IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JASON LEOPOLD,

Plaintiff,

v.

MICHAEL G. SULLIVAN,

Defendant.

Civil Action No. 1:25-cv-01026 (BAH)

MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT

Allyson Veile
Adam A. Marshall
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1020
Washington, DC 20005
Phone: 202.800.3534
Facsimile: 202.795.9310
Email: aveile@rcfp.org
Email: amarshall@rcfp.org

Counsel for Plaintiff

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTRODUCTION AND SUMMARY OF ARGUMENT 1

BACKGROUND 4

I. The U.S. Capitol Police. 4

II. The events of January 6, 2021 and scrutiny over the Capitol Police's response. 6

A. Public discussion and scrutiny over Capitol Police's preparedness and response. 6

B. Governmental investigations and reports scrutinizing the Capitol Police's response. 10

III. Plaintiff's Request and Procedural History 12

LEGAL STANDARDS 15

ARGUMENT 16

I. The balance of interests clearly and indisputably weighs in favor of disclosure under the common law. 16

A. The public has a substantial interest in accessing the directives of the U.S. Capitol Police, particularly those in place on January 6, 2021. 16

1. The general public interest in the openness of governmental processes strongly favors access to the U.S. Capitol Police's governing policies. 17

2. The public has a powerful interest in accessing the directives to evaluate USCP's preparedness and response to January 6. 21

B. Defendant fails to articulate any meaningful harm that would flow from disclosure of the directives that do not contain security information. 25

1. USCP's use of the "Law Enforcement Sensitive" label does not relieve it of its burden to articulate a specific harm flowing from disclosure. 25

2. Defendant's categorical assertion that some directives reflect "law enforcement techniques" is insufficient to overcome the public interest. 26

3. Defendant's categorical assertion that some directives reflect "administrative practices" is insufficient to overcome the public interest. 29

4. Defendant's categorical assertion that some directives reflect "internal personnel practices" is insufficient to overcome the public interest. 31

C. Defendant has failed to justify withholding the entirety of the directives it avers contain "security information." 33

1. Section 1979 establishes at least three criteria for information to qualify as "security information," which USCP has not demonstrated are met for each of the directives it seeks to withhold. 34

2. Even if any of the directives contain "security information," Defendant has a ministerial duty to release all reasonably segregable information from those directives..40

II. The other mandamus factors favor issuance of the writ to enforce the public's common law right to access these directives. 44

CONCLUSION 45

TABLE OF AUTHORITIES

Cases

ACLU v. Dep't of Just.,
655 F.3d 1 (D.C. Cir. 2011).....25

ACLU of N. Ca. v. Dep't of Just.,
880 F.3d 473 (9th Cir. 2018).....29

Ass'n of Retired R.R. Workers v. U.S. R.R. Ret. Bd.,
830 F.2d 331 (D.C. Cir. 1987).....43

Blackwell v. FBI,
646 F.3d 37 (D.C. Cir. 2011).....29

CIA v. Sims,
471 U.S. 159 (1985).....43, 44

Citizens for Resp. & Ethics in Wash. v. Dep't of Just.,
746 F.3d 1082 (D.C. Cir. 2014).....17, 18, 19

Citizens for Resp. & Ethics in Wash. v. DHS,
525 F. Supp. 3d 181 (D.D.C. 2021).....31, 33

Cobell v. Norton,
157 F. Supp. 2d 82 (D.D.C. 2001).....24

Ctr. for Nat'l Sec. Studies v. Dep't of Just.,
331 F.3d 918 (D.C. Cir. 2003).....45

Dep't of Just. v. Reps. Comm. for Freedom of the Press,
489 U.S. 749 (1989).....18, 26, 36

Dhiab v. Trump,
852 F.3d 1087 (D.C. Cir. 2017).....28

E.E.O.C. v. Nat'l Child.'s Ctr., Inc.,
98 F.3d 1406 (D.C. Cir. 1996).....2

Elec. Priv. Info. Ctr. v. Dep't of Just.,
511 F. Supp. 2d 56 (D.D.C. 2007).....43

Founding Church of Scientology of Wash. D.C., Inc. v. Nat'l Sec. Agency,
610 F.2d 824 (D.C. Cir. 1979).....29

In re Aiken Cnty.,
725 F.3d 255 (D.C. Cir. 2013).....45

In re Fort Totten Metrorail Cases,
960 F. Supp. 2d 2 (D.D.C. 2013).....20

In re L.A. Times Commc'ns LLC,
28 F.4th 292 (D.C. Cir. 2022).....18, 20

In re L.A. Times Commc'ns LLC,
628 F. Supp. 3d 55 (D.D.C. 2022).....34

In re Leopold to Unseal Certain Elec. Surveillance Applications & Ords.,
964 F.3d 1121 (D.C. Cir. 2020).....41

In re Nat'l Broad. Co.,
653 F.2d 609 (D.C. Cir. 1981).....19

In re Appl. of United States for 2703(d) Order,
548 F. Supp. 3d 31 (D.D.C. 2021).....41

Jud. Watch, Inc. v. Nat'l Archives & Recs. Admin.,
214 F. Supp. 3d 43 (D.D.C. 2016).....44

Jud. Watch, Inc. v. Schiff,
998 F.3d 989 (D.C. Cir. 2021).....16, 17, 21

L.A. Press Club v. Noem,
171 F.4th 1179 (9th Cir. 2026).....19

**Leopold v. Manger*,
102 F.4th 491 (D.C. Cir. 2024).....*passim*

Leopold v. Manger,
630 F. Supp. 3d 71 (D.D.C. 2022).....13

**Leopold v. Sullivan*,
823 F. Supp. 3d 59 (D.D.C. 2026).....*passim*

Lopez v. Council on Am.-Islamic Rels. Action Network, Inc.,
826 F.3d 492 (D.C. Cir. 2016).....16

**Metlife, Inc. v. Fin. Stability Oversight Council*,
865 F.3d 661 (D.C. Cir. 2017).....1, 32, 35

Mokhiber v. Davis,
537 A.2d 1100 (D.C. 1988).....18

N.Y. Times Co. v. U.S. Secret Serv.,
17 Civ. 1885 (PAC), 2018 WL 722420 (S.D.N.Y. Feb. 5, 2018).....33

Nixon v. Warner Commc'ns, Inc.,
435 U.S. 589 (1978) 1, 15, 17, 21

Parhat v. Gates,
532 F.3d 834 (D.C. Cir. 2008).....26

Riley v. California,
573 U.S. 373 (2014) 28

Rivera-Rodriguez v. Dep't of Just., Exec. Off. of U.S. Att'y,
No. 1:19-cv-02510 (APM), 2022 WL 136793 (D.D.C. Jan. 14, 2022).....43

Schilling v. U.S. House of Representatives,
102 F.4th 503 (D.C. Cir. 2024).....15

Serv. Emps. Int'l Union Nat'l Indus. Pension Fund v. *Jersey City Healthcare Providers, LLC*,
358 F. Supp. 3d 12 (D.D.C. 2019).....42

