Including only voluntarily submitted information reduces the level of standardization of records. In addition, by only including licensing or certification actions, the intersection of the Misconduct Definition and Complaint Status design element loses effectiveness. Some type of egregious conduct would have to occur in order to trigger decertification of an officer. Tracking such decertifications in a database is helpful to address preventing problematic officers from getting hired by another agency. But such decertification-only databases do little to prevent police misconduct from occurring in the first place. Collection of broad categories of disciplinary action (those not resulting in decertification) and matters pending investigation would help alert law enforcement executives to officers at risk for misconduct and their need for additional training and education.

Due to the local nature of policing, we recommend that a Working Model establish standardized categories and outcomes of misconduct that should be collected in each database. A mandatory floor of “misconduct types” would enable analysis and comparisons of discipline practices and outcomes across law enforcement agencies. We propose the following nine categories and outcomes of misconduct, at a minimum, be included regardless of how individual law enforcement agencies define each category of misconduct. This recommendation is based on how frequently these categories were used in the databases included in Appendix B:

- Dishonesty
- Excessive Force
- Sexual Misconduct
- Unlawful Search & Seizure
- False or Wrongful Arrest
- Failure to Intervene
- Resignations during misconduct investigations
- Terminations
- Decertifications



Record Details: Our Working Model would report a minimum of six data fields to enable quality and efficient analytics. **2**

We recommend establishing a baseline of required information to be included for each record reported into the database to 1) standardize the types of background information available for each incident, and 2) eliminate the cost and burden of obtaining additional information through FOIA requests or follow up with the local agencies. The more information provided upfront, the easier stakeholders can determine which officer behaviors or law enforcement agency policing practices are possible concerns. The databases in our analysis contained a variety of data fields for each record. Our analysis methodology identified 11 key data fields, and databases reporting on at least six of those fields provided more meaningful background on the incident. Those six fields are as follows:

- Officer name/unique ID: Prompts accountability and acts as a unique identifier across other jurisdictional data sources
- One or more dates (incident, outcome, case closure, etc.): Brings specificity to the incident as a differentiator from other potentially similar incidents
- Incident category: For purposes of easily categorizing data
- Detailed description of incident: Brings additional context to the incident that sheds light on the allegation
- Disciplinary outcome/ investigation status: Shows where in the investigative process a complaint may be as well as the final disposition of the complaint
- Complainant demographics (gender, race, age, etc.): Provides opportunity for analysis in determining any bias in the conduct / misconduct of an officer.

These data fields can be gathered as part of a complaint form, internal investigation, or legal case, and as such, would not require significant effort to collect. Any database that contains more fields in addition to these six would create additional transparency and provide opportunities for advanced analytics identifying trends and correlations among data fields.

Lastly, some data fields should make users choose from predefined values with standardized definitions for each option to enable consistent data collection, reporting and analysis. If left undefined, fields such as disciplinary outcome/ investigation status and incident category could contain vastly different information depending on who entered the data. The goal would be to provide clear guidance to the Reporting Agency on what facts and circumstances should be used to complete each field.



Access Rights: Our Working Model would provide levels of tiered access, allowing some stakeholders increased access to select information. **2**

Accountability databases should provide some level of free, public, and online access to officer misconduct information. Access to officer misconduct records has been a longstanding controversy, with law enforcement unions often claiming that public access would jeopardize the privacy and physical safety of the officers.⁷⁶ Academics who surveyed the effects of public access,⁷⁷ however, found that officer harm does not necessarily ensue from granting access to misconduct records. Among the 15 databases analyzed in Appendix B, 12 granted some level of access to the public, ranging from a list of decertified or terminated officers to background on the incident, name of the officer, and the disciplinary outcome/ investigation status. To balance the perceived safety issues raised by officers with the public interest in identifying problematic officers, databases should redact sensitive personal information. Databases could also include commendations, awards, and other forms of recognition as part of the officer's record in the database.

Most importantly, public access could present an opportunity to change policing culture. Culture drives behavior and changing police culture is highly challenging.⁷⁸ A lack of transparency and accountability fuels the "organizational structure and culture of policing."⁷⁹ If officer misconduct records were made publicly available, this disclosure might incentivize

⁷⁶ Rachel Moran and Jessica Hodge, "Law Enforcement Perspectives on Public Access to Misconduct Records", 1238-39.


⁷⁷ Rachel Moran and Jessica Hodge, "Law Enforcement Perspectives on Public Access to Misconduct Records," 1240.

⁷⁸ Jane Miller and Rashawn Ray, "Highlights: Improving Police Culture in America," *Brookings in America*, November 4, 2019, <https://www.brookings.edu/blog/up-front/2019/11/04/highlights-improving-police-culture-in-america/>.

⁷⁹ Jane Miller and Rashawn Ray, "Highlights: Improving Police Culture in America."

officers to engage with community members differently and follow department use of force and other policies to avoid reputational harm.

We recommend an access model that grants data rights appropriate for the stakeholder group's interests. Under this model, law enforcement involved in hiring and misconduct investigations may have access to more detailed information. The public, including advocacy/research groups, would have the right to review, at a minimum, the elements reported in Record Details to inform pattern analysis and policy advocacy.

 **Audit and Compliance:** Our Working Model would be regularly audited and provide adequate incentives for compliance. **3**

To be useful, the information in a database should be current, accurate, and complete. Our Working Model would have both Audit and Compliance mechanisms to help confirm that the data in the database remains useful to all stakeholders.

The Database Administrator should perform periodic audits of the data in the database to identify missing, inaccurate, or incomplete records. Depending on how records originally get entered into a database, the Database Administrator may need to audit its own records or audit a sample of records from Reporting Agencies. These audits will also inform a Database Administrator of an individual Reporting Agency's compliance with any reporting requirements.

In addition to audits, Reporting Agencies should be incentivized to submit compliant data to the Database Administrator. One key to compliance is appropriating adequate funding from state and/or federal sources. Conditioning government grants on compliance with database requirements can be effective if meaningful dollar amounts are involved. As part of a meaningful compliance framework, we recommend both incentives and disincentives. Agencies should be provided access to grants (to support the data reporting requirements) and be restricted from applying for future grants where there is sustained noncompliance.

Finally, in order to increase departmental accountability, we recommend that the head of each Reporting Agency annually certify to the Database Administrator that the Reporting Agency complied with all the data submission requirements.

 **Record Retention:** Our Working Model would establish a definitive period for retaining records in the database. **2**

Data retention policies are foundational for data management and governance. Database Administrators should clearly disclose the number of years that misconduct records are to be maintained, what types of data are included in the data retention policy and whether records will be archived (i.e., not viewable in the database but available for accessing through other means, such as FOIA). Because all data in an accountability database is so valuable, permanent deletion of records is highly discouraged.

Stakeholders have a need to review misconduct records to help determine an officer's credibility for trial, post-conviction relief (which can continue for years) and research. Hiring agencies also have a need to access historical discipline records of candidates, which may extend well beyond the common seven-year lookback period for background checks. Community organizations may also seek to evaluate lengthier periods of citizen interactions to see if there are any instances of misconduct that could influence current behavior.



Reporting Frequency: Our Working Model would require regularly scheduled reporting at a minimum interval of every three to six months. **2**

Misconduct records should be regularly updated so that accurate and complete information is available for users of the database. Adding new allegations and updating disciplinary outcomes/ investigation status for existing records is critical so that timely information is available to law enforcement agencies to use in their hiring processes and for other stakeholders to use in monitoring law enforcement practices or preparing cases for trial. Stale information undermines the credibility and quality of any database and can adversely impact decision making by law enforcement and other stakeholders. While the need for real-time data is important, achieving that goal would require significant resources. There needs to be a balance between the administrative burden of updating and submitting data and the goal of providing end users of a database current data.

The Working Model would establish a minimum reporting schedule of every three to six months. An iterative process could also be established when an increased Reporting Frequency is required following the initial creation of a database. Reporting Agencies may need to undergo considerable administrative changes when the database is created including data cleansing, digitizing paper records, creating new data fields, and establishing an electronic information exchange between the Reporting Agency and the Database Administrator. Once those processes are in place, regularly submitting misconduct records to a database should not be an overly burdensome process.

Future law enforcement reform

In the absence of a nationwide LEO accountability database, stakeholders should continue to compile and share misconduct information, even while knowing it may not paint a complete picture.

In lieu of a nationwide LEO accountability database and supplemental to existing efforts by local governments, many journalists, advocacy groups and other public safety professionals have used publicly accessible data (gathered from news outlets or through FOIA requests) to create their own databases and conduct their own analyses of misconduct in their respective jurisdictions (e.g., the CPDP in Chicago). Equipped with that data, analysts have been able to generate important insights into officer misconduct. For example, using the CPDP data, analysis found that fewer than 4% of Chicago police officers were responsible for 25% of use-of-force complaints, city payouts, and police shootings, as well as a disproportionate amount of the complaints generated by and arrests of Black and Hispanic civilians.⁸⁰ Stakeholders should continue to build out these databases across jurisdictions, using common data structures and technology platforms where possible.

Additional research is needed to measure the impact of accountability databases. Those who accept this call to action should collaborate and share their findings.

As mentioned earlier, we believe that funding for the creation, adoption and operation of a database is critical. However, the rationale for implementing such a significant operational change or making a large capital expenditure will typically be evaluated based on the return for the investment (across all resources). To date, it is especially difficult to quantify the

⁸⁰ Akshay Jain, Rajiv Sinclair, Andrew Papachristos, "Identifying misconduct-committing officer crews in the Chicago Police Department." *PLOS ONE*. Retrieved May 12, 2022, <https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0267217>

impact of databases. Further academic research is needed to understand how effective databases have been in 1) preventing wandering officers from securing employment, 2) reducing incidents of misconduct that result in trauma, physical injury, death or costly municipal settlements and 3) providing data that various organizations (e.g., community and advocacy organizations and law enforcement agencies) can use to develop solutions to curb future misconduct.

Accountability databases are one key element in changing inappropriate officer conduct. Stakeholders should continue efforts to find compromise and alignment on other reforms that will contribute to transparency and accountability.

Advancing accountability databases is just one method for bringing about necessary reform. Investing in community-based initiatives along with intra-law enforcement racial bias training, mental health situational awareness and de-escalation training are just a few examples of the actions an agency can take to limit future misconduct and protect the lives and well-being of Black Americans. Continued evaluation of legal constructs such as qualified immunity, FOIA exceptions and collective bargaining agreements can also have an impact on transparency and accountability. But, as we have seen with the stalling of several prominent omnibus bills, including too many reform issues into a single bill can undermine the compromise found on specific issues. There is broad alignment on the premise of an accountability database across the law enforcement community,⁸¹ reform advocacy groups⁸² and the business community.⁸³ As such, we should accelerate momentum to find compromise across these seven design elements and communicate that alignment to policymakers immediately.

Disclaimer: *The analysis of individual databases was based on publicly available information obtained through online sources. Where information was not available or could not be clearly discerned, we documented the matter with a question mark (?).*

Engage with Us: *We are releasing the database analysis as a working draft for the public's review. In addition, we appreciate any feedback regarding our proposed framework and recommendations in the hopes that future iterations will incorporate more comprehensive input from all stakeholders. Share your comments, questions or interest in collaboration by reaching out to leta@ceoactionracialequity.com*

⁸¹ "Research," The Lewis Registry, accessed August 1, 2022, <https://www.thelewisregistry.org/research>, Civic Pulse Survey Results.

⁸² "NYCLU expands NYPD misconduct database with new CCRB Data," *New York Civil Liberties Union*, May 3, 2021, retrieved April 26, 2022, <https://www.nyclu.org/en/press-releases/nyclu-expands-nypd-misconduct-database-new-ccrb-data>.

⁸³ "Police reform," Business Roundtable, accessed April 26, 2022, <https://www.businessroundtable.org/policereform>.

Appendix A: Law Enforcement Officer Accountability Database Matrix

This appendix contains a list of the law enforcement officer accountability databases that we have encountered in our research. This is by no means an exhaustive list of all law enforcement officer accountability databases that exist in the United States but is a helpful tool to understand the breadth and diversity of databases.