Shapiro v. Dep't of Just.,
893 F.3d 796 (D.C. Cir. 2018).....31

Stein v. Sec. & Exch. Comm'n,
266 F. Supp. 3d 326 (D.D.C. 2017).....43

Teva Pharms. USA, Inc. v. Kennedy,
187 F.4th 587 (D.C. Cir. 2026).....35

Trump v. Thompson,
20 F.4th 10 (D.C. Cir. 2021)……..22

United States v. Hubbard,
650 F.2d 293 (D.C. Cir. 1980).....17, 18

United States v. Jackson,
No. 1:21-mj-00115, 2021 WL 1026127 (D.D.C. Mar. 17, 2021) 17, 21

United States v. Texas,
507 U.S. 529 (1993) 35

United States v. Torrens,
560 F. Supp. 3d 283 (D.D.C. 2021).....21, 25

**Wash. Legal Found. v. U.S. Sent'g Comm'n*,
17 F.3d 1446 (D.C. Cir. 1994).....*passim*

**Wash. Legal Found. v. U.S. Sent'g Comm'n*,
89 F.3d 897 (D.C. Cir. 1996).....1, 2

Statutes

2 U.S.C. § 1901 4

2 U.S.C. § 1961 4

2 U.S.C. § 1966 4

2 U.S.C. § 1967 4

2 U.S.C. § 1969 4

2 U.S.C. § 1979 ..... *passim*

49 C.F.R. § 1520 38

49 C.F.R. § 1542 38

49 C.F.R. § 1544 38

49 C.F.R. § 1548 38

49 U.S.C. § 114 38

5 U.S.C. § 552 ..... 17, 43

Pub. L. No. 108-447, 118 Stat. 2809 (2004) 36

Other Authorities

150 Cong. Rec. E2205-03, 2004 WL 2935758 (Nov. 20, 2004) 36

Fed. Bureau of Prisons, Policy No. P5562.05 (Hunger Strikes) (July 29, 2005), https://www.bop.gov/policy/progstat/5562_005.pdf 28

H.R. Rep. No. 108-577 (2004) 36

H.R. Rep. No. 116-447 (2020) 5

H.R. Rep. No. 117-80 (2021) 5

U.S. Dep't of Just., Off. of Community Oriented Policing Servs., *Standards and Guidelines for Internal Affairs: Recommendations from a Community of Practice*, https://perma.cc/42NQ-MT4Q (last visited Nov. 7, 2026) 21

Rules

Fed. R. Civ. P. 56(a) 16

INTRODUCTION AND SUMMARY OF ARGUMENT

Plaintiff Jason Leopold ("Plaintiff"), an investigative journalist, seeks to compel Defendant Michael G. Sullivan, in his official capacity as Chief of United States Capitol Police ("USCP" or "Capitol Police"), to comply with his duty under the common law to provide access to USCP directives in place on January 6, 2021—the most significant breach of the Capitol in 200 years.

The common law protects "the public's interest in keeping 'a watchful eye on the workings of public agencies.'" *Wash. Legal Found. v. Sent'g Comm'n*, 89 F.3d 897, 905 (D.C. Cir. 1996) ("*WLF II*") (quoting *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978)). It "is a fundamental element of the rule of law," *Metlife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 663 (D.C. Cir. 2017). It applies to "the 'public records' of all three branches of government," *Leopold v. Manger*, 102 F.4th 491, 497 (D.C. Cir. 2024) ("*Leopold II*") (citation omitted), and is appropriately enforced via mandamus where the government fails to demonstrate to the court that the "specific interests favoring secrecy outweigh the general and specific interests favoring disclosure," after a close review of "the contents of the particular documents at issue." *Wash. Legal Found. v. Sent'g Comm'n*, 17 F.3d 1446, 1451–52 (D.C. Cir. 1994) ("*WLF I*") (citation and quotation omitted).

This is the second lawsuit Plaintiff has filed to secure the public's right of access to records which would improve the "public understanding of an immensely important historical occurrence." *Nixon*, 435 U.S. at 602. In the first iteration of this litigation, the D.C. Circuit held that the written policy directives of USCP are "public documents" for purposes of the common-law right of access but left for this Court to decide "whether the duty to provide access to records is ministerial or discretionary" in the event that Plaintiff brought the case anew. *Leopold II*, 102 F.4th at 500–01. Following Plaintiff's initiation of the instant case, this Court rejected Defendant's motion to dismiss and concluded that he must perform his ministerial duty under the common law

of complying with a court order to release the Directives at issue here if "the public's interest in the records outweighs the government's interest in secrecy—as to some or all of the directives." *Leopold v. Sullivan*, 823 F. Supp. 3d 59, 85 (D.D.C. 2026) ("*Leopold III*").

The parties now agree that the basic question remaining for summary judgment is whether Defendant's asserted "specific interests favoring secrecy outweigh the general and specific interest favoring disclosure," *WLF I*, 17 F.3d at 1451, both for the directives Defendant concedes do not contain any "security information" under 2 U.S.C. § 1979 ("Section 1979"), and for the directives Defendant asserts do contain such information. This balancing clearly and indisputably favors public access. USCP's directives reflect the "quintessential business of the public's institutions," *E.E.O.C. v. Nat'l Child.'s Ctr., Inc*., 98 F.3d 1406, 1409 (D.C. Cir. 1996), just as judicial decisions have long been recognized to reflect the business of the courts. The public has a profound interest in accessing these directives to evaluate the adequacy of USCP's policies for carrying out its mission "to protect the Congress—its Members, employees, visitors and facilities." Pl.'s Statement of Undisputed Facts ("SMF") ¶ 1. And in this case, the public has a right to understand what role these policies may have played in the Capitol being overrun on January 6.

Because it is impossible to apply the common-law balancing test "without knowing precisely what records [are] at issue," *Leopold II*, 102 F.4th at 500 (citation omitted), "a comprehensive index" thereof is necessary to aid this Court's review. *WLF II*, 89 F.3d at 906. USCP's proffered index, however, fails its most basic purpose. It does little more than re-phrase the names of the directives and assert their release would result in "harm" ranging from the benign to the implausible. USCP fails to meet its burden to avoid disclosure under the common law.

As to the directives USCP concedes do not contain any "security information," as that term is defined in Section 1979, its assertions are both unsubstantiated and belied by the fact that federal

and local law enforcement agencies across the country make analogous policies available to the public. There is no evidence that providing such basic transparency has inhibited those agencies' functionality. And, in any event, USCP's arguments do not overcome the general or specific public interests in these directives. They must be released.

As to the directives USCP avers were designated "security information" under Section 1979, it offers no engagement, whatsoever, with the substance of that law or any explanation of why such a designation is proper. Moreover, this Court has already concluded that the "plain text" of Section 1979 "protects only 'security information' itself, not surrounding non-security-information contained in the same document as security information." *Leopold III*, 823 F. Supp. 3d at 87 (citation omitted). USCP has not and cannot show that the vast majority of the directives it has designated as "security information" satisfy the requirements of that statute, much less that each and every sentence of these directives must be withheld. Accordingly, those directives, too, must be released in light of the general and specific public interests Plaintiff has identified.

To aid this Court's analysis under the common law, Plaintiff submits a Response to Defendant's Index, which contains a directive-by-directive response to the government's assertions, cross-referencing the undisputed material facts and the record evidence in this case. The Response Index identifies both the general and specific public interests in each directive and rebuts Defendant's assertions of harm. Additionally, for the directives that Defendant avers have been "designated" as "security information" under Section 1979, Plaintiff shows why that designation is inappropriate and why Defendant has not met its segregability obligations.

For the reasons stated herein, Plaintiff respectfully requests that the Court deny Defendant's motion for summary judgment, grant his cross-motion for summary judgment, and enter an order requiring Defendant to produce to Plaintiff the directives that remain at issue, with

only narrow redactions for information (if any) that the Court determines properly consist of "security information," as that term is defined by Section 1979. In the event the Court believes *in camera* review would aid its review, Plaintiff respectfully requests that review include Directives 1032.001, 1073.001, 1020.004, 1030.001, and 1033.001.

BACKGROUND

I. The U.S. Capitol Police.

The principal mission of the Capitol Police is "to protect the Congress—its Members, employees, visitors and facilities—so it can fulfill its constitutional and legislative responsibilities in a safe, secure and open environment." SMF ¶ 1. USCP is required to "police the United States Capitol Buildings and Grounds under the direction of the Capitol Police Board[.]" 2 U.S.C. § 1961(a). USCP officers are authorized to "make arrests within the United States Capitol Buildings and Grounds for any violations of any law of the United States, of the District of Columbia, or of any State, or any regulation promulgated pursuant thereto." *Id.* USCP officers are also authorized to make arrests outside Capitol Grounds in certain circumstances. *Id.* § 1967. Additionally, USCP "is authorized to protect, in any area of the United States, the person of any Member of Congress, officer of the Congress . . . and any member of the immediate family of any such Member or officer, if the Capitol Police Board determines such protection to be necessary." *Id.* § 1966(a). For its part, the Capitol Police Board is empowered to make regulations for the "movement of all vehicular and other traffic, including the parking and impounding of vehicles and limiting the speed thereof, within the United States Capitol Grounds," *Id.* § 1969(a). USCP is subject to oversight from the Senate's Committee on Rules and Administration and the House of Representatives' Committee on House Administration. *Id.* § 1901b(a). USCP is also subject to oversight by its Office of the Inspector General. SMF ¶ 10.

Like many police departments throughout the country, USCP "maintains policies and

procedures that provide guidance to employees for the performance of their duties." *Id.* ¶ 11. USCP "policies and procedures are categorized as either an SOP or a Directive." *Id.* ¶ 12. "SOPs are policies that are specific to a particular bureau or division, whereas Directives are department-wide guidance." *Id.* ¶ 13. USCP's "[e]mployees are required to obey all Departmental rules, regulations, Directives, orders, policies and procedures." *Id.* ¶ 14. However, USCP does not make its directives or SOPs available to the public, unlike many federal and state law enforcement entities throughout the country including the District of Columbia's Metropolitan Police Department ("MPD"), the United States Park Police ("Park Police"), the Department of Homeland Security ("DHS"), the Transportation Security Administration ("TSA") and Homeland Security Investigations ("HSI"), the Maryland Capitol Police ("MCP"), the New York Police Department ("NYPD"), the Atlanta Police Department ("APD"), the Los Angeles Police Department ("LAPD"), and many others. *Id.* ¶¶ 143–302.

In 2020, the House Committee on Appropriations expressed concern about USCP's lack of transparency, including by "encourag[ing] the USCP to develop a policy and procedure for the sharing of information that follows the spirit of the Freedom of Information Act." H.R. Rep. No. 116-447, at 22 (2020). It also encouraged the Capitol Police Inspector General to "make an effort to make appropriate reports public if they do not compromise law enforcement activities, national security, or Congressional security and processes without redaction." *Id.* When USCP did not adopt Congress' suggestion, the following year the House Committee "direct[ed] the USCP to develop a policy and procedure for the sharing of information that follows the spirit of the Freedom of Information Act," and further, instructed "the Inspector General to institute procedures to make reports publicly available whenever practicable and to begin publishing reports on its website." H.R. Rep. No. 117-80, at 26 (2021). Beginning in mid-2023, USCP's Inspector General began

publicly releasing such reports on its website, with certain redactions applied. SMF ¶¶ 132–139.

II. The events of January 6, 2021 and scrutiny over the Capitol Police's response.

On January 6, 2021, a mob attacked and breached the U.S. Capitol, disrupting a joint session of Congress that was certifying the results of the 2020 presidential election. *Id*. ¶¶ 15–17. It was the "most significant breach of the Capitol in over 200 years." *Id*. ¶ 18. "Seven hours elapsed between when the security perimeter was first breached and when USCP declared the building secure." *Id*. ¶ 19. In the days and months that followed, USCP was "thoroughly—and understandably—scrutinized" over its preparedness and response to the attack, *id*. ¶ 21, including by members of the press and public and by governmental oversight bodies, *id*. ¶¶ 22–102.

A. Public discussion and scrutiny over Capitol Police's preparedness and response.

In the wake of January 6, many news articles focused on whether USCP had adequate intelligence and an appropriate response plan in the lead up to January 6. For example, one news outlet reported that "during planning meetings prior to Jan. 6 led by the Justice Department, city officials and federal law enforcement agencies requested only modest support from the National Guard and did not anticipate large-scale violence," despite reporting that "online forums popular with far-right activists were filled with threats and expectations of violence in the days leading up to Jan. 6." *Id*. ¶¶ 23–25. As January 6 was underway, USCP "failed to deploy enough officers to protect the Capitol from rioters, and put them out in regular uniforms instead of riot gear." *Id*. ¶ 26. "Meanwhile, whatever plan the Capitol Police had to request reinforcements didn't work." *Id*. ¶ 27. Another outlet reported that USCP officers "la[id] ultimate blame for what happened on Jan. 6 at the feet of their managers, who they said appeared utterly blindsided by the attack, despite weeks of open planning by the conspirators online." *Id*. ¶¶ 35–36. The same article reported that "[u]sually, on a day when police leaders are expecting a big protest or riot, they'd organize a roll call, where they'd inform officers of the perceived threats and give them information about what

to expect," but "no such meeting occurred" in advance of the insurrection. *Id.* ¶ 37. Instead, USCP "management didn't even take 'simple measures' ahead of the attack like building a temporary barrier around the Capitol ahead of time." *Id.* ¶ 38.