#	Database Name	Jurisdiction Name	Jurisdiction Type			Administrator	
			National	State	Municipal	Independent	Government
Databases Analyzed in Appendix A							
Active Databases							
1	Chicago Citizens Police Data Project (CPDP)	Chicago Police Department (Illinois)			X	X	
2	Colorado Peace Officer Standards and Training (POST) Database	Colorado		X			X
3	CopMonitor SE	San Francisco, CA			X		X
4	Illinois Officer Professional Conduct Database	Illinois		X			X
5	National Decertification Index (NDI)	US	X			X	
6	New Jersey Major Discipline Report	New Jersey		X			X
7	NYPD Member of Service History Database	New York City Police Department (NYPD)			X		X

#	Database Name	Jurisdiction Name	Jurisdiction Type			Administrator	
			National	State	Municipal	Independent	Government
8	Oregon Department of Public Safety Standards & Training (DPSST) Professional Standards Cases Database	Oregon		X			X
9	University of Southern California (USC) Police Misconduct Registry (PMR)	US	X			X	
10	USA Today Decertified Officer Database	US	X			X	
11	Washington Certification Database	Washington		X			X
Recently Authorized Databases Under Development							
12	Alabama	Alabama		X			X
13	Massachusetts	Massachusetts		X			X
14	National Law Enforcement Accountability Database	US	X				X
15	North Carolina Officer Search: Revocation/Suspension Data	North Carolina		X			X
Other Databases							
16	ACLU MA Police Violence Happens Here Database	Massachusetts		X		X	
17	Beacon Police Department Complaints	Beacon Police Department (New York)			X		X
18	CAPSTAT NYC Federal Civil Rights Lawsuit Data	NYPD			X	X	

#	Database Name	Jurisdiction Name	Jurisdiction Type			Administrator	
			National	State	Municipal	Independent	Government
19	Chicago COPA	Chicago Police Department (Illinois)			X		X
20	Chicago Police Board Info Center	Chicago Police Department (Illinois)			X	X	
21	Connecticut Decertified Officers List	Connecticut		X			X
22	Democrat & Chronicle New York State Police Disciplinary Records	New York		X		X	
23	Florida Criminal Justice Standards & Training Commission Quarterly Update Newsletter	Florida		X			X
24	Giglio Brady List	US	X			X	
25	Gothamist Brooklyn District Attorney Letters	NYPD - criminal investigations in Brooklyn			X	X	
26	Henry A. Wallace Police Crime Database	US	X			X	
27	Honolulu PD Disciplinary Report	Honolulu Police Department			X		X
28	Idaho POST Decertification Search	Idaho		X			X
29	Indiana Certificate Revocations List	Indiana		X			X

#	Database Name	Jurisdiction Name	Jurisdiction Type			Administrator	
			National	State	Municipal	Independent	Government
30	Kansas Certification Actions & Proceedings	Kansas		X			X
31	Middlesex County District Attorney's Brady List	Middlesex County (Massachusetts)			X	X	
32	Minnesota Peace Officer License Revocations	Minnesota		X			X
33	Muckrock Misconduct and Disciplinary Materials FOIL Requests	New York			X		X
34	NACDL Full Disclosure Project	US	X			X	
35	Norfolk County Brady List	Norfolk County (Massachusetts)			X		X
36	NY State Division of Criminal Justice Police and Peace Officer Decertification List	New York		X			X
37	NYCLU NYPD Misconduct Complaint Database	NYPD			X	X	
38	NYPD Officer Profile	NYPD			X		X
39	Officer Complaint History Search	Minneapolis Police Department (Minnesota)		X			X
40	Open Police.org	US	X			X	
41	ProPublica NYPD Files	NYPD			X	X	

#	Database Name	Jurisdiction Name	Jurisdiction Type			Administrator	
			National	State	Municipal	Independent	Government
42	Rochester Police Department Discipline Database	Rochester Police Department (New York)			X		X
43	Suffolk County District Attorney's Brady List	Suffolk County (Massachusetts)			X		X
44	The Problematic	Los Angeles County Sheriff's Department (California)			X	X	
45	Utica Police Department Personnel Records	Utica Police Department (New York)			X		X
46	Vermont List of Decertified Law Enforcement Officers	Vermont		X			X
47	Woke Windows Project	Boston Police Department (Massachusetts)			X	X	
48	Wyoming Peace Officer Standards and Training – Certification Actions	Wyoming		X			X

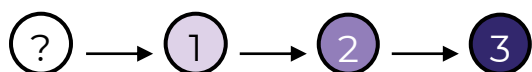
Appendix B: Database Analyses

Introduction

This appendix contains analyses of individual LEO accountability databases against the Design Framework. We have analyzed 11 active databases and have also provided comments on four databases that are soon to be created (“Under Development”) based on either a Presidential Executive Order or recently passed state legislation. These analyses are intended to demonstrate how the Design Framework can be used to better understand individual databases and provide common language to use in discussing and/or developing databases.

In selecting databases for analysis, we aimed to choose a diverse set that includes data covering different jurisdiction levels (national, state, municipal) and that are administered by both governments and independent/private organizations.

We applied our framework to evaluate each of these databases, using our Analysis Methodology. As indicated, we use a consistent scale to assess how that database approaches each of the design elements. The analysis of individual databases was based on publicly available information obtained through online sources. Where information was not available or could not be clearly discerned, we documented the matter with a question mark (?).



A “?” indicates that there is either no information or there is insufficient information available to understand how a database addresses a specific design element. Using the Reporting Frequency design element as an example, a database would be assessed as a “?” if there was no public information about how often records were added to or updated in the database. Levels 1 through 3 are defined for each design element in the following section of this Report.

Our goal is to analyze each database under a common framework that can be applied for consistent analysis. It is not to rank or judge the database’s effectiveness. We recognize that each database is designed with certain end goals in mind and within certain regulatory and legal environments. These factors need to be considered in reviewing the analyses. This framework is a tool for understanding databases, but it’s not intended to identify which databases are “leading” examples. Readers, based on their individual needs, will be able to use the framework to identify elements among databases that are of most interest to them and help to ground policy discussions with a diverse set of stakeholders

We are releasing the database analysis as a working draft for the public’s review. In addition, we appreciate any feedback regarding our proposed framework and recommendations in the hopes that future iterations will incorporate more comprehensive input from all stakeholders. Share your comments, questions or interest in collaboration by reaching out to leta@ceoactionracialequity.com.

Active Databases

1. Chicago Citizens Police Data Project
2. Colorado Peace Officer Standards and Training (POST) Database
3. CopMonitor SF

4. Illinois Officer Professional Conduct Database and Law Enforcement Training and Standards Board (ILETSB) Officer Lookup Database
5. National Decertification Index (NDI)
6. New Jersey Major Discipline Report
7. NYPD Member of Service History Database
8. Oregon Department of Public Safety Standards & Training (DPSST) Professional Standards Cases Database
9. University of Southern California (USC) Police Misconduct Registry (PMR)
10. USA Today Decertified Officer Database
11. Washington Certification Database

Recently Authorized Databases Under Development

12. Alabama
13. Massachusetts
14. National Law Enforcement Accountability Database
15. North Carolina Officer Search: Revocation/Suspension Data

Active Databases

#	Database	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
1	Chicago Citizens Police Data Project	3	1	3	3	2	3	1
2	Colorado Peace Officer Standards and Training (POST) Database	2	3	1	3	2	1	3
3	CopMonitor SF	3	1	3	3	?	?	?
4	Illinois Officer Professional Conduct Database	1	3	2	1	?	1	?
5	National Decertification Index (NDI)	1	1	1	1	1	1	?
6	New Jersey Major Discipline Report	1	2	1	3	?	1	1
7	NYPD Member of Service History Database	2	3	1	3	1	1	?
8	Oregon Department of Public Safety Standards & Training (DPSST) Professional Standards Cases Database	3	3	3	3	?	2	3
9	University of Southern California (USC) Police Misconduct Registry (PMR)	1	1	2	2	?	?	?
10	USA Today Decertified Officer Database	1	1	1	3	?	?	?
11	Washington Certification Database	3	3	3	3	1	2	3

Recently Authorized Databases Under Development

#	Database	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
12	Alabama	1	3	1	1	3	2	3
13	Massachusetts	3	3	3	2	?	?	3
14	National Law Enforcement Accountability Database	1	3	?	2	2	?	3
15	North Carolina Officer Search: Revocation/Suspension Data	1	2	1	3	?	?	?

Active Databases

1. Chicago Citizens Police Data Project

Background

“The Citizens Police Data Project (CPDP) takes records of police interactions with the public – records that would otherwise be buried in internal databases – and opens them up to make the data useful to the public, creating a permanent record for every [Chicago Police Department] officer.”⁸⁴

The CPDP is not an official government website but is the work of the Invisible Institute. The Invisible Institute was created to support ordinary persons in the Chicago area in their quest to bring accountability to public institutions. Using information gathered through lawsuits and FOIA requests,⁸⁵ the CPDP takes misconduct data directly from the city of Chicago and makes it available to the public. The CPDP data is structured in a way that creates profiles of active and former Chicago police department (PD) officers. The Columbia Chronical reported that “since its launch in 2015, the CPDP has been used more than 1.2 million times by users who have used it to download 88,000 case documents.”⁸⁶

The CPDP includes a substantial amount of information on each officer, including awards, promotions, honorable mentions and transfers in addition to use-of-force reports and misconduct complaints.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the CPDP against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
Chicago Citizens Police Data Project	3	1	3	3	2	3	1

Analysis

1. Complaint Status: 3

The CPDP includes both substantiated and complaints against Chicago PD officers that have not been substantiated. The types of misconduct included in the database include conduct unbecoming (off duty), criminal misconduct, domestic lockup procedures, operation/personnel violations, supervisory responsibilities, traffic, verbal abuse, use of force, drug/alcohol abuse, bribery/official corruption and illegal search.⁸⁷ The CPDP also includes

⁸⁴ “Citizens Police Data Project,” Invisible Institute, accessed October 25, 2022, <https://invisible.institute/police-data/>.

⁸⁵ “Where does the data come from? Who is doing this and why?” CPDP (Invisible Institute), accessed October 25, 2022, <http://how.cdpd.works/en/articles/1889786-where-does-the-data-come-from-who-is-doing-this-and-why>.

⁸⁶ Isaiah Colbert, “Invisible Institute’s Database Makes Police Department Records Accessible to Citizens,” *The Columbia Chronicle*, June 10, 2021, <https://columbiachronicle.com/invisible-institutes-database-makes-police-department-records-accessible-to-citizens>.

⁸⁷ “Search,” CPDP, accessed October 25, 2022, <https://cpdp.co/search/>.

investigative files known as “complaint registers” containing the full record of investigations undertaken in response to complaints.⁸⁸

2. Misconduct Definition: 1

The CPDP gathers information on misconduct complaints to the Chicago PD. Because this is an independently administered database, we consider the submission/ collection to be voluntary. All records in the database are based on the department’s policies and definitions of misconduct. The CPDP contains several categories of misconduct including a definition of what each category represents. The definitions exist in a glossary section, which also places each infraction or term into color-coded categories.

3. Record Details: 3

Each record in the database includes multiple data fields. These fields include the officer’s name, officer and complainant demographics, date and location of the incident, and the officer’s tenure as a peace officer. The race demographics are in line with those that are used by the Integrated Postsecondary Education Data System.⁸⁹

The results of the complaints are listed as administrative termination, disciplined 1-9 days, disciplined 10-30 days, disciplined 30+ days, exonerated, no affidavit, no cooperation, no discipline, not sustained, reprimand, penalty not served, reinstated by Police Board, resigned, sustained, open, unsustained, unfounded, violation noted, and no action taken.⁹⁰

4. Access Rights: 3

The full database is publicly accessible.

5. Audit and Compliance: 2

The CPDP is administered by the Invisible Institute using information gathered through lawsuits and FOIA requests. The Invisible Institute publishes “the city’s records without alteration, except for minor typos and spelling errors. As we identify information needs and develop new sources, we also develop internal protocols for ensuring the integrity of the data we publish”.⁹¹ As the Invisible Institute discovers errors in the data, it contacts the city for corrections, which are then updated in the CPDP.⁹² This review serves as an informal audit process.

Regarding compliance incentives, the Invisible Institute is an independent organization and does not rely on participation from the Chicago PD. The data in the CPDP is sourced through public records requests.

6. Record Retention: 3

The information in the CPDP is maintained indefinitely and the underlying data set is also available for download.

⁸⁸ Kalven, J. (2018, August 16). Invisible Institute relaunches the Citizens Police Data Project. *The Intercept*. Retrieved October 31, 2022, from <https://theintercept.com/2018/08/16/invisible-institute-chicago-police-data/>

⁸⁹ “Changes to Race/Ethnicity Reporting to IPEDS,” *The Integrated Postsecondary Education Data System*, accessed October 25, 2022, <https://nces.ed.gov/ipeds/report-your-data/race-ethnicity-reporting-changes>.

⁹⁰ “Search,” CPDP.

⁹¹ “How Accurate Is the Data?” CPDP (Invisible Institute), accessed October 25, 2022, <http://how.cdpd.works/en/articles/1889781-how-accurate-is-the-data>.

⁹² “Why is this information imperfect?” CPDP (Invisible Institute), accessed October 25, 2022, <http://how.cdpd.works/en/articles/1889809-why-is-this-information-imperfect>.

7. Reporting Frequency: 1

The data in the CPDP spans from 1988 to 2018 and the Invisible Institute “regularly request[s] updates to [the] existing dataset from the City of Chicago.”⁹³ For purposes of this analysis, “regularly” requested was assumed to refer to at least annually. The Invisible Institute also makes updates to the CPDP as inaccurate data is found.

⁹³ “How Current Is the Data?” CPDP (Invisible Institute), accessed October 25, 2022, <http://how.cpdp.works/en/articles/1889777-how-current-is-the-data>.

2. Colorado Peace Officer Standards and Training (POST) Database

Background

The Colorado POST Board’s Peace Officer Database⁹⁴ launched on January 2, 2022. The public database is administered by the Colorado POST Board⁹⁵ and was created through law enforcement accountability legislation enacted by the Colorado General Assembly and signed by the Governor in 2020⁹⁶ and 2021⁹⁷. The legislation, enacted following the law that opened public access to Colorado peace officer internal investigation records⁹⁸, mandates all Colorado law enforcement agencies to submit records to POST for inclusion in the database. The Peace Officer Database contains reports of untruthfulness, repeated failure to follow POST board training requirements, certification revocation, termination for cause, being the subject of a criminal investigation that could result in revocation or termination, and credibility disclosure actions⁹⁹.

In addition to creating the Peace Officer Database, the law requires that beginning on July 1, 2023, POST must publish an annual report, aggregating, by department, information on all use of force instances, all instances of officers resigning while under investigation, all contacts conducted by officers, and data relating to use of unannounced entry by an officer. It is unclear if that aggregated information will also be included in the public-facing database.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the Colorado POST Database against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
Colorado POST Database	2	3	1	3	2	1	3

Analysis

1. Complaint Status: 2

The Peace Officer Database includes outcome-oriented actions (e.g., decertifications, terminations, and resignations) and other issues that may affect the officer’s credibility or certification status. Although the vast majority of records are related to substantiated misconduct, some records are related to ongoing criminal investigations of misconduct that have not been deemed substantiated. The database does not include actions for which an officer has been exonerated or cleared.

⁹⁴ Peace Officer Database, Colorado Attorney General, accessed October 26, 2022, <https://post.coag.gov/s/>.

⁹⁵ “Home,” Colorado Peace Officer Standards and Training, accessed October 26, 2022, <https://post.colorado.gov/>.

⁹⁶ “Enhance Law Enforcement Integrity,” Colorado General Assembly, June 13, 2020, accessed October 27, 2022, <https://leg.colorado.gov/bills/sb20-217>.

⁹⁷ “Measures to Address Law Enforcement Accountability,” Colorado General Assembly, June 8, 2021, accessed October 26, 2022, <https://leg.colorado.gov/bills/hb21-1250>.

⁹⁸ “Peace Officer Internal Investigation Open Records,” Colorado General Assembly, March 27, 2019, accessed October 26, 2022, <https://leg.colorado.gov/bills/hb19-1119>.

⁹⁹ Colo. Rev. Stat. § 24-31-303(1)(r)

2. Misconduct Definition: 3

Law enforcement agencies are required to submit the following information related to credibility and certification to the POST database:¹⁰⁰

- Untruthfulness.
- Three or more failures to follow POST board training requirements within ten consecutive years.
- Revocation of the certification by the POST board, including the basis for the revocation.
- Termination for cause unless the termination is overturned or reversed by an appellate process.
- Resignation or retirement while under investigation by the peace officer's employing law enforcement agency, a district attorney, or the attorney general that could result in being entered into the database
- Resignation or retirement following an incident that leads to the opening of an investigation within six months following the peace officer's resignation or retirement that could result in being entered into the database.
- Being the subject of a criminal investigation for a crime that could result in revocation or suspension of certification.
- Credibility disclosure information reported by prosecutors that could impact an officer's credibility as a witness in court.

This creates a standardized definition of misconduct, that includes, but is not limited to, all actions that result in an officer's decertification. In addition, under Colorado Revised Statutes § 24-31-305, POST is responsible for revoking the certification of a peace officer convicted of a felony or certain misdemeanors.¹⁰¹ That results in the administering agency being directly responsible for setting the standards and definition for records to be included in the database.

3. Record Details: 1

The database includes, at a minimum, officer names and ID numbers; a high-level description of the action, which could include an outcome; date; and the agency employing the officer. Some actions include additional information, such as charge level, court details, and sentencing data. The database does not include any information about complainants, demographic information or officer rank.

4. Access Rights: 3

It appears that the public has access to all the information available on the database website. The public database is designed such that requesters must search for specific officers, or actions and does not allow an aggregate download. The database does provide aggregate charts by year, decertification type, and employing agency.

While reporting agencies are required to provide the underlying details of a misconduct case, even when an officer has been cleared of misconduct, that information is available only to law enforcement outside of the database.

5. Audit and Compliance: 2

It is unclear whether the POST conducts a formal audit of the information in the database. The database does include a disclaimer that states that, "While POST Board uses reasonable efforts to include accurate and up to date information, POST Board cannot guarantee that

¹⁰⁰ Ibid.

¹⁰¹ "Disqualifying Incidents," Colorado Peace Officer Standards and Training, accessed April 26, 2022, <https://post.colorado.gov/disqualifying-incidents>.

the information found here is accurate and up to date. POST Board makes no warranties as to the accuracy of the content and assumes no liability or responsibility for an error or omission in the content."¹⁰² Regarding compliance incentives, POST has the authority to fine any agency that fails to meet its reporting requirements.¹⁰³

6. Record Retention: 1

Individual law enforcement agencies in Colorado have varying retention periods for internal affairs records. For example, the Colorado State University police force¹⁰⁴ permanently retains their internal investigation records while the Colorado Municipal Records Retention Schedule¹⁰⁵ has a period of five years. However, there is no explicit language available on the POST site regarding how long records are retained in the Peace Officer Database.

7. Reporting Frequency: 3

"The Colorado POST staff updates the information in the database at least monthly and uses reasonable efforts to include accurate and up-to-date data."¹⁰⁶

¹⁰² Peace Officer Database, Colorado Attorney General.

¹⁰³ Colo. Rev. Stat. § 24-31-303(1)(r)(II)

¹⁰⁴ "Retention Schedule," Colorado State University Police Department, accessed October 27, 2022, https://police.colostate.edu/wp-content/uploads/sites/85/2021/07/808-Retention_Schedule.pdf, 12

¹⁰⁵ "Schedule No. 100 Public Safety Records," Colorado State Archives, accessed October 27, 2022, https://drive.google.com/file/d/1-iY-7pkQU6_LIbRZbrJKdzqCdTG2vrhf/view, 100-8.

¹⁰⁶ "New state database launched to provide public transparency on peace officer certification, training compliance, and misconduct," Colorado Attorney General, January 2, 2022, accessed October 27, 2022, <https://coag.gov/press-releases/post-database-launched-1-2-22/>.

3. CopMonitor SF

Background

In November 2020, the Integrity Unit of the San Francisco Public Defender's Office (Public Defender's Office) launched CopMonitor SF, a database designed to provide public access to LEO complaints and misconduct records.¹⁰⁷ The database collects information about police, sheriffs and other law enforcement personnel in San Francisco. The database contains records of certain types of misconduct complaints, both substantiated and not, that have been obtained from public records requests, media coverage, civil lawsuits, records of officer arrests, prosecution or convictions and complaints filed with the San Francisco Department of Police Accountability.¹⁰⁸ Prior to 2019, officer personnel records were highly confidential in California. With the passage of California Senate Bill 1421, the law was amended to allow the release of records relating to incidents involving officer use of a firearm, use-of-force resulting in death or serious bodily injury and sustained allegations of sexual assault or dishonesty.¹⁰⁹ Following the enactment of SB 1421, the Public Defender's Office Integrity Unit filed requests for information about complaints made with the San Francisco Department of Police Accountability, San Francisco Police Commission, San Francisco Sheriff's Office, California Highway Patrol, San Francisco District Attorney's Office and BART Police.¹¹⁰ After receiving information from the public safety agencies, the Integrity Unit supplemented that data with media reports and other publicly sourced information.

CopMonitor's purpose is to make the records and information available to all members of the public including journalists, news outlets, advocates, academics, and community members. While the information is available to the public through various websites, the CopMonitor database aggregates the information in a single location and serves as a resource to all stakeholders.

Note: In September 2021, California Senate Bill 16 was signed into law, which among other matters, expanded access to misconduct records where officers have engaged in biased or discriminatory behavior, conducted unlawful arrests or searches, or used excessive or unreasonable force.¹¹¹ The CopMonitor website does not currently indicate whether there are efforts underway to collect records for the expanded types of misconduct authorized under the 2021 law.

¹⁰⁷ Valerie Ibarra, "San Francisco Public Defender Launches "CopWatch SF" Database to Ensure Public Access to Available Police Records," November 18, 2020, <https://sfpublicdefender.org/news/2020/11/sf-public-defender-launches-copwatch-sf-database-to-ensure-public-access-to-available-police-records/>.

¹⁰⁸ San Francisco Public Defender, CopMonitor, "What Kinds of Public Records are Available in CopMonitor SF?" <https://sfpublicdefender.org/copmonitor/>.

¹⁰⁹ Steven P. Shaw, Howard Jordan, Walter Tibbet and Jim Leal, "Everything You Need to Know About SB 1421 and AB 748," *League of California Cities*, October 2019, 4-5, <https://www.cacities.org/Resources-Documents/Member-Engagement/Professional-Departments/City-Attorneys/Library/2019/2019-Annual-Conference/10-2019-AC;-Jordan-Shaw-Tibbet-Everything-You-Need.aspx>.

¹¹⁰ San Francisco Public Defender, CopMonitor, "Where Does the Public Records Law Material Come From," <https://sfpublicdefender.org/copmonitor/>.

¹¹¹ Nancy Skinner, "Governor Signs SB 16 to Expand and Strengthen Access to Police Records," September 2021, <https://sd09.senate.ca.gov/news/20210930-governor-signs-sb-16-expand-and-strengthen-access-police-records>.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of CopMonitor against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
CopMonitor SF	3	1	3	3	?	?	?

Analysis

1. Complaint Status: 3

CopMonitor reports records of Substantiated Misconduct and Cleared/Exonerated cases. The records contain complaints that resulted in a finding of misconduct, along with complaints where investigations determined that officers acted lawfully or were exonerated from wrongdoing. The database reports the status of the allegations and findings, as furnished by the applicable law enforcement agency. Additionally, the database includes information of media accounts of misconduct by an officer, civil lawsuits alleging wrongdoing and records of officers who have been arrested or prosecuted. Such records may not indicate whether the misconduct has been substantiated or cleared, but rather under our analysis fall under the Pending Investigation category.

2. Misconduct Definition: 1

CopMonitor is a voluntary database, as there is no legal requirement mandating law enforcement agencies to report information to the Administrator of the database. CopMonitor aggregates the records based on its public records requests and publishes the public records as made available by the state of California. As such, the database contains misconduct based on select categories permitted for disclosure under state law: use of a firearm, use-of-force resulting in death or serious bodily injury and sustained allegations of sexual assault or dishonesty.

Due to the limitations of the public record law exemptions when the database was initially developed in 2020, the database excluded many other categories of misconduct including allegations of bias based on race, ethnicity, gender identity, sexual orientation, age, religion, physical or mental disability or immigration status. With the enactment of SB 16, the categories of misconduct included in the database may be expanded.

3. Record Details: 3

CopMonitor reports the details of the incidents, as furnished by the agency releasing the public records. Many documents are searchable and/or can be downloaded. CopMonitor reproduces the documents, as provided and redacted by the Releasing Agency. The database lists officers by name and information displayed includes:

- Incident details — date of incident, agency, type of incident (e.g., shooting firearm at person)
- Files received — official and/or public documentation of the matter including the complaint, findings of the internal investigation and/or the Commission oversight commission, as available, media reports and civil court proceedings

4. Access Rights: 3

CopMonitor records are accessible to the public. The purpose of the database was to aggregate records from across law enforcement agencies and make the information readily available to all stakeholders including lawyers, journalists, academics and community members.

5. Audit and Compliance: ?

There is no information available regarding audits, compliance penalties, Record Retention or frequency of updates to the database.

6. Record Retention: ?

No information available.

7. Reporting Frequency: ?

No information available.

4. Illinois Officer Professional Conduct Database and Law Enforcement Training and Standards Board (ILETSB) Officer Lookup Database

Background

The Illinois Law Enforcement Training and Standards Board (ILETSB) administers the Officer Professional Conduct Database, which was created by the passage of HB3653 (Public Act 101-0652, known as the SAFE-T Act).¹¹² The law went into effect on July 1, 2021.

Before the law was passed, law enforcement agencies were required to notify ILETSB when an officer was fired or resigned under investigation for “willful violation of department policy.”¹¹³ The SAFE-T Act requires additional reporting to ILETSB including extended suspensions and actions that “would trigger an official or formal investigation under a government agency policy.”¹¹⁴ The law also aims to help agencies avoid hiring officers with histories that could indicate the potential for future misconduct by requiring departments to check the Officer Professional Conduct Database prior to appointing any law enforcement officer.¹¹⁵ The database is accessible as part of the hiring process by any government agency, the Illinois State Police, any county State Attorney and the Attorney General, but it is not accessible by the public.¹¹⁶ The public can, however, access individual officer conduct records from specific law enforcement agencies through open records requests

It should be noted that the ILETSB website also offers a separate database, with more limited information, referred to as an Officer Lookup Database. The Officer Lookup Database provides the public with information related to the law enforcement officer's local or state governmental agency; the date of the officer's initial certification and the officer's current certification status; and any sustained complaint of misconduct that resulted in decertification and the date thereof.¹¹⁷ To use the Lookup Database, users must search for a specific officer by name. For purposes of this analysis, the Officer Professional Conduct Database is evaluated, only.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the Officer Professional Conduct Database against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
IL Officer Professional Conduct Database	1	3	2	1	?	1	?