In September 2021, Plaintiff published an article showing that "[t]he chief of the Capitol Police and its top intelligence officer personally approved permits for six demonstrations to be held on Jan. 6, 2021, despite signs that one of the applications was filed for an organization that didn't exist and that five of them were a proxy for a group staging large, violent protests across the country." *Id.* ¶¶ 47–48. Despite "documented concerns that organizers had attempted to conceal their affiliation with Ali Alexander, the right-wing activist behind the group Stop the Steal, in a secret effort to coordinate their protests against the results of the 2020 presidential election . . . the Capitol Police force's intelligence assessment said there were 'no plans for participants to enter the buildings' and noted 'no adverse intelligence related to the upcoming event.'" *Id.* ¶ 49. And USCP "assessed 'the Level of Probability of acts of civil disobedience/arrests to occur' during the demonstration 'as Highly Improbable.'" *Id.*

Other reporting focused on whether USCP's officers had adequate training, policies, and protective equipment to respond to the attack. One outlet reported that elected officials "wondered whether the Capitol Police were instructed to avoid confrontation," and that USCP was "so overwhelmed they didn't appear to arrest any of the rioters." *Id.* ¶¶ 28–29. Another outlet reported that "[m]ost officers who fought that day did so without helmets, face shields or gas masks that would have better protected them from chemical irritants and blunt force imposed by the rioters." *Id.* ¶ 42. The same article stated that "[t]he day before the insurrection, officers were directed to pick up helmets from the department's equipment office," but an officer assigned to a CDU "soft squad for Jan. 6, was hassled by those handling equipment distribution over whether the new

helmet was actually needed and had to negotiate to obtain it in preparation for the next day." *Id.* ¶ 43. One officer assigned to a "CDU hard squad[]" was "told by a supervisor to leave all its protective gear on a bus on the West Front and patrol without it" on January 6. *Id.* ¶ 44. Meanwhile, "Capitol Police grenadiers, who are trained and equipped to use less lethal munitions, were in short supply that day[.]" *Id.* ¶ 45. When the MPD stepped in to fill the void and "deployed stun grenades and large tanks of OC spray . . . many Capitol Police officers—not equipped with gas masks or face shields—were getting hit with the OC spray." *Id.* ¶ 46.

Some news articles contrasted USCP's preparation for and response to January 6 to the Black Lives Matter protests of 2020. One outlet reported that USCP had been "criticized for some of its members' light touch with the largely white crowd who participated in the attack on the Capitol, particularly in comparison to violence many non-white protesters faced this summer during the racial justice demonstrations." *Id.* ¶ 32. The same article reported that "the Capitol Police force has faced multiple lawsuits over the years, and has been plagued with allegations of racism by organizations including the U.S. Capitol Black Police Association." *Id.* ¶ 33. But because "the Capitol Police is super opaque," the public had no way to "know the racial makeup of their force," *id.* ¶ 34, much less exercise oversight over it. Another outlet similarly reported how USCP officers contrasted the January 6 attacks with "how management handled the Black Lives Matter protests" the preceding summer, noting "the contrast is stark." *Id.* ¶ 39. One officer opined "[transparency] would improve this department on every level. We're paid by the taxpayers—they should be able to access anything that goes on within this department within reason." *Id.* ¶ 40 (alteration in original).

Following January 6, USCP "launched 38 internal investigations, after reports that some officers assisted or supported pro-Trump rioters." *Id.* ¶ 53. Although "disciplinary action was

recommended in six cases," USCP "did not release the names of those being disciplined, did not specify what disciplinary measures would be taken, and did not provide details about their conduct." *Id.* ¶ 54. It was later reported by media outlets that one USCP officer had been indicted for obstruction of justice on allegations that the officer sent a Facebook direct message to one of the rioters encouraging the rioter "to delete incriminating social media posts." *Id.* ¶ 55.

Meanwhile, "competing narratives" emerged about certain aspects of the January 6 attack and USCP's response. *Id.* ¶ 62. The fatal shooting of Ashli Babbitt by a USCP officer became "particularly polemical," *id.* ¶ 61, with at least one elected official, Congressman Paul Gosar of Arizona, questioning why "a 110-pound woman with nothing in her hands, not a rock, not a stick or a bat, was shot dead" without "warnings given or escalation of command and force in proper law enforcement technique," *id.* ¶ 59. However, "USCP's Office of Professional Responsibility (OPR) determined the officer's conduct was lawful and within Department policy, which says an officer may use deadly force only when the officer reasonably believes that action is in the defense of human life, including the officer's own life, or in the defense of any person in immediate danger of serious physical injury," *id.* ¶ 60, but USCP did not release its underlying use of force policy. In June 2025, it was reported that the "Trump administration will pay a $4.975 million settlement in the lawsuit over the wrongful death of Ashli Babbitt." *Id.* ¶ 63.

Competing narratives also emerged about whether "certain 'reconnaissance tours' took place" prior to January 6, "potentially providing some rioters with a layout of the complex." *Id.* ¶ 70. In response to such allegations, one elected official "sent a letter to the US Capitol Police Board demanding release of all January 5th Capitol Security Tapes to the public in a timely manner," to dispute "recent press reports" that "the partisan January 6 Select Committee" had "falsely accused" certain officials of "leading so called reconnaissance tours." *Id.* ¶ 72–73.

Another news article reported that then-Representative-elect Lauren Boebert, had received "an exclusive after-hours tour of the Capitol building" in December 2020, on the night of the "first Stop the Steal rally" in D.C. *Id.* ¶ 65. A Capitol Police officer was photographed with her group at the top of the Capitol Dome. *Id.* ¶ 66. The article noted that it was "not clear who authorized" such a tour, that "guidelines for member-led Capitol tours state they are only available on weekdays . . . and all tours must be led by official Capitol guides, not Capitol Police officers." *Id.* ¶¶ 67–68. Congresswoman Boebert denied giving reconnaissance tours, while USCP "didn't immediately return Salon's request for comment on [the] story." *Id.* ¶ 69.

B. Governmental investigations and reports scrutinizing the Capitol Police's response.

Governmental oversight bodies who conducted investigations into January 6 and USCP's response raised many of the same questions identified in reporting from the press. The Senate Committee on Rules and Administration and Senate Homeland Security and Governmental Affairs Committee issued a report concluding, among other things, that:

- "USCP's intelligence components failed to convey the full scope of information they possessed," even though USCP had "received information from a variety of sources about threats of violence" in the lead up to January 6, *id.* ¶ 79;
- USCP "failed to prepare a department-wide operational plan for the Joint Session," *id.* ¶ 80;
- "USCP leadership also failed to provide front-line officers with protective equipment or training," *id.*;
- "Many of [USCP's] front-line officers had not received training in basic civil disturbance tactics since their initial Recruit Officer Class training," *id.*;
- USCP "did not authorize [Civil Disturbance Unit ("CDU")] platoons to use all available less-than-lethal munitions, which could have enhanced officers' ability to push back rioters," *id.*;
- "USCP's Incident Command System broke down during the attack, leaving frontline officers without key information or instructions as the events unfolded," *id.* ¶ 81;
- "USCP leadership never took control of the radio system to communicate orders to front-

line officers," *id.*;

- "Opaque processes and a lack of emergency authority delayed requests for National Guard assistance," *id.* ¶ 83.

In the House of Representatives, a Select Committee to Investigate the January 6th Attack on the United States Capitol (the "House Select Committee"), H. Res. 503 (June 30, 2021), was established and published a report (the "House Report"). *Id.* ¶¶ 85–86. The House Report described how "[f]ederal and local law enforcement authorities were in possession of multiple streams of intelligence predicting violence," and that "[t]he failure to sufficiently share and act upon that intelligence jeopardized the lives of the police officers defending the Capitol and everyone in it." *Id.* ¶ 87. The House Report also noted USCP "did not create a department-wide plan for the January 6 event," did not "cancel officers' days off," and believed a "request for the DC National Guard would not be necessary." *Id.* ¶¶ 88–90.

The Committee on House Administration also conducted oversight hearings. *Id.* ¶ 91. In testimony provided to that Committee, USCP Inspector General Michael A. Bolton discussed how in OIG's reports relating to January 6, OIG identified deficiencies such as "(a) lack of a comprehensive operational plan or adequate guidance for operational planning, (b) failure to disseminate relevant information obtained from outside sources, (c) lack of consensus on the interpretation of threat analyses, (d) dissemination of conflicting intelligence, and (e) lack of security clearances," and a lack of "adequate policies and procedures for CDU defining its responsibilities, duties, composition, equipment, and training." *Id.* ¶ 93–94. Four of OIG's January 6 reports, Flash Report 2021-I-0003-A, -C, -D, and -E, have now been released to the public in redacted form. *Id.* ¶¶ 135–138. In January 2022, then-USCP Chief J. Thomas Manger provided a statement to the Committee on Appropriations Subcommittee on the Legislative Branch detailing how, in response to recommendations issued by the Inspector General and other oversight

bodies, USCP "developed, and in many instances implemented, significant strategic, tactical, and operational improvements to *every* USCP Bureau." *Id.* ¶ 95 (emphasis in original).

The Government Accountability Office ("GAO") also issued "several reports examining federal efforts to prepare for January 6 events, gather intelligence, coordinate, and later respond to the attack." *Id.* ¶ 96. One such report described the results of GAO's survey of USCP officers who were deployed during the attack (the "GAO Survey Report"), including its findings that:

- "Related to use of force, 207 [USCP officers] felt well or somewhat prepared and 96 felt slightly or not at all prepared," *id.* ¶ 99;
- "Related to crowd control tactics, 134 felt well or somewhat prepared and 153 felt slightly or not at all prepared," *id.*;
- Respondents "felt discouraged or hesitant to use force because of a fear of disciplinary actions (57); and that leadership needed to clarify the appropriate use of force during situations like the January 6 attack (39)," *id.* ¶100;
- "Over half of respondents (180) expressed that more training was needed, including crowd control (128), very large or violent crowd control (84), and more realistic training (46)," *id.* ¶ 101.
- "108 respondents commented that more protective equipment is needed, including helmets, riot gear, and shields. Some officers noted that their gear was old or of poor quality and that it was difficult to move around in the hard gear," *id.* ¶ 102;
- "20 respondents stated that Capitol Police equipment needs to be better positioned, as some of it was not readily accessible to them during the January 6 attack," *id.*

III. Plaintiff's Request and Procedural History

On January 28, 2021, Plaintiff sent a letter to USCP's Public Information Office (PIO) requesting access to—among other public records—USCP's written directives in effect on January 6, 2021 ("Plaintiff's Request"). *Id.* ¶ 103. On February 11, 2021, USCP denied Plaintiff's Request, stating the directives were not public records. *Id.* ¶ 104. In February 2021, Plaintiff filed suit seeking a writ of mandamus ordering then-acting Chief of USCP to comply with her duty under the common law to disclose certain public records to Plaintiff, including USCP's written

directives in effect on January 6, 2021. *Id.* ¶ 105. In that proceeding, USCP represented that "a USCP Document Review Team" had determined that a subset of the directives it had identified as responsive to Plaintiff's Request did not contain "security information" as set forth in 2 U.S.C. § 1979 ("Section 1979"). *Id.* ¶ 111. Plaintiff voluntarily narrowed his request to 36 of the directives USCP conceded did not contain "security information." *Id.* ¶ 112. USCP represented that a "USCP Document Review Team" had determined that 65 other directives were "security information." *Id.* ¶ 113. USCP submitted no further evidence regarding its assertion that the 65 directives contained "security information" as defined by statute. Instead, USCP contended that "[n]one of the requested USCP directives, regardless of whether they are security information under 2 U.S.C. § 1979, constitute 'public records'" because they were "Law Enforcement Sensitive." Joyce Decl. ¶ 11 (filed at ECF No. 19-5 in *Leopold I*, No. 1:21-cv-00465).[1]

This Court dismissed for lack of subject matter jurisdiction on the parties' cross-motions for summary judgment. *Leopold v. Manger*, 630 F. Supp. 3d 71 (D.D.C. 2022) ("*Leopold I*"). As to the 36 directives that did not contain any "security information," this Court concluded that the directives were not "public records" under *WLF I* and that, in the alternative, the government's interest in secrecy outweighed the public interest. *Id.* at 83–85. As to the 65 directives that USCP averred contained "security information," this Court agreed the directives "constitute[d] security information," relying on USCP's assertions that all of the "directives 'contain operational information that would reveal [the] confidential sources and methods, investigative activities and techniques' of USCP and 'reflect the USCP's internal policies, rules, protocols, and guidance for USCP personnel on a variety of subjects.'" *Id.* at 82 (quoting Joyce Decl. ¶ 11).

The D.C. Circuit affirmed this Court's dismissal in *Leopold II*, 102 F.4th 491, but on

[1] Attached as Exhibit 28 to the Declaration of Allyson Veile ("Veile Decl.").

different grounds. As to the directives not containing any "security information," the D.C. Circuit concluded that those documents were "public records," but declined to reach the question whether they should be disclosed on the grounds that Plaintiff "failed to brief . . . whether the duty to provide access to public records is discretionary or ministerial" for purposes of mandamus relief. *Id.* at 500–01. As to the 65 directives USCP averred contained "security information," the Circuit similarly concluded that whether the duty to segregate and disclose information ***not*** made confidential by Section 1979 is nondiscretionary was "unbriefed." *Id.* at 501–02. Although Plaintiff challenged the sufficiency of the evidence in the record to support USCP's designation of the 65 "security information" directives, *id.* at 501, the D.C. Circuit declined to rule on this issue, because it was "far from clear what [Plaintiff's] Section 1979-specific argument achieves" in light of its holding on jurisdiction. *Id.* The D.C. Circuit thus left Plaintiff "free to refile his complaint with the requisite allegations to satisfy the mandamus standard," *id.* at 503, without opining on the appropriateness of USCP's designation of "security information."

This action followed. *See* Compl., ECF No. 1. Plaintiff seeks to compel Defendant to comply with his obligation under the common law to provide public access to those same USCP directives in effect on January 6, 2021. *Id.* ¶ 4. Defendant filed a motion to dismiss, ECF No. 10, which this Court denied as to "100 of the 101 directives sought," while dismissing Plaintiff's claim as to Directive 1000.002 (Retrieval of Archived Video) only, *Leopold III*, 823 F. Supp. 3d at 79, because Defendant already released that directive to Plaintiff, notwithstanding Defendant's assertion that it contained "security information." *See* ECF No. 1-2 (categorizing Directive 1000.002 as "security information"). As to the other directives, this Court recognized that "binding D.C. Circuit precedent recognizes a common law nondiscretionary duty to make . . . records available to the public when those records satisfy the two-step *WLF I* test." *Leopold III*, 823 F.