Assumptions

The analysis is based only on the Officer Professional Conduct Database, not the publicly accessible Officer Lookup Database. Given the Officer Professional Conduct Database is not

¹¹² “Public Act 101-0652,” Illinois General Assembly, July 1, 2021, <https://www.ilga.gov/legislation/publicacts/101/PDF/101-0652.pdf>, 68.

¹¹³ Sam Stecklow, “Illinois’ Criminal Justice Overhaul Makes It Easier to Decertify Bad Cops. But It Could Be Harder for the Public to Learn about Them,” *Injustice Watch*, January 13, 2021, <https://www.injusticewatch.org/news/2021/illinois-criminal-justice-overhaul-decertify-bad-cops-transparency/>.

¹¹⁴ Illinois General Assembly, “Public Act 101-0652,” 744.

¹¹⁵ *Ibid.*, 747.

¹¹⁶ *Ibid.*, 745 (c).

¹¹⁷ ILETSB - Officer Lookup, accessed July 26, 2022, <https://www.ptb.illinois.gov/resources/officer-lookup/>.

accessible by the public, our evaluation of the database is based on information in the governing law (HB3653) and other publicly available information shared by the Illinois Law Enforcement Training and Standards Board related to the database.

Analysis

1. Complaint Status: 1

The Officer Professional Conduct Database contains officer decertifications, terminations and substantiated complaints resulting in certain outcomes. The Illinois State Police and all government agencies must notify the ILETSB if they make a final determination on an officer's misconduct. They must notify the ILETSB of a violation of law, willful violation of policy or any other type of official misconduct that results in the following conditions:¹¹⁸

- A sustained instance of departmental misconduct leads to a suspension at least 10 days.
- The infraction triggers an official investigation.
- The officer is discharged or dismissed as a result of the violation.
- There is an allegation of misconduct or regarding the truthfulness of a material fact, bias or integrity.
- The officer resigns or retires during an investigation.
- Any other reported violation, the nature of the violations, the reason for the final decision of discharge or dismissal, and any statement provided by the officer.

2. Misconduct Definition: 3

Illinois public officers (including law enforcement officers) are bound by a high-level definition of misconduct. Official misconduct happens when, in an official capacity, a public officer:

- Intentionally or recklessly fails to perform any mandatory duty as required by law.
- Knowingly performs an act which the officer knows is forbidden by law.
- With intent to obtain a personal advantage for himself or another, the officer performs an act in excess of his lawful authority.
- Solicits or knowingly accepts for the performance of any act a fee or reward which the officer knows is not authorized by law.¹¹⁹

Illinois government agencies are required to notify the Board of any final determination of a willful violation of department, agency, Illinois State Police policy, official misconduct or violation of law. Agencies shall report to the ILETSB information regarding the nature of the violation, and these violations may not necessarily trigger review of certification.¹¹⁸

Additionally, the ILETSB is an oversight agency that “promulgate[s] standards for the selection and training of employees of law enforcement agencies both at the entry and advanced level so as to improve their training and performance, and to establish their qualification to be certified in the State of Illinois according to the standards and rules of the Board and the requirements of the [Illinois Police Training] Act.”¹²⁰

3. Record Details: 2

The database includes each officer's name, each sustained instance of departmental misconduct, as defined above, “the nature of the violation, the reason for the final decision of discharge or dismissal, and any statement provided by the officer.” The database will also

¹¹⁸ Illinois General Assembly, “Public Act 101-0652,” 744.

¹¹⁹ 720 ILCS 5/33-3(a). <https://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K33-3>.

¹²⁰ “Agency Information,” Illinois Law Enforcement Training and Standards Board, accessed July 26, 2022, <https://www.ptb.illinois.gov/about/agency-information/>.

include the “date of separation from employment from any local or state law enforcement agency” and “the reason for separation from employment, including, but not limited to whether the separation was based on misconduct or occurred while the [law enforcement agency] was conducting an investigation of the certified individual for a violation of an employing agency's rules, policy or procedure or other misconduct or improper action.”¹²¹

Neither officer nor complainant demographics or incident details are available.

4. Access Rights: 1

The Officer Professional Conduct Database is accessible to any law enforcement agency (chief or other delegate), the Illinois State Police, any County or State Attorney, and the Attorney General to determine whether to hire a law enforcement officer. Requesting agencies must fill out a request form to initiate process and receive information.¹²² No access is granted to other stakeholders.

5. Audit and Compliance: ?

Information on Audit and Compliance is not publicly available. It is unclear whether there are penalties or disincentives for agencies that do not submit information within the expected timeframe.

6. Record Retention: 1

HB3653 requires that all public and non-public officer misconduct records be permanently retained.¹²³ However, the retention period for records within the database is unclear.

7. Reporting Frequency: ?

Illinois agencies are legally required to “report to the Board within 10 days of a final decision of discharge or dismissal and final exhaustion of any appeal, or resignation, and shall provide information regarding the nature of the violation.”¹²⁴ It is unclear when the board inputs the information into the database.

¹²¹ Illinois General Assembly, “Public Act 101-0652,” 69, 746.

¹²² “Professional Conduct Database Request,” Illinois Law Enforcement Training and Standards Board, accessed July 26, 2022, https://www.ptb.illinois.gov/media/1341/professional_conduct_database_request.pdf.

¹²³ Illinois General Assembly, “Public Act 101-0652,” 66.

¹²⁴ *Ibid.*, 745.

5. National Decertification Index

Background

The International Association of Directors of Law Enforcement Standards and Training (IADLEST) is a membership association of POST directors and other law enforcement educators in each state. IADLEST developed and operates the National Decertification Index (NDI) which, according to IADLEST’s website, is a web application that serves “as a national registry of certificate or license revocation actions relating to officer misconduct.”¹²⁵ IADLEST proposed the idea of the NDI to the US Department of Justice in 2000 and developed the application using funds from DOJ. The NDI was updated in 2005 and is in the process of being expanded as of late-2022.

Records in the NDI are entered by the POST agency in each state. The POST agency also determines which individuals within the state can access information in the NDI. The NDI contains very little information on specific records but is instead a “pointer” system. The NDI will indicate the status of an officer’s certification (decertified, suspended, probation, voluntary relinquishment, etc.) and provides contact information for the agency that entered the record. Users can contact the relevant POST agency to gather additional information where needed.

In addition to providing decertification data to the NDI, some states/departments also publish or allow searches of their decertification information on their own websites. While use of the NDI is voluntary, recent law enforcement reform legislation in North Carolina¹²⁶ and Massachusetts¹²⁷ has created a state-level requirement for law enforcement agencies to check the NDI prior to hiring any candidate.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the NDI against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
National Decertification Index	1	1	1	1	1	1	?

Assumptions

The analysis conducted herein is based on the NDI’s structure prior to the completion of the expansion project that began in 2021.

¹²⁵ “About NDI,” IADLEST, accessed October 25, 2022, <https://www.iadlest.org/our-services/ndi/about-ndi>.

¹²⁶ “House Bill 547 (2021-2022 Session),” North Carolina General Assembly, April 13, 2021, <https://www.ncleg.gov/Sessions/2021/Bills/House/PDF/H547v0.pdf>, Section 1(a)(21).

¹²⁷ “An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth,” The General Court of the Commonwealth of Massachusetts, accessed April 13, 2022, <https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter253>, Section 4(d).

Analysis

1. Complaint Status: 1

The NDI contains records only where an officer's misconduct resulted in decertification. Other types of misconduct are not included.

2. Misconduct Definition: 1

IADLEST does not define the types of misconduct that lead to an officer's decertification. Each POST agency that submits records to the NDI determines what types of misconduct could result in an officer's decertification. Therefore, what decertifies an officer in one state may not result in decertification in another state.

3. Record Details: 1

The NDI contains records of individual decertifications including the officer's name and the status of the officer's certification. The NDI does not include descriptions of the event that led to the decertification, demographic information, information about the complainant, or details on the investigation. These Record Details may be available from the POST agency that submitted the record to the NDI.

4. Access Rights: 1

Access to the NDI is controlled by POST agencies in each state. Those POST agencies generally provide access to individuals involved with officer training and hiring. Other stakeholders and the general public do not have access to the information available in the NDI.

5. Audit and Compliance: 1

IADLEST does not conduct audits of the information added to the NDI by individual POST agencies. It is unclear whether individual POST agencies audit any of the data posted to the NDI. As IADLEST does not have authority over any individual POST agency or law enforcement agency, it cannot require participation.

6. Record Retention: 1

Data in the NDI can be deleted by IADLEST administrators and/or POST administrators. It is not clear whether there are processes in place to determine when records can be deleted from the NDI.

7. Reporting Frequency: ?

It is unclear how often POST agencies submit data to the NDI. Participation in the NDI is voluntary, so it's unlikely that IADLEST sets any requirements for frequency of submission.

6. New Jersey Major Discipline Report

Background

The Major Discipline Report was created through Law Enforcement Directive AG 2021-6 and requires mandatory reporting.¹²⁸ Its launch stemmed from the NJ Attorney General's earlier issuance of Law Enforcement Directive No. 2020-5, known as the "Major Discipline Directive," which was intended to promote a culture of transparency and accountability in policing across the state.¹²⁹ The directive was first posted in August 2021 and included data from the second half of 2020 and more recently the 2021 report was published which reflected a full year.

New Jersey law enforcement misconduct records had historically been closed to the public due to Revised Statutes Section 47:1A-10.¹³⁰ Directive 2021-6 established that a County Prosecutor or Attorney General may direct the disclosure of internal affairs related information. Senate Bill 2656 from the 2020-2021 legislative session would have made public access to officer misconduct complaints permanent law.¹³¹ Other entities, like the journalists behind Force Report NJ, have coalesced information based on media reports and approved open record requests made to the Attorney General.¹³²

The latest published Major Discipline Report identified 350 officers from 128 different departments that were disciplined between January 1, 2021, and December 31, 2021. Offenses described in the report range from "falling asleep on the job" to "terroristic threats."

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the Major Discipline Report against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
New Jersey Major Discipline Report	1	2	1	3	?	1	1

Analysis

1. Complaint Status: 1

The Major Discipline Report contains only substantiated complaints that resulted in major discipline, defined as termination, reduction in rank or grade, and/or suspension of more than five days.

¹²⁸ "Attorney General Law Enforcement Directive No. 2021-6," accessed October 26, 2022, https://www.nj.gov/oag/iapp/docs/AG%20Directive%202021-6%20IAPP%20June%202021_All-Documents.pdf.

¹²⁹ "Attorney General Law Enforcement Directive No. 2020-5," accessed October 26, 2022, https://www.nj.gov/oag/dcj/agguide/directives/ag-Directive-2020-5_Major-Discipline.pdf.

¹³⁰ NJ Rev Stat § 47:1A-10 (2013), accessed March 23, 2022, <https://law.justia.com/codes/new-jersey/2013/title-47/section-47-1a-10/>.

¹³¹ "Bill S2656," New Jersey Legislature, accessed October 26, 2022, <https://www.njleg.state.nj.us/bill-search/2020/S2656>.

¹³² "Every Punch, Kick and Pepper Spray by Police in Your Town. Search Our Database," *Force Report*, accessed October 26, 2022. <https://force.nj.com/>.

Outside of the report, every law enforcement agency provides to each county prosecutor and publishes on its public website an annual report summarizing the types of complaints received and the dispositions of those complaints. These reports are statistical in nature. County prosecutors then submit a summary of the reports from all agencies in their jurisdiction to the Office of Public Integrity and Accountability.

2. Misconduct Definition: 2

While the Attorney General defines major discipline as “terminations, reductions in rank, or suspension of more than five days,” each agency is able to determine what conduct would warrant such a categorization.¹³³ However, the New Jersey Attorney General and broader NJ Department of Law & Public Safety exhibit some oversight in instituting policies and regulations that apply to NJ reporting agencies (e.g., training certification¹³⁴ and police-community initiatives¹³⁵). In addition, the database is limited to only records that resulted in some action against an officer’s license (e.g., termination, suspension, reduction in rank)

3. Record Details: 1

The report includes a brief synopsis of discipline including the names and rank of the officers sanctioned, a standardized categorization of the charge, and the outcome (terminated, demoted, suspended including for how many days). It also includes the agency name and the county. Note that the New Jersey Attorney General’s directive states that “public reports concerning major discipline shall not disclose the identities of the victims of officer misconduct.¹³⁶ No other demographic information is available.”

4. Access Rights: 3

The Major Discipline Report is published annually on the New Jersey’s Attorney General’s website, which is available to the public.

5. Audit and Compliance: ?

“Reports disclosed to the public reflect a law enforcement agency’s independent, good-faith assessment of the information appropriate to be disclosed under the Directive.”¹³⁷ County prosecutors are responsible for ensuring agencies comply with these public disclosure responsibilities in a timely manner. However, an audit schedule and compliance incentives/disincentives are not clear from the available information.