Supp. 3d at 84 (quotations omitted). Defendant's discretion to withhold the 36 directives that do not contain "security information," must "give way to the ministerial duty of complying with a court order to release the documents." *Id*. at 85. As to the 64 remaining directives USCP maintains contain "security information," Section 1979 "protects only 'security information' itself, not surrounding non-security-information contained in the same document as security information." *Id.* at 87 (citation omitted). Although in *Leopold I*, this Court concluded that USCP had "proper[ly]" designated the "security information" directives at the summary judgment stage, *id.* at 87, in the instant litigation it recognized that Plaintiff had adequately "alleged that at least some portions of these 64 directives may not be security information." *Id.* Accordingly, "should the Court find that public's interest in segregable non-security-information portions of these remaining 64 USCP policy directives outweigh the Government's interest in secrecy, defendant must fulfill his ministerial duty to produce those portions." *Id.* at 89.

Thus, the issues for summary judgment are (i) whether the balance of interests favors disclosure as to the 36 non-security information directives; (ii) whether this Court should revisit the *Leopold I* finding that the 64 remaining directives USCP avers contains "security information" were properly so designated; (iii) whether the balancing test favors disclosure of those 64 directives, or otherwise, the segregable portions thereof; and (iv) whether mandamus should issue.

LEGAL STANDARDS

The common law affords the public a "general right to inspect and copy public records and documents, including judicial records and documents." *Nixon*, 435 U.S. at 597 (footnote omitted). This right of access "extends . . . to the public records of all three branches of government, . . . including the Legislative Branch." *Schilling v. U.S. House of Representatives*, 102 F.4th 503, 507 (D.C. Cir. 2024) (first omission in original) (citation and quotation omitted). To determine whether the common law right of access applies, the D.C. Circuit has set forth a

"two-step inquiry." *Jud. Watch, Inc. v. Schiff*, 998 F.3d 989, 995 (D.C. Cir. 2021). First, the court decides whether the records at issue qualify as "'public records' covered by the common law right." *WLF I*, 17 F.3d at 1451. If so, the Government may avoid disclosure only if it demonstrates that the "specific interests favoring secrecy outweigh the general and specific interests favoring disclosure," after a close review of "the contents of the particular documents at issue (as reflected in the *Vaughn* index)." *Id.* at 1451–52 (internal quotation omitted).

Mandamus relief is available if Plaintiff shows (1) "there are no other adequate means to attain the relief sought," (2) "his right to issuance of the writ is clear and indisputable," "its issuance will compel the government official to perform a ministerial duty," and (3) "the issuing court, in the exercise of its discretion, [is] satisfied that the writ is appropriate under the circumstances." *Leopold III*, 823 F. Supp. 3d at 78–79 (citation and quotation omitted). The inquiry under the second prong merges with the merits of the *WLF I* inquiry, because the common law creates a "nondiscretionary duty to make . . . records available to the public when those records satisfy the two-step *WLF I* test." *Id.* at 84 (citation and quotation omitted) (omission in original).

Summary judgment is warranted where "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). It is appropriate "when, viewing the evidence in the light most favorable to the non-movants and drawing all reasonable inferences accordingly, no reasonable jury could reach a verdict in their favor." *Lopez v. Council on Am.-Islamic Rels. Action Network, Inc.*, 826 F.3d 492, 496 (D.C. Cir. 2016).

ARGUMENT

I. The balance of interests clearly and indisputably weighs in favor of disclosure under the common law.

A. The public has a substantial interest in accessing the directives of the U.S. Capitol Police, particularly those in place on January 6, 2021.

Both the "general public interest in the openness of governmental processes" and the

"specific nature of the . . . public interests as they relate to the document itself" compel disclosure of the directives at issue in this case. *WLF I*, 17 F.3d at 1452. USCP's directives operate not only "to ensure that the Capitol Police, and its officers, are behaving in a manner that is consistent with the Constitution" when they exercise authority over members of the public, *Leopold II*, 102 F.4th at 500, but to ensure that USCP fulfills its mission of protecting Congress. SMF ¶ 1. Also weighing heavily on the public interest "side of the scales is the incremental gain in public understanding of an immensely important historical occurrence that arguably would flow from the release" of the directives that governed USCP's preparation and response to January 6. *Schiff*, 998 F.3d at 997 (Henderson, J., concurring) (quotation omitted). Those substantial, concrete public interests readily outweigh the hypothetical and exaggerated assertions of harm levied by USCP.

1. *The general public interest in the openness of governmental processes strongly favors access to the U.S. Capitol Police's governing policies.*

The public has a substantial interest in accessing all of USCP's directives, as set forth herein and in the attached Response Index. "Access to records serves the important functions of ensuring the integrity of judicial proceedings in particular and of the law enforcement process more generally." *United States v. Hubbard*, 650 F.2d 293, 314–15 (D.C. Cir. 1980). In keeping with that principle, the public has an interest in "keep[ing] a watchful eye on the workings of public agencies," *United States v. Jackson*, No. 1:21-mj-00115, 2021 WL 1026127, at *6 (D.D.C. Mar. 17, 2021) (quoting *Nixon*, 435 U.S. at 598), and the D.C. Circuit has recognized in particular when evaluating public interest under the Freedom of Information Act, 5 U.S.C. § 552 ("FOIA"), that "[m]atters of substantive law enforcement policy . . . are properly the subject of public concern." *Citizens for Resp. & Ethics in Wash. v. Dep't of Just.*, 746 F.3d 1082, 1093 (D.C. Cir. 2014) ("*CREW*") (omission in original) (quoting *Dep't of Just. v. Reps. Comm. for Freedom of the Press*,

489 U.S. 749, 766 n.18 (1989)).[2] The directives at issue here implicate at least four distinct categories of "law enforcement process," *Hubbard*, 650 F.2d at 314, or "substantive law enforcement policy," *CREW*, 746 F.3d at 1093, bolstering the public's right of access.

First, many of the directives "operate[] to ensure that the Capitol Police, and its officers, are behaving in a manner that is consistent with the Constitution." *Leopold II*, 102 F.4th at 500. That includes USCP's policies with respect to the use of force, searches and seizures, searches and seizures involving particular groups, applications for authorization of warrants and other process, arrests and release of persons accused of crimes, and traffic enforcement.[3] The public cannot meaningfully engage in debate about USCP's policies addressing, for example, use of force, without basic information about whether those policies include "de-escalation techniques," or "instruct officers to intervene and report use of excessive force by fellow officers." *See* SMF ¶¶ 303–05 (describing news reporting on "[c]alls for police reform" for D.C. area police departments in recent years, including reforms to policies for "how officers use force against citizens"). Nor can the public exercise oversight over USCP's search of persons or suspicious activity stop reporting without basic information about the circumstances in which USCP's officers are

---

[2] Some of FOIA's exemptions require courts "to balance the [] privacy interest against the public interest in disclosure," *CREW*, 746 F.3d at 1091 (alteration in original) (citation omitted). However, the public interest analysis under the common law is broader than under FOIA. *Compare, e.g.*, *Mokhiber v. Davis*, 537 A.2d 1100, 1117 (D.C. 1988) ("A claim to access is bolstered when the materials sought will shed light on events of historical or contemporary interest to a wider audience; an issue of greater and wider public importance may create a stronger claim of access than a less important issue") *and In re L.A. Times Commc'ns LLC*, 28 F.4th 292, 298 (D.C. Cir. 2022) (public had an interest in "learning of a sitting Senator's potential violation of insider-trading laws based on information acquired in his official capacity") *with CREW*, 746 F.3d at 1093 (under FOIA "[t]he only relevant public interest . . . is the extent to which disclosure of the information sought would shed light on an agency's performance of its statutory duties or otherwise let citizens know what their government is up to" (cleaned up)).