6. Record Retention: 1

A retention schedule or policy related to the data in the annual report does not appear to be available. However, the broader New Jersey Division of Archives and Records Management retention schedule suggests that all “criminal or administrative internal affairs investigative records be maintained for at least 5 years” and the New Jersey Attorney General’s Internal Affairs Policy & Procedures state that “agencies should maintain these files as they relate to a particular officer for that officer’s career plus 5 years.”¹³⁸ The exceptions are for files

¹³³ “Major Discipline”, New Jersey Office of Attorney General, accessed October 26, 2022, <https://www.njoag.gov/majordiscipline/>.

¹³⁴ “Police Training Commission,” New Jersey Office of Attorney General, February 4, 2022, <https://www.njoag.gov/about/divisions-and-offices/division-of-criminal-justice-home/police-training-commission/>.

¹³⁵ “Policing initiative”, New Jersey Office of Attorney General, July 17, 2021, <https://www.njoag.gov/programs/policing-initiative/>.

¹³⁶ “Attorney General Law Enforcement Directive No. 2021-6,” 3

¹³⁷ Ibid

¹³⁸ “Internal Affairs Policy & Procedure”, Office of the Attorney General, State of New Jersey, December 2021, accessed October 26, 2022, https://www.nj.gov/oag/dcj/agguide/directives/ag-Directive-2021-6_Major-Discipline-Supplemental-Directive-12-21-21.pdf, 55

concerning criminal homicide which must be permanently maintained.¹³⁹ The retention schedule “also requires that any other file involving a criminal matter resulting in the subject officer’s arrest must be maintained for 75 years.”¹⁴⁰

7. Reporting Frequency: 1

Data is required to be published by local law enforcement agencies and submitted to the New Jersey Attorney General at least once per year.¹⁴¹ The New Jersey Attorney General publishes the report on its website only on an annual basis.¹⁴²

¹³⁹ Ibid.

¹⁴⁰ Ibid.

¹⁴¹ “Major Discipline”, New Jersey Office of Attorney General, accessed October 26, 2022, <https://www.njoag.gov/majordiscipline>

¹⁴² Ibid.

7. NYPD Member of Service History Database

Background

The New York City Police Department Member of Service History Database was established in May of 2020. The database is administered by the Civilian Complaint Review Board (CCRB) and includes police disciplinary data of over 83,000 active and former police officers, for all closed allegations that fall under the CCRB's jurisdiction, dating back to 2000.

The creation of the database followed the repeal of New York State Civil Rights Law section 50-a, which was used to shield officer misconduct records from the public. Prior to the repeal, New York had one of the most restrictive police secrecy laws in the country.¹⁴³ After the repeal of section 50-a, these records were made accessible to the public to increase transparency and accountability in the NYPD.¹⁴⁴ There are several other complementary accountability databases in New York State, many specifically related to the NYPD, all of which were made possible by the repeal of section 50-a.¹⁴⁵

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the NYPD Member of Service History Database against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
NYPD Member of Service History Database	2	3	1	3	1	1	?

Analysis

1. Complaint Status: 2

The NYPD Member of Service History Database includes closed complaints, whether substantiated or unfounded, that fall under CCRB's jurisdiction. The database does not include open allegations, successfully mediated allegations, mediation attempted allegations or referrals to the NYPD or other investigative entities.¹⁴⁶

2. Misconduct Definition: 3

The database is administered by the CCRB and mandatorily includes all closed complaints that fall under its jurisdiction, regardless of whether they may result in a license or certification action. Under the current New York City Charter, the CCRB attends to complaints against members of the police department that allege misconduct involving excessive use of force, abuse of authority including bias-based policing and racial profiling, discourtesy, or use of offensive language, including, but not limited to, slurs relating to race,

¹⁴³ Stephanie Wykstra, "The Fight for Transparency in Police Misconduct, Explained," Vox, June 16, 2020, accessed October 27, 2020. <https://www.vox.com/2020/6/16/21291595/new-york-section-50-a-police-misconduct>.

¹⁴⁴ "Law Enforcement Disciplinary Records," New York State Defenders Association, accessed October 27, 2022, <https://www.nysda.org/page/LawEnforcementDisciplinaryRecords>.

¹⁴⁵ "Law Enforcement Disciplinary Records," New York State Defenders Association, accessed October 27, 2022, <https://www.nysda.org/page/LawEnforcementDisciplinaryRecords>.

¹⁴⁶ "NYPD Member of Service Histories," Civilian Complaint Review Board (New York City), accessed October 27, 2022, <https://www1.nyc.gov/site/ccrb/policy/MOS-records.page>.

ethnicity, religion, gender, sexual orientation and disability.”¹⁴⁷ The CCRB board submits its findings and recommendations to the police commissioner¹⁴⁸, who may impose a penalty on the offending officer. The penalty, which could be decertification, along with the separate dispositions of the CCRB and NYPD, are recorded in the database.

3. Record Details: 1

The database includes officer’s name and a unique complaint ID; the date of alleged incident; incident category, known as “FADO” type (Force, Abuse of authority, Discourtesy or Offensive language; a high-level description; and outcome, including board disposition, NYPD disposition, and penalty. The database does not include any demographic data about complainants or officers, nor does it include any primary documents from the investigation.¹⁴⁹

4. Access Rights: 3

The public has access to the entire database and it is searchable by officer details or number of substantiated complaints. While an aggregate data download is not possible by the public, the CCRB “issues a minimum of 14 reports per year based on data in the database to fulfill its mandate to inform the public and New York City elected officials about NYPD operations, complaint activity, case dispositions and police department discipline. These reports include monthly statistical reports, annual and semi-annual reports, as well as issue-based reports on topics related to police misconduct with recommendations on NYPD policies, procedures, and training.”¹⁵⁰

5. Audit and Compliance: 1

There is no information regarding any audit or compliance measures for the database. However, the audit board has the power to “perform assessments and audits of the police department’s internal systems for detecting, investigating and preventing corruption among uniformed and civilian members of the police department, and make recommendations for the improvement of those systems.”¹⁵¹

6. Record Retention: 1

While the database contains records from as early as the year 2000, it’s unclear how long misconduct records are retained in the database.¹⁵²

7. Reporting Frequency: ?

It’s unclear how often the CCRB updates the database, but the website shows the date that the data represents.¹⁵³

¹⁴⁷ New York City Charter Chapter 18-A Section 440(c)1

¹⁴⁸ Ibid.

¹⁴⁹ Civilian Complaint Review Board, “NYPD Member of Service Histories.”

¹⁵⁰ “Reports,” Civilian Complaint Review Board (New York City), accessed October 27, 2022, <https://www1.nyc.gov/site/ccrb/policy/reports.page>.

¹⁵¹ New York City Charter Chapter 18-B Section 451(a)1

¹⁵² “Law Enforcement: General,” New York State Archives (The Office of Cultural Education), accessed October 27, 2022, <http://www.archives.nysed.gov/records/local-government-record-schedule/law-enforcement-general>.

¹⁵³ Civilian Complaint Review Board, “NYPD Member of Service Histories.”

8. Oregon Department of Public Safety Standards & Training (DPSST) Professional Standards Cases Database

Background

In June 2020, the Oregon Legislative Assembly passed House Bill 4207 requiring the state Department of Public Safety Standards & Training (DPSST) to establish a publicly accessible, statewide online database of the suspensions and revocations of police officer certifications.¹⁵⁴

The Professional Standards Cases Database was released in August 2020 and expanded in January 2021 to include information on all open professional standards cases and the disposition of each case.¹⁵⁵ In June 2021, the Oregon Legislative Assembly passed House Bill 3145 requiring the DPSST to also include “discipline of police officers involving economic sanctions” in the database.¹⁵⁶ Submission to the Professional Standards Cases Database is mandatory, including cases that result in actions against an officer’s license/certification and cases that do not result in a license/certification action.

The database includes information on all professional standards cases opened related to public safety officers statewide, including police, corrections and dispatchers. “Professional standards cases are opened when DPSST receives information that an officer has been arrested or receives a criminal citation to appear; terminated from an agency; resigned/retired from an agency during an investigation or as a result of a settlement agreement; directed by a policy committee to open a case as a result of certain complaints; dismissed from the Oregon Public Safety Academy, and falsification.”¹⁵⁷

The public database includes links to supporting documentation and the information can be exported to Excel. Additional information is available to the public through public records requests.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the Oregon Professional Standards Cases Database against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
Oregon DPSST Professional Standards Cases Database	3	3	3	3	?	2	3

¹⁵⁴ Relating to records of discipline of police officers; and declaring an emergency, HB 4207, Oregon legislative assembly. (2020 1st Special Session), <https://olis.oregonlegislature.gov/liz/2020S1/Downloads/MeasureDocument/HB4207/Enrolled,2>.

¹⁵⁵ “Update to DPSST’s Professional Standards Case Database (2020 HB 4207),” Oregon Department of Public Safety Standards and Training, January 22, 2021, <https://content.govdelivery.com/accounts/ORDPSST/bulletins/2bac760?reqfrom=share>.

¹⁵⁶ “House Bill 3145”, Oregon legislative assembly, 2021 Regular Session, <https://olis.oregonlegislature.gov/liz/2021R1/Downloads/MeasureDocument/HB3145/enrolled,1>.

¹⁵⁷ “Professional Standards,” Department of Public Safety Standards & Training (Oregon.gov), accessed October 26, 2022, <https://www.oregon.gov/dpsst/cj/pages/professionalStandards.aspx>, Case Opening.

Analysis

1. Complaint Status: 3

The Professional Standards Cases Database includes professional standards cases that have been substantiated and misconduct allegations that have not been substantiated. Cases are opened for officer terminations, suspensions, resignations/retirements during an investigation, dismissals from the Oregon Public Safety Academy, falsifications and as directed by policy committees related to certain complaints. The database includes all professional standards cases including those that are “under review” and those that have been cleared or exonerated, which is indicated by the case status “Admin Closure.”

2. Misconduct Definition: 3

The Oregon Board on Public Safety Standards and Training is responsible for setting “policies, standards and minimum requirements for public safety certification and training”¹⁵⁸ for Oregon’s public safety professionals including “corrections officers, emergency medical dispatchers, parole and probation officers, police officers, certified reserve officers, reserve officers, telecommunicators and regulatory specialists.”¹⁵⁹ These requirements are laid out in Oregon Administrative Rules (OAR) Chapter 259, Division 8. The DPSST is responsible for opening, reviewing, and presenting professional standards cases to the board, which ultimately decides how to close each case. Under the law, cases of officer arrest, criminal citation, and employee separation are required to be submitted to the Professional Standards Cases Database, regardless of whether the case will result in actions against an officer’s license/certification or not. All professional standards cases included in the database are handled by DPSST and the board based on the rules set forth by the board.

3. Record Details: 3

Individual case records are available in the database. Each case includes the officer’s name, DPPST number, the officer’s certifications, reason for reporting, status of the investigation, documents, employer, revoke/deny reason, case open/close dates, ineligibility periods, time employed and the officer’s highest certification. The database does not highlight officer or complainant demographic information, though that information is sometimes available in the documents attached to each case.

4. Access Rights: 3

The database is fully accessible to the public via the DPSST website¹⁶⁰ and data can be downloaded to Microsoft Excel.

5. Audit and Compliance: ?

Neither the enabling legislation that created the database nor the OAR require an audit of the database or of professional standards cases. Because individual agencies are not responsible for reporting into the database, there are no compliance incentives or disincentives for participation. The DPSST administers and populates the database without input from individual agencies.

¹⁵⁸ “Bylaws of the Board on Public Safety Standards and Training,” The Board on Public Safety Standards and Training, April 25, 2019, <https://www.oregon.gov/dpsst/BD/Documents/By-Laws/BPSST%20Bylaws%20Final%204-25-19.pdf>, 1.

¹⁵⁹ “Chapter 259, Division 8, Criminal Justice Employment, Training and Certification,” Oregon Secretary of State, September 3, 2021, <https://secure.sos.state.or.us/oard/viewSingleRule.action?ruleVrsnRsn=280838>, Section 30.

¹⁶⁰ “DPSST Professional Standards/Economic Sanctions Database,” Department of Public Safety Standards & Training (Oregon.gov), accessed October 26, 2022, <https://www.oregon.gov/dpsst/cj/pages/cases.aspx>.

6. Record Retention: 2

The database has a definitive period for how long data is maintained in the database. Officers and dispatchers will remain in the database until five years after the case is closed.¹⁶¹

7. Reporting Frequency: 3

HB 4207 requires that the DPSST publish information within 10 days after:

- The time for filing an appeal of the department's decision under Oregon Revised Statutes (ORS) 181A.650 has passed and no appeal has been filed; or
- The decision of the department is appealed under ORS 181A.650 and the department's decision has been sustained by the Court of Appeals or the appeal has been dropped.

¹⁶¹ Department of Public Safety Standards & Training, "DPSST Professional Standards/Economic Sanctions Database."