[3] *E.g.*, Directives 1020.004, 1020.003, 1020.011, 1021.001, 1041.002, 1060.001, 1022.005, 1020.002, 1020.007, 1020.009, 1020.01, 1021.004, 1032.002, 1021.005, 1021.006, 1023.004, 1020.006, 1022.001, 1053.002.

authorized to conduct stops, pat-downs, or more intrusive searches. *See id.* ¶¶ 315–18 (describing news reporting on debate over changes to Chicago's stop and frisk policy). By the same token, the public has a substantial interest in accessing USCP's policies with respect to the exercise of First Amendment rights—including its policies with respect to demonstrations and the use of crowd-control techniques.[4] *Cf. L.A. Press Club v. Noem*, 171 F.4th 1179, 1188 (9th Cir. 2026) (recognizing use of crowd-control techniques can implicate First Amendment rights).

Second, the public has a weighty interest in evaluating the adequacy of USCP's policies that reflect how it "handle[s] the investigation and prosecution of crimes that undermine the very foundation of our government." *CREW*, 746 F.3d at 1093; *cf. In re Nat'l Broad. Co.,* 653 F.2d 609, 614 (D.C. Cir. 1981) (finding a "legitimate and important interest" in allowing the public to access for itself information about the activities of government officials) (citation omitted). This interest readily applies to USCP's policies for conducting investigations, handling crime scenes and evidence, sharing information with other agencies, and traveling in a law enforcement capacity.[5] The public likewise has an interest in evaluating the adequacy of USCP's policies with respect to processing and safeguarding personal information it may access in the performance of its functions—particularly considering that USCP may have privileged access to information about members of Congress and Congressional employees through its protective functions.[6]

Third, the public has a powerful interest in accessing information that will enable it to exercise democratic oversight over USCP's performance of its primary mission: "to protect the

---

[4] *E.g.*, Directives 1012.001 and 1020.012.

[5] *E.g.*, Directives 1032.001, 1062.001, 1033.001, 1053.001, 2023.002, 2053.019, and 1073.003.

[6] *E.g.*, Directives 2023.003, 1080.001, 2081.001, 1010.003, 2011.002, 2022.001, 2080.003, 2081.003, 2081.005, 2081.006, 2081.007, 2081.008, 2081.010, 2081.011, 2081.012, 2081.013, 2082.001, 2083.001, 2083.002, 2083.003, 2083.004, 2081.004, 2084.001, and 2081.002.

Congress—its Members, employees, visitors and facilities—so it can fulfill its constitutional and legislative responsibilities in a safe, secure and open environment." SMF ¶ 1. This interest applies to USCP's policies for controlling access to the Capitol Complex and its perimeter and securing it against threats.[7] It also extends to USCP's policies relating to preparedness for responding to emergencies and maintaining sufficient equipment for doing so,[8] including how it "utilize[s] taxpayer funds" to perform those functions. *Cf. In re Fort Totten Metrorail Cases*, 960 F. Supp. 2d 2, 7 (D.D.C. 2013) (recognizing records reflecting use of "taxpayer funds in settling lawsuits further strengthens the public's stake in their release").

Finally, the public has a substantial interest in accessing information about USCP's training policies so that it can assess whether USCP's training adequately prepares officers to fulfill USCP's mission and statutory duties while ensuring compliance with USCP's own policies and the Constitution.[9] *Cf. In re L.A. Times Commc'ns LLC*, 28 F.4th at 298 (accessing judicial records related to allegations of official misconduct raised a "powerful public interest"). And the public also has an interest in knowing "what programs and training methods and procedures USCP use to eliminate racial profiling," *see* H.R. Rep. No. 116-447, at 21 (seeking such information from USCP), because such policies reflect internal practices that are "essential in building and maintaining mutual trust and respect between agencies and the public." U.S. Dep't of Just., Off. of Community Oriented Policing Servs., *Standards and Guidelines for Internal Affairs: Recommendations from a Community of Practice* at 11, https://perma.cc/42NQ-MT4Q (last visited

---

[7] *E.g.*, Directives 1000.001, 1010.004, 1020.005, 1040.001, 1040.002, 1040.003, 1040.004, 1041.001, 1031.001, 2052.010, 2052.015, 1022.006, 1040.005, 1030.001, 1052.004, 1052.005, 1054.001, 1056.001, 1056.002, 1056.003, 1056.004, 1057.001, and 2092.004.

[8] *E.g.*, Directives 1050.001, 1052.003, 2052.011, 1073.001, 2052.006, 2071.001, 2074.003, 2093.001, 2092.002, 2092.003, and 2075.001.

[9] *E.g.*, Directives 2052.012, 2061.001, 2064.001.

Nov. 7, 2026). This interest readily extends to USCP's policies regarding bias prevention and preventing discrimination within the Department and for addressing complaints.[10] It also extends to information about USCP's organizational structure and oversight bodies.[11]

2. The public has a powerful interest in accessing the directives to evaluate USCP's preparedness and response to January 6.

In addition to these "general . . . interests," there are "specific interests favoring disclosure" of the directives at issue here. *WLF I*, 17 F.3d at 1451–52 (citation omitted). The public has an "extraordinary public interest surrounding the events that took place at the U.S. Capitol on January 6." *United States v. Torrens*, 560 F. Supp. 3d 283, 292 (D.D.C. 2021); *accord Jackson*, 2021 WL 1026127, at *6 ("This violent challenge to a constitutionally mandated process is of deep national importance and public interest . . . "). Even an "incremental gain in public understanding" of the "immensely important historical occurrence" that was January 6 would suffice. *See Schiff*, 998 F.3d at 997 (D.C. Cir. 2021) (Henderson, J., concurring) (quoting *Nixon*, 435 U.S. at 602–04). But access to USCP's policies will lead to far more than an incremental gain—it will fill critical gaps in the public's understanding of USCP's response to that day. For example, while the public knows USCP "failed to prepare a department-wide operational plan for the Joint Session," SMF ¶ 80, "organize a roll call, where they'd inform officers of the perceived threats and give them information about what to expect," *id.* ¶ 37, "build[] a temporary barrier" around the Capitol, *id.* ¶ 38, "cancel officers' days off," *id*. ¶ 89, or call on the National Guard for assistance in advance, *id.* ¶ 88, it has no access to any of USCP's policies and so has no way to assess whether USCP was required to do any of those things. Nor has the public had the opportunity to exercise democratic oversight over the improvement of USCP's policies to ensure such failures do not

[10] *E.g.*, Directives 1020.001, 2033.001, 2053.011, and 2053.002.
[11] *E.g.*, Directives 2000.001 and 2031.001.

happen again. And while the public knows USCP ultimately approved "six demonstrations to be held on Jan. 6, 2021, despite signs that one of the applications was filed for an organization that didn't exist and that five of them were a proxy for a group staging large, violent protests across the country," *id.* ¶ 48, it has no information about how USCP was supposed to evaluate permit applications.