9. University of Southern California Police Misconduct Registry

Background

In May 2021, the University of Southern California (USC) Safe Communities Institute (SCI) launched a pilot program to create the USC Police Misconduct Registry (PMR), a database dedicated to cataloging information on police officers nationwide who were terminated or resigned due to misconduct including excessive use of force, corruption, violent extremism, domestic violence, sexual assault, physical assault and harassment, perjury, falsifying a police report, and planting or destroying evidence. The registry is intended to provide transparency on officer misconduct to the public and to law enforcement executives who are hiring new recruits and was cofounded by Dr. Erroll Southers, former SCI director, and DreamView President and Chief Information Officer Dr. Güz Salinas.¹⁶² One key objective of the registry is “to hold police officers and departments accountable and increase public trust in law enforcement.”¹⁶³ SCI is the site administrator and regularly updates and maintains the information in the registry. SCI uses publicly sourced data to populate the information.

In October 2021, the PMR went live to the public with the names of terminated or resigned officers in a system commonly referred to as the public portal. The public portal reports the officer’s name, gender, category of misconduct (physical, harassment, corruption, etc.), rank of officer, name of agency, county, state, date of reported information and source link. Users can search the public portal by officer name to find whether an officer has ever been fired or resigned due to misconduct. Some law enforcement agencies also use the PMR as part of their standard hiring practices.¹⁶⁴

In addition to the public-facing part of the registry, there is a backend accessible only to law enforcement agencies, referred to as the private portal. The private portal has more information on misconduct incidents that have not resulted in terminations or resignations. The objective is to build a collective body of data, helping to identify patterns and trends among officers and departments and supporting agencies to make better informed hiring decisions.¹⁶⁵

The PMR’s governance and strategic objectives are set by the PMR Advisory Board, a group of community and law enforcement stakeholders. The board oversees and reviews record entries and facilitates redress decisions regarding officers that may need to be removed from the database.

¹⁶² Victoria Valenzuela, “Institute to Launch First Public Registry on Police Misconduct,” *Daily Trojan*, June 16, 2021, <https://dailytrojan.com/2021/06/16/institute-to-launch-first-public-registry-on-police-misconduct/>.

¹⁶³ Jenesse Miller, “How a National Police Misconduct Registry Can Help Rebuild Trust in Law Enforcement,” USC News, May 27, 2021, <https://news.usc.edu/187367/national-police-misconduct-registry-trust-law-enforcement-erroll-southers-usc/>.

¹⁶⁴ City of Long Beach, City Council Minutes, Agenda Item 61 (21-1191), “Motion Passes to Adopt Resolution in Support of the Establishment of the Law Enforcement Work Inquiry System, and Request City Manager to Have the Long Beach Police Department Partner with LEWIS Registry at the University of Southern California,” November 9, 2021, <http://longbeach.legistar.com/View.ashx?M=A&ID=902751&GUID=38C70F59-525B-4504-A1E8-C6ED67346B09>.

¹⁶⁵ Miller, “How a National Police Misconduct Registry Can Help Rebuild Trust in Law Enforcement.”

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the USC PMR against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
USC PMR	1	1	2	2	?	?	?

Assumptions

The following analysis has been conducted on the Public Portal only, except as noted below regarding the Access Rights design element. Details on the Private Portal are not publicly available.

Analysis

1. Complaint Status: 1

The USC PMR documents misconduct that has resulted in an officer's termination or resignation. These incidents have been substantiated through internal investigations, disciplinary proceedings and/or criminal convictions and have been publicly reported.. No records outside of substantiated complaints are included in the Public Portal registry.

2. Misconduct Definition: 1

The records in the PMR do not adhere to a standardized definition of misconduct and law enforcement agencies are not mandated to report to the database. SCI uses information "drawn from public sources, such as official department statements, court records, police notices, news reports and other open sources."¹⁶⁶ The termination and resignation data is derived from law enforcement agencies across the country. Individual agency and department policies and procedures establish what type of conduct is considered inappropriate and is grounds for termination. Each record in the PMR is based on determinations made by the applicable state or local law enforcement agency. The state and municipal standards for termination, along with the application of those standards to the facts will vary considerably across jurisdictions.

The purpose of the PMR is to prevent wandering officers who were terminated for or resigned due to misconduct from being hired in other jurisdictions.

3. Record Details: 2

For each record there is a source link which provides information on the termination or resignation.¹⁶⁷ The sourced information may be articles, statements or other journalistic publications that identify the officer's name, outcome of the investigation, disciplinary proceeding or court trial and the circumstances of the misconduct. Primary source documents related to the termination or resignation (from the law enforcement agency, courts, etc.) are not included.

¹⁶⁶ SCI, "SCI Recognizes Frank Serpico with First-Annual Humanitarian Award," USC Price School of Public Policy Safe Communities Institute, July 16, 2021, <https://sci.usc.edu/2021/07/16/lewis-registry-frank-serpico-humanitarian-award/>.

¹⁶⁷ E.g., The entries on officers Ryan Starbuck, Samuel Routledge, and Jonathan Jackson link to a news source: Dylan Smith, "Details Revealed about Ingram-Lopez Death in Police Custody: Tucson Police Department Chief Offers to Resign," *Tucson Sentinel*, June 24, 2020, that reported the three officers resigned before they could be fired.

4. Access Rights: 2

The PMR offers tiered access through two avenues: the public portal and private portal. The public portal provides complete access to substantiated misconduct matters resulting in an officer's termination or resignation. Law enforcement executives have additional access to other misconduct matters that have not resulted in termination or resignation. Details on the information in the private portal are not known.

5. Audit and Compliance: ?

It is unknown if the PMR has an audit or compliance function.

6. Record Retention: ?

It is unknown if the PMR has a Record Retention process.

7. Reporting Frequency: ?

It is unknown if the PMR has set standards for Reporting Frequency.

10. USA Today Decertified Officer Database

Background

In 2019, USA Today led a national effort to publish LEO disciplinary records. USA Today investigated and found that at least 85,000 officers across the country had been investigated or disciplined for misconduct over the past decade. USA Today and its affiliated newsrooms across the country spent more than a year creating a collection of over 200,000 incidents of alleged misconduct obtained from thousands of state agencies, prosecutors, police departments and sheriffs. The records obtained include more than 110,000 internal affairs investigations by hundreds of individual departments and more than 30,000 officers who were decertified by 44 state oversight agencies. USA Today created the database to provide transparency about police misconduct in local communities and more broadly, including helping to identify decertified officers who continue to work in law enforcement. The information collected includes officer names, the department they worked for when the state revoked their certification and the reasons for the decertification. The list is not exhaustive, but it does provide insights for most states. Of the more than 30,000 law enforcement officers who lost their certifications, the most common reasons were drugs and alcohol followed by assaults and violence, dishonesty, theft, misconduct with prisoners, sexual misconduct and other officer misconduct.¹⁶⁸

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the USA Today's database against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
USA Today Decertified Officer Database	1	1	1	3	?	?	?

Analysis

1. Complaint Status: 1

The USA Today database includes officer decertification's due to misconduct. The database does not provide information on misconduct that results in other disciplinary outcomes or misconduct that has not been substantiated through internal investigations.

2. Misconduct Definition: 1

The information in the USA Today database does not adhere to a standardized definition of misconduct. The database contains information about officers decertified by state oversight agencies that each have varying processes and policies for decertifying officers.

3. Record Details: 1

Each record in the database includes the officer's department, the officer's name and, in most cases, why the officer was decertified. Primary source documents related to the

¹⁶⁸ John Kelly and Mark Nichols, "Search the List of More than 30,000 Police Officers Banned by 44 States," USA Today, Gannett Satellite Information Network, December 17, 2019, <https://www.usatoday.com/in-depth/news/investigations/2019/04/24/biggest-collection-police-accountability-records-ever-assembled/2299127002/>.

misconduct and decertification from the law enforcement agency, courts, etc., are not included.

4. Access Rights: 3

The database is accessible by the public. Access is not limited to a specific stakeholder.

5. Audit and Compliance: ?

It is unknown if there are any policies/procedures in place regarding any audit of the data in the database.

6. Record Retention: ?

It is unknown how long the information in the database is retained.

7. Reporting Frequency: ?

It is unknown how often information is submitted to the database.

11. Washington Certification Database

Background

The Washington State Criminal Justice Training Commission (WSCJTC) has the power to “deny, suspend, or revoke certification of, or require remedial training for” peace officers if they are found to have committed certain misconduct.¹⁶⁹ Depending on the offense committed, the WSCJTC is either required to or has the discretion to deny or revoke an officer’s certification.¹⁷⁰ When WSCJTC is made aware of misconduct, upon a request by an officer’s employment, through a submitted complaint, or on its own initiative, as outlined in RCW 43.101.105, the Certification Division will open a case, conduct an investigation and “if the alleged misconduct meets the burden of proof, the commission” will issue a statement of charges to the officer and then make a final determination on whether to deny, revoke or suspend the officer’s certification. Certification hearings can be requested by peace officers who have received a statement of charges regarding the denial or revocation of their certification.¹⁷¹

WSCJTC reports all officer decertifications to the National Decertification Index and maintains a publicly accessible online certification database of all certification cases reviewed by its certification division.¹⁷² The hearings are open to the public.

WSCJTC provides public notice on its website of certification hearings and all previous certification revocations and eligibility reinstatements.¹⁷³ Within the certification database, supporting documents are provided for each case with a “closed” status and for certain cases that are “under review.” These may include a statement of charges and the outcome of the case.

Along with the database, the WSCJTC provides a variety of summary tables and visualizations that assist users with identifying trends across included data fields. The full dataset is also exportable.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the certificate revocations and hearings data against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
Washington Certification Database	3	3	3	3	1	2	3

¹⁶⁹ “Denial, suspension, or revocation of peace and corrections officer certification,” Washington State Legislature, accessed October 25, 2022, <https://app.leg.wa.gov/RCW/default.aspx?cite=43.101.105>.

¹⁷⁰ Ibid.

¹⁷¹ Ibid.

¹⁷² WSCJTC Certification Database, WA.gov, accessed October 25, 2022, <https://data.wa.gov/stories/s/WSCJTC-Certification-Database/3xkp-u89m/>.

¹⁷³ “Certification Hearings,” Washington State Criminal Justice Training Commission, accessed October 25, 2022, <https://www.cjtc.wa.gov/certification/certification-hearings>.

Analysis

1. Complaint Status: 3

The WSCJTC's Certification Database relates only to cases that may impact an officer's certification. However, the WSCJTC opens certification cases based on information received from an officer's employer or a complaint.¹⁷⁴ Based on the "reason for opening case" field in the database, cases are opened only for complaints that rise to the level of misconduct outlined in RCW 43.101.105, requests for certification to be reinstated, or when an officer separates from the employing agency.¹⁷⁵ The WSCJTC publishes those cases which are pending review and have not been assigned for investigation as well as those instances where an officer has been cleared of the complaint/ allegation against them.¹⁷⁶

2. Misconduct Definition: 3

Agencies must submit any instances when Discipline, Suspension, Use of Force causing serious injury or death, or Criminal Charges have occurred and it is probable that the incident meets the criteria in RCW 43.101.095.¹⁷⁷ The WSCJTC provides clear standards for certification and decertification on their website and bases its certification revocation decisions on that definition.¹⁷⁸ All certification revocations and hearings listed on the website are based on this common definition. However, the database holds pending investigations in addition to certification reviews that resulted in an officer being cleared.

3. Record Details: 3

The database contains case number, date of record opening, officer name, agency of employment, case category, status, outcome and date the record was closed (if applicable). For certain cases (generally those where the case is closed), primary source documents including hearing outcomes and statements of charges are provided. These documents provide a more robust record than what is included on the record in the database. The documents do not include demographic information or information about the complainant.

4. Access Rights: 3

Access is made available to the public with no authorization needed.

5. Audit and Compliance: 1

It is unclear if WSCJTC proactively identifies officers whose certifications may need to be revoked as part of ongoing business or through any periodic audit. However, the department is notified to open a case either through the officer's employer or through a complaint submitted online. For officers who choose to have a certification hearing, those hearings are open to the public, which allows for some oversight of the revocation process. Details on compliance incentives or disincentives, if any, are not available.

6. Record Retention: 2

The WSCJTC has a Record Retention schedule which states that records related to peace officer revocation and reinstatement hearings are retained for 40 years after disposition of

¹⁷⁴ WSCJTC Certification Database

¹⁷⁵ Ibid.

¹⁷⁶ Ibid.

¹⁷⁷ Washington State Criminal Justice Training Commission, accessed October 25, 2022, <https://www.cjtc.wa.gov/certification/certification-hearings>

¹⁷⁸ "RCW 43.101.105: Denial, suspension, or revocation of Peace and corrections officer certification," Washington State Legislature, accessed October 25, 2022, <https://app.leg.wa.gov/RCW/default.aspx?cite=43.101.105>.

the case and are then destroyed.¹⁷⁹ In addition, based on RCW 43.101.400, the commission should include relevant case records in the online, public database for a period of at least 30 years.¹⁸⁰

7. Reporting Frequency: 3

Within 15 days, agencies must submit any instances when Discipline, Suspension, Use of Force causing serious injury or death, or Criminal Charges have occurred and it is probable that the incident meets the criteria in RCW 43.101.095.¹⁸¹ WSCJTC posts findings from revocation hearings to its website within 95 days of the hearing date.¹⁸² It is unclear how quickly a case record is added to the database, but as of July 26, 2022 there were records posted as recently as July 7, 2022. Prior to the publishing of the online database, the WSCJTC posted its certificate revocation list approximately every two weeks.¹⁸³

¹⁷⁹ “Criminal Justice Training Commission Records Retention Schedule,” Washington State Criminal Justice Training Commission, April 2018, https://www.cjtc.wa.gov/docs/default-source/public-records/wscjtc-records-retention-schedule.pdf?sfvrsn=2f859b1b_2, page 6.

¹⁸⁰ RCW 43.101.400: Confidentiality of Records-Public Database. Washington State Legislature. Retrieved October 25, 2022, from <https://app.leg.wa.gov/RCW/default.aspx?cite=43.101.400>

¹⁸¹ Washington State Criminal Justice Training Commission, accessed October 25, 2022, <https://www.cjtc.wa.gov/certification/certification-hearings>.

¹⁸² Ibid.

¹⁸³ Ibid.

Recently Authorized Databases Under Development

12. Alabama

Background

In March 2021, Alabama legislators passed a bill to create a centralized database of use-of-force misconduct for all law enforcement officers and applicants which was signed by Governor Ivey in April of that year. The law requires the database be operational by October 1, 2023¹⁸⁴. Under the legislation, the Alabama Peace Officers' Standards and Training Commission (APOSTC) maintains the database and law enforcement agencies are required to submit use-of-force complaints filed against officers to APOSTC.¹⁸⁵ The bill enables departments, that may not have the resources to conduct adequate background checks during the hiring process, to access the state database to obtain information on a candidate's history. Chief Alan Benefield, the executive secretary of APOSTC stated, "It's a big problem in law enforcement. It has been forever that you have problem officers fired or resigned that nobody knows, they go to another job and they're employed by another department and there's no background information on them."¹⁸⁶

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the Alabama database against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
Alabama	1	3	1	1	3	2	3

Analysis

1. Complaint Status: 1

The Alabama database includes only substantiated or formal corrective actions based on use-of-force complaints.

2. Misconduct Definition: 3

The Alabama database will have a standard definition for the misconduct records. Records will be included in the database for "any formal corrective action resulting in a recommendation of reprimand, suspension, or termination based on a use-of-force complaint, as defined in this section, or investigation, and which is deemed final after the conclusion of any and all appeals or avenues of appellate review in the underlying disciplinary proceedings."¹⁸⁷

3. Record Details: 1

Each disciplinary record in the database will include the "name of the law enforcement officer; the date of the disciplinary action; the type of disciplinary action imposed; a

¹⁸⁴ Rep. Artis McCampbell and Rep. Neil Rafferty, "HB411: 2021," Alabama State Legislature, February 11, 2021, <http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2021RS/PrintFiles/HB411-enr.pdf>, page 3 line 22

¹⁸⁵ Rep. Artis McCampbell and Rep. Neil Rafferty, "HB411: 2021.", page 1, line 3.

¹⁸⁶ Jennifer Horton, "Alabama Passes Law to Track Officers Accused of Misconduct," WBRC News, May 21, 2021, <https://www.wbrc.com/2021/05/20/alabama-passes-law-track-officers-accused-misconduct/>.

¹⁸⁷ Rep. Artis McCampbell and Rep. Neil Rafferty, "HB411: 2021.", page 2, line 3.

description of the conduct upon which such disciplinary action is based; and the name of the person alleging the complaint.”¹⁸⁸ Other types of records will also include the substance of the complaint, the outcome of any investigations and internal appeals.

4. Access Rights: 1

Law enforcement agencies will be given access. The database will not be accessible to the public.

5. Audit and Compliance: 3

The legislation reads that the “Alabama Peace Officers' Standards and Training Commission shall randomly audit law enforcement agencies' compliance with the reporting requirements.”¹⁸⁹ It also states that APOSTC “may assess a civil penalty against the [noncompliant] agency in the amount of one thousand dollars (\$1,000) for each violation and an additional one hundred dollars (\$100) thereafter for each day the information is not reported to the commission for entry into the database.”¹⁹⁰

6. Record Retention: 2

Law enforcement agencies will be required to maintain information for 12 years.¹⁹¹

7. Reporting Frequency: 3

Disciplinary actions, reassignment for cause and use-of-force complaints must be reported within 30 days of those items becoming final. Reportable separations must be reported within 15 days.¹⁹²

¹⁸⁸ Ibid., page 5, line 11.

¹⁸⁹ Ibid., page 10, line 12.

¹⁹⁰ Ibid., page 10, line 22.

¹⁹¹ Ibid., page 6, line 15.

¹⁹² Ibid., pages 5-6.

13. Massachusetts

Background

On December 31, 2020, former Massachusetts Governor Charlie Baker (R) signed a landmark law enforcement reform bill into law. The legislation, “An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth,” created significant changes to law enforcement training, certification and oversight. It sets forth numerous changes to increase accountability and transparency in law enforcement. As part of the process to enable hiring and promoting qualified law enforcement officers, the law established an independent commission, the Massachusetts Peace Officer Standards and Training Commission (MA POST), to oversee the training, certifying, and disciplining all law enforcement officers in the Commonwealth.¹⁹³ In June 2022, MA POST adopted administrative regulations on the process to receive, investigate and adjudicate complaints from the local law enforcement agencies¹⁹⁴ Among its other duties, MA POST has been charged with creating and maintaining information in one or more databases.

- **MA POST Database for Certified Law Enforcement Officers:** Records on each certified law enforcement officer including date of initial certification, recertification, completion of trainings, written reprimands and the reasons for the reprimands, internal affairs complaints and the reason for the internal affairs complaints, the outcome of internal affairs investigations, the date of any separation from employment with an agency and the nature of the separation including suspension, resignation, termination or misconduct.¹⁹⁵
- **MA POST Database on Police Misconduct:** Records on complaints about officer misconduct, including information relating to an officer’s certification or decertification, arrests or convictions, disposition of internal affairs complaints and investigations, and any information relating to an officer’s prior separation from a law enforcement agency. MA POST also “shall actively monitor the database to identify patterns of unprofessional police conduct.”¹⁹⁶
- **MA Publicly Searchable Database on Law Enforcement Officers:** Records that make certain information on law enforcement officers available to the public subject to the health and safety of the officers, as determined by rulemaking conducted by the MA POST.¹⁹⁷
- **MA Publicly Available Database on Decertification/Suspension/Retraining:** Names of all decertified/suspended officers, the date of decertification/suspension, the officer’s last appointing agency and the reason(s) for decertification/suspension, the names of all officers who have been ordered to undergo retraining, the date of the retraining, the type of retraining, the appointing agency and the reason for the retraining order.¹⁹⁸

We analyzed the four databases in the aggregate considering the type, scope and access to the information collected among the four databases, which MA POST is required to establish. In October 2022, MA POST approved the draft regulations CMR 8.00 on Databases and

¹⁹³ Sarah Finlaw, Office of Governor Charlie Baker and Lt. Governor Karyn Polito, Press Release, “Governor Baker Signs Police Reform Legislation,” December 31, 2020, <https://www.mass.gov/news/governor-baker-signs-police-reform-legislation>.

¹⁹⁴ Code of Massachusetts Regulations, 555 CMR 1.00, et. seq. [555 CMR 1.00 \(mass.gov\)](https://www.mass.gov/info-details/555-cmr-1-00).

¹⁹⁵ “An Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth”, Chapter 253, December 31, 2020, <https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter253>, Chapter 6E, Section 4(h)(1)-(13).

¹⁹⁶ *Ibid.*, Chapter 6E, Section 8(e)-(f).

¹⁹⁷ *Ibid.*, Chapter 6E, Section 4(j).

¹⁹⁸ *Ibid.*, Chapter 6E, Section 13(a).

Dissemination of Information. The proposed regulations are intended to govern the administration of the public database. The draft regulations are currently being prepared for public notice and public comment hearing.

Our analysis is based on the draft regulations 555 CMR 8.00 Databases and Dissemination of Information, available on the [MA POST website](#), and final regulations 500 CMR 1.00 on Receiving, Investigating, Hearing, and Adjudicating Complaints regarding Law Enforcement Officers in Massachusetts.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the Massachusetts databases against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
Massachusetts	3	3	3	2	?	?	3

Status of the Databases

The MA POST is currently in the process of compiling the records to create the databases. State law enforcement agencies were required to submit summaries of disciplinary records of their officers and transferred officers to the MA POST. Information was submitted via excel spreadsheets:

A	B	C	D	E	F	G	H	I	J	K	L
1	LEA Name:										
2	Active Personnel LEA										
3	Last Name	First Name	Date of Start of Employment	Date of Complaint	Internal Affairs Investigation No.	Investigation Admin/Criminal	Charge(s) / Infraction/Violation	Admin. Leave (Y/N)	Disposition (S, NS, E, U)	Discipline (WR, RT, S, T, RN)	Comments *
4	1	Doe	Jane	January 1, 2020	NONE	NONE	NONE	NONE	NONE	NONE	
5	2	Doe	John	June 30, 2010	XX/XX/XX	N/A	Admin	Describe Category	Y	S	S- 3 Days
6	3	Doe	Thomas	Dec 1, 2005	XX/XX/XX	XX-YY	Admin	Describe Category	N	U	NONE
7					XX/XX/XX	XX-YY	Admin	Describe Category	N	E	NONE
8											
9											
10	Notes:										
11	In the example above, Officer #1 (Jane Doe) has not complaints submitted, but still needs to be listed										
12	In the example above, Officer #2 (John Doe) has more than one complaint (two in this example). Add a row for each additional complaint for each officer in the case of multiple complaints										
13											
14											
15	Disposition Codes:										
16	S - Sustained										
17	E - Exonerated										
18	NS - Not Sustained										
19	U - Unfounded										
20											
21	Discipline Codes:										
22	WR - Reprimand										
23	S - Suspension										
24	RT - Re-Training										
25	RN - Resignation										
26	T - Termination										

Disciplinary Records of Transferred Officers Submission Template

Analysis

1. Complaint Status: 3

In June 2022, MA POST adopted final regulations 555 CMR 1.00 to establish rules governing the Receiving, Investigating, Hearing and Adjudicating Complaints regarding Law Enforcement Officers in Massachusetts. The regulations generally require reporting all credible and non-minor complaints to MA POST, regardless of whether the allegations have been substantiated. Complaints are considered “any credible report, written or oral, evidencing or alleging the misconduct of an officer from a member of the public, personnel at the agency, or any other source.”¹⁹⁹ As part of the procedure, law enforcement agencies are

¹⁹⁹ 555 CMR 1.01(1).

required to take certain actions on the complaint (as described below) within two days of receipt. There are distinct procedures set forth, based on the category of the following types: 1) complaints relating to minor matters including discourtesy, tardiness, grooming violations and other “basic work rule violations”²⁰⁰ that do not involve allegations relating to discrimination, excessive, prohibited or deadly force or actions which resulted in serious bodily injury or death (“Minor Violations”) and 2) complaints that are not Minor Violations (“Non-Minor Violations”).

Complaints of Minor Violations

Law enforcement agencies are not required to submit copies of the complaints for Minor Violation to MA POST, provided the complaints are resolved under the agency’s internal resolution policy, which must also satisfy MA POST’s minimum requirements for such policies.²⁰¹ If the agency does not have a compliant internal resolution policy, the agency shall maintain documentation of the complaint and related summary materials.²⁰² Such complaints and policies must be made available to MA POST upon request.²⁰³

Complaints of Non-Minor Violations

Complaints (written or non-written) of Non-Minor Violations must be transmitted to MA POST. Agencies must also submit supporting documentation and related information (except as noted below) including but not limited to the officer’s name and certification number, date and location of the incident, alleged victim’s race, ethnicity, sex, gender identity and sexual orientation and whether the complainant alleges that the officer’s conduct involved acts of race, gender or other discrimination.²⁰⁴ However, agencies do not have to forward “investigatory materials that were necessarily compiled out of the public view by law enforcement or other investigatory officials, the disclosure of which materials to the commission would prejudice the possibility of effective law enforcement to the extent that such disclosure would not be in the public interest.”²⁰⁵ Agencies must also forward patterns of misconduct complaints.²⁰⁶

2. Misconduct Definition: 3

The law requires the newly created MA POST Commission to aggregate disciplinary history about each officer employed by a law enforcement agency in Massachusetts. Through mandatory reporting by the local law enforcement agencies, MA POST is collecting information on the officer’s licensing status and disciplinary history. While each agency may investigate individual complaints and interpret agency policies and procedures for each allegation, the administrator, MA POST, requires reporting a summary of disciplinary history to the database.

3. Record Details: 3

The MA POST Commission is also required to compile summaries of disciplinary records of all active officers employed by law enforcement agencies in Massachusetts.²⁰⁷ Law enforcement agencies are required to provide a listing of disciplinary records including key information about each law enforcement officer in the agency such as name, start date of employment and complaint data including:

- Date of complaint

²⁰⁰ 555 CMR 1.01(1)(a).

²⁰¹ 555 CMR 1.01(1)(a)3a.

²⁰² 555 CMR 1.01(1)(a)3b.

²⁰³ 555 CMR 1.01(a)(3c).

²⁰⁴ 555 CMR 1.01(b).

²⁰⁵ 555 CMR 1.01(c).

²⁰⁶ Ibid.

²⁰⁷ MA POST Website, Disciplinary Records, <https://www.mass.gov/info-details/post-commission-disciplinary> records.

- Nature of complaint (charge(s)/infraction/violation)
- Internal affairs investigation (file/control number)
- Investigation (admin/criminal)
- Administrative leave? (Y/N)
- Disposition (sustained, exonerated, not sustained and unfounded)
- Discipline (reprimand, retraining, suspension, termination or resigned)

Law enforcement agencies are also required to submit this information for officers who have been transferred or ended their employment with the agency. For transferred officers, agencies are also required to report two additional fields, employment end date (referring to the end of the individual's employment with the agency) and notes (allowing for any explanatory comments).

If an officer resigns during an agency investigation, prior to the conclusion of an agency investigation or prior to the imposition of agency discipline, the agency must immediately transmit to the MA POST the officer's full employment history, a description of the events or complaints surrounding the resignation, and a recommendation by the head of the agency for disciplinary action by the commission, including retraining or suspension or revocation of the officer's certification.

In addition, agencies are required to submit significant details of the internal investigations to MA POST. On completion of the internal investigation of the complaint, the agency shall immediately transmit the investigation report to the MA POST on the prescribed form that includes a description of the investigation and disposition of the complaint, a list of witnesses interviewed, whether witnesses or evidence were inaccessible and a description of the circumstances as to the unavailability of such witnesses and recommended disciplinary action by the agency including retraining, suspension or termination and recommended disciplinary action by the agency including retraining, suspension or termination.²⁰⁸ On final disposition of the complaint, the agency also is to transmit the final discipline imposed among other details of the investigation and disposition.²⁰⁹

4. Access Rights: 2

MA POST is required to maintain a publicly, searchable database of information regarding officers who are certified, conditionally certified, whose certifications are pending, restricted, limited or suspended and officers who have been decertified or not recertified.²¹⁰ Information will be included in the database, subject to the health and safety of the officers.²¹¹ While agencies are required to submit significant information regarding Non-Minor complaints, internal investigations and final disposition to MA POST, not all such information will be made available to the public (exonerated matters are included, but unfounded and unsubstantiated complaints are excluded)²¹². As of October 2022, when MA POST approved the draft regulations for the public database, the following information²¹³ is expected to be disclosed:

1. The officer's first and last name;
2. The officer's current certification status in Massachusetts;
3. The dates on which the officer was first certified and was most recently certified in Massachusetts;
4. All of the officer's employing law enforcement agencies in Massachusetts and elsewhere, and the dates of such the officer's employment with such agencies;

²⁰⁸ 500 CMR 1.01(3).

²⁰⁹ 500 CMR 1.01(4).

²¹⁰ Draft 555 CMR 8.05.

²¹¹ Ibid.

²¹² Draft 555 CMR 8.05(10).

²¹³ Draft 555 CMR 8.05(4).

5. Commendations received by the officer in connection with his/her law enforcement work;
6. The date of, and reason for, any decertification by the Commission or by a comparable body in any other jurisdiction;
7. The beginning date and end date of, and the reason for, any suspension of certification by the Commission;
8. Regarding any retraining order issued, the date of the order, the reason for the order, the type of any retraining ordered, and the any date of completion of any the retraining ordered retraining;
9. A copy of each final opinion, decision, order, set of findings, and vote issued by MA POST regarding any proceedings concerning the officer, accessible in a commonly available electronic format;
10. A summary of the officer's disciplinary record, based on information provided by agencies that have employed the officer, excluding unsustained or unfounded complaints; and
11. Information concerning any decision that reversed or vacated an action adverse to the officer, or that exonerated the officer in relation to a particular matter, where such action or matter is referenced in the database.

5. Audit and Compliance: ?

There is no current information on audit or compliance practices for any of the four databases.

6. Record Retention: ?

There is no current information on database-specific Record Retention policies.

7. Reporting Frequency: 3

Law enforcement agencies are required to transmit complaints, subject to the conditions described above (principally Minor Violation complaints are not reportable to MA POST), regarding an officer to the MA POST within 2 business days from the agency's receipt.²¹⁴ Internal investigations of the Non-Minor Violations shall commence within 14 days of the agency's receipt of the complaint and be completed within 90 days of such receipt.²¹⁵

²¹⁴ 500 CMR 1.01(1).

²¹⁵ 500 CMR 1.01(2)(a), (d).

14. National Law Enforcement Accountability Database

Background

In 2020, the deaths of George Floyd and Breonna Taylor sparked demands for police reform across the country. On May 25, 2022, President Joe Biden signed an executive order titled “Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety.” The order includes presidential action addressing multiple issues including improving training for investigations, supporting officer wellness, banning chokeholds and restricting no-knock warrants. Most notably, the order created the National Law Enforcement Accountability Database.

The order mandates that within 240 days of May 25, 2022, “the Attorney General shall establish the National Law Enforcement Accountability Database as a centralized repository of official records documenting instances of law enforcement officer misconduct as well as commendations and awards.”²¹⁷ These records will include “official records documenting officer misconduct, including, as appropriate: records of criminal convictions; suspension of a law enforcement officer’s enforcement authorities, such as de-certification; terminations; civil judgments, including amounts (if publicly available), related to official duties; and resignations or retirements while under investigation for serious misconduct or sustained complaints or records of disciplinary action based on findings of serious misconduct.” These records will be included to the maximum extent that the law allows.²¹⁶

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes the analysis of the accountability database against the Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
National Law Enforcement Accountability Database	1	3	?	2	2	?	3

Assumptions

This analysis is based on the text of the president’s executive order. As the database is built, the assessment of each design element may be subject to change.

Analysis

1. Complaint Status: 1

The database will include substantiated complaints as well as convictions, terminations, decertifications, civil judgments, resignations and retirements while under investigation for serious misconduct, and disciplinary actions for serious misconduct. Currently, the executive order does not contemplate including cleared or exonerated allegations.

²¹⁶ Executive Order 14074 of May 25, 2022, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, 87 FR 32945, Sec 5, <https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and>.

2. Misconduct Definition: 3

The executive order does not create or explicitly define a federal definition for misconduct. It does define “serious misconduct” as “excessive force, bias, discrimination, obstruction of justice, false reports, false statements under oath, theft, or sexual misconduct.” The executive order states that Federal Law Enforcement Agency’s will be required to submit information defined as misconduct. Other Law Enforcement Agency’s (State, Tribal, local and territorial) will be encouraged, but not required, to submit. Our analysis is based on the mandated federal law enforcement agency submissions only. The database will contain sustained complaints or records of disciplinary action based on sustained misconduct.²¹⁷

3. Record Details: ?

The President’s order states that the database will include, “all available information that the [Attorney General] deems necessary, appropriate, and consistent with law and with considerations of victim confidentiality, concerning misconduct by Federal law enforcement officers relevant to carrying out their official duties.”²¹⁸ The federal database will also utilize publicly accessible and reliable sources of information such as court records, federal records from DOJ databases, information held by other agencies or entities by entering into agreements with the heads of other agencies or entities.²¹⁹ Although the order says that “all available information” will be included, it is unclear how many data fields will ultimately be available.

4. Access Rights: 2

The database will be accessible to state and local law enforcement agencies for hiring purposes. The Attorney General will make the aggregated data available to law enforcement agencies and will further determine if, when and/or how records from the database may be accessible to the public. There will also be a publicly available annual report of anonymized, aggregated data.

5. Audit and Compliance: 2

The order states that, “the [Attorney General] will establish appropriate procedures to ensure that the records stored in the Accountability Database are accurate.”²²⁰ As the database is still in development, details are unknown surrounding a formal audit and to what extent, if at all, incentives or disincentives will be incorporated.

6. Record Retention: ?

The order does not identify any data retention requirements.

7. Reporting Frequency: 3

The order requires that data be submitted quarterly.²²¹

²¹⁷ Ibid. at Sec.5, part b (ii)

²¹⁸ Ibid. at Sec.5, part b (i)

²¹⁹ Ibid. at Sec.5, part d (i)

²²⁰ Ibid. at Sec.5, part b (iv)

²²¹ Ibid. at Sec.5, part c (i)

15. North Carolina Officer Search: Revocation/Suspension Data

Background

In the fall of 2021, the Criminal Justice Reform Bill (Senate Bill 300, now Session Law 2021-138) was signed into law. The bill contains many components related to LEO conduct. The bill requires that the North Carolina Criminal Justice Education and Training Standards Commission search the National Decertification Index (NDI) for every applicant to determine if an applicant has any record that would disqualify the application for certification. Additionally, the bill requires that the Commission create a publicly accessible statewide database containing all revocations and suspensions of law enforcement certifications.²²² The law requires the database include revocations and suspensions of law enforcement certifications in the database. To use the database, users must search for a specific officer by name.

The bill also mandates the development and implementation of an early warning system by each law enforcement agency. The early warning systems will include information, at a minimum, regarding incidents involving the discharge of a firearm, use of force, vehicle collisions and citizen complaints.²²³

The bill also requires that the commission create a critical incidents database to be used by law enforcement only.²²⁴ Critical incidents are defined as an incident involving any use of force by a law enforcement officer that results in death or serious bodily injury to a person. Law enforcement and justice officers have the right to a hearing in superior court if they dispute being involved in a critical incident, prior to being added to the critical incidents database. Of the three systems established by the bill, only the statewide database will be publicly accessible. Information collected for the early warning systems and critical incidents database that is confidential under state or federal law will remain confidential.²²⁵

For purposes of this analysis, only the publicly accessible statewide database, titled “Officer Search: Revocation/Suspension Data,” is evaluated.

Summary of Analysis

Based on information available as of October 2022, the graphic below summarizes our analysis of the North Carolina Officer Search: Revocation/Suspension Data, which was created as a result of Session Law 2021-138, against our Design Framework.

	Complaint Status	Misconduct Definition	Record Details	Access Rights	Audit & Compliance	Record Retention	Reporting Frequency
NC Officer Search: Revocation/Suspension Data	1	2	1	3	?	?	?

²²² North Carolina Criminal Justice Reform, Session Law 2021-138, Part XV, Section 15.(a),(b); and Part I Section 1.(a) , (b), July 26, 2022, <https://www.ncleg.gov/Sessions/2021/Bills/Senate/PDF/S300v8.pdf>.

²²³ Ibid. at Part VIII, Sec. 8.(a).

²²⁴ Ibid. at Part III, sec. 3.(a)-(e).

²²⁵ Ibid., Part III, sec. 3.(d). and Part VIII, sec. 8.(a).

Analysis

1. Complaint Status: 1

The statewide database tracks revocations and suspensions of certifications only. This is available to the public on the website.²²⁶

2. Misconduct Definition: 2

North Carolina law establishes standards for suspension, revocation and denials of a license. A “criminal justice officer” can lose licensure for reasons including but not limited to:

- Having committed or been convicted of (1) a felony offense or (2) a criminal offense for which punishment included imprisonment for more than two years.
- Failure to enroll in and complete the required basic training within prescribed time periods.
- Failure to meet or maintain one or more of the minimum employment standards.
- Conviction of a motor vehicle offense requiring the revocation of the officer's driver's license or any other offense involving moral turpitude.
- Being discharged by a criminal justice agency for lack of the mental or physical capabilities required.
- Failure to satisfactorily complete the minimum in-service training requirements.
- Refusing to submit to a drug screen or producing a positive result on a drug screen.²²⁷

The law requires that the database include all revocations and suspensions of law enforcement certifications in the database. Cases of misconduct that do not result in actions against an officer's license/certification are not included in the database.

3. Record Details: 1

The database includes officer name, certification status, date of separation, division, and agency name. The database does not include descriptions of the event that led to the revocation or suspension, demographic information, information about the complainant, or details on the investigation.

4. Access Rights: 3

The database is accessible to the public. The purpose of the database was to create a centralized location for the public to view revocations and suspensions of law enforcement certifications in the state of North Carolina.

5. Audit and Compliance: ?

There is no information available regarding audits, compliance penalties, Record Retention, or frequency of updates to the database.

6. Record Retention: ?

No information available.

7. Reporting Frequency: ?

No information available.

²²⁶ Officer search: Revocation/suspension data. NCDNJ. (2022, October 12). Retrieved October 31, 2022, from <https://ncdoj.gov/officer-search/>

²²⁷ 12 N.C. Admin. Code 09A.0204(a), (b)(1)-(16), <https://www.law.cornell.edu/regulations/north-carolina/12-N-C-Admin-Code-09A-.0204>

Use of this Report is subject to the terms and conditions applicable to content on <https://www.ceoaction.com/legal/>