Because Defendant's Index contains only the most bare-bones descriptions of their contents, and because the agency has refused to release any information from any of the directives at issue, it is impossible to meaningfully evaluate which might contain information relevant to these questions. For just that reason, the public's ability to evaluate the adequacy of USCP's policies in the lead up to January 6 will continue to be handicapped without access to all directives active on that day, to determine not only which speak exactly to these issues but also which do not. At a minimum, from the sparse information in Defendant's Index, access to USCP's policies for demonstration activities, application, interpretation and enforcement (Directive 1012.001), notification and reporting for duty for emergency situations (Directive 2052.006), securing the Capitol Complex during active threats (Directive 1030.001) and utilization of containment and emergency response team (Directive 1057.001) would provide the public with crucial information about how USCP was supposed to prepare for and respond to the demonstration activity that devolved into the "most significant breach of the Capitol in over 200 years." SMF ¶ 18.

Similarly, public access to USCP's directives with respect to its organizational structure (2000.001), incident command (1052.003), and radio communications systems (1050.001), would help inform the public of how these systems were supposed to work, and to better assess the reasons why they failed on January 6. SMF ¶¶ 80–81; *cf. Trump v. Thompson*, 20 F.4th 10, 48 (D.C. Cir. 2021) ("'[F]acilitating a full airing of the events leading to' such political crises

constitutes a 'substantial public interest.'") (quoting *Nixon v. Adm'r of Gen. Servs*., 433 U.S. 425, 453 (1977)). Access to USCP's policies with respect to intelligence gathering and information exchange with other agencies (1033.001), as well as its view of the scope of its jurisdiction (1010.002), and shared authority (1010.001), would help the public better understand why "USCP's intelligence components failed to convey the scope of information they possessed," even though USCP had "received information from a variety of sources about threats of violence" in the lead up to January 6, SMF ¶ 79, and why "whatever plan the Capitol Police had to request reinforcements didn't work," *id.* ¶ 27. And access to USCP's directive with respect to bias-based profiling (1020.001), and its internal policies regarding anti-discrimination and anti-harassment (2053.011), would allow the public to better evaluate allegations that USCP's response to January 6 reflected a "light touch" in comparison to its response to the racial justice demonstrations in 2020. SMF ¶ 32.

The public also has a substantial interest in understanding why many of USCP's officers did not feel well prepared to use force or employ crowd control tactics on January 6, "felt discouraged or hesitant to use force," and felt that "more training was needed," on these topics. *Id.* ¶¶ 99–01. Access to USCP's use of force and training policies, including Directives 1020.004 (Use of Force), 2052.012 (Police Training Officer Program), and 2061.001 (Recruit Officer Entry-Level Training Program), and policies concerning non-lethal crowd control techniques, such as Directives 1020.012 (Use of Long-Range Acoustical Device (LRAD)), 1020.011 (Electrical Control Devices (ECD)) (tasers), would allow the public to better evaluate these issues. Access to USCP's use of force policies would also allow the public to better assess the appropriateness of the use of deadly force against Ms. Babbitt, USCP's subsequent assertion that "the officer's conduct was lawful and within Department policy," and the appropriateness of the $4.975 million

settlement paid by taxpayers as a result of that use of force. SMF ¶¶ 57–63. At the same time, access to USCP's policies with respect to protective equipment, its maintenance, and its procurement, including Directives 1073.001 (Protective Body Armor), 2092.002 (Respiratory Protection Program), 2092.003 (Self-Contained Breathing Apparatus Inspection and Maintenance), 2071.001 (Budget Object Classification Codes), 2074.003 (Purchase Card Program), 2093.002 (Maximo Security Policy), would allow the public to evaluate whether USCP's policies were adequate to provide for sufficient equipment, whether the "gear was old or of poor quality," and whether it was "readily accessible" to officers on January 6. SMF ¶ 102.

The public also has a sizable interest in evaluating questions about alleged "reconnaissance tours" that took place in the days leading up to January 6, SMF ¶¶ 64–73, which access to USCP's policy for providing USCP-led tours (Directive 1000.001) would inform. Moreover, the public lacks any information about USCP's own internal investigations into certain officers following January 6, including the officer indicted for obstruction of justice for allegedly sending a message to a rioter on Facebook instructing him to remove incriminating evidence from social media. SMF ¶¶ 55–56. Accordingly, access to USCP's policies governing the conduct of its officers including Directives 2053.019 (Employee Use of Electronic Social Media), 2081.001 (Acceptable Use of the Internet, Email, and Information Technology Equipment), and 2043.001 (Ethics Policy) would allow the public to better evaluate the appropriateness of officer-conduct on that day. *Cf. Cobell v. Norton*, 157 F. Supp. 2d 82, 89 (D.D.C. 2001) (recognizing the "public has a bona fide interest in having the conduct of government agencies and its officials . . . revealed").

The identification of these interests is not intended to suggest that the public's right of access to the directives turns on whether USCP's policies were adequate or inadequate to anticipate, prepare for, and ultimately respond to the events of January 6. As the D.C. Circuit has

recognized, whether a particular law enforcement "policy is legal or illegal, proper or improper, is irrelevant" in assessing public interest, because either way, the public has an interest in knowing what a law enforcement "policy is and how effective or intrusive it is." *ACLU v. Dep't of Just.*, 655 F.3d 1, 14 (D.C. Cir. 2011). But in light of the substantial public debate concerning the adequacy of USCP's policies and procedures in the lead up to January 6, the public's interest in accessing the directives at issue here is hardly an "abstract" one. *Contra* Def.'s Mem. at 9. Rather, the public has a powerful interest in accessing the directives at issue in this case, which readily outweighs the harms Defendant asserts would flow from disclosure.

B. Defendant fails to articulate any meaningful harm that would flow from disclosure of the directives that do not contain security information.

Because the public's general and specific interests in disclosure here are weighty, "the government must articulate a *specific* threat and may not generally invoke its interests in the security of the U.S. Capitol without articulating how these [records] might undermine particular security interests" to justify withholding these records from public view. *See Torrens*, 560 F. Supp. 3d at 294 (emphasis in original). But far from making such a showing, USCP relies on the "law enforcement sensitive" label, or otherwise on generalized assertions of harm, to justify withholding all 35 remaining directives it concedes do not contain "security information." USCP's showing is insufficient, and the public interest readily outweighs it.

1. *USCP's use of the "Law Enforcement Sensitive" label does not relieve it of its burden to articulate a specific harm flowing from disclosure.*

As an initial matter, USCP's averment that it has designated the directives "Law Enforcement Sensitive" does not meaningfully inform the balancing inquiry required by the common law. As the D.C. Circuit has recognized, "'Law Enforcement Sensitive' is an imprecise term; at least seven different federal agencies define it differently." *Parhat v. Gates*, 532 F.3d 834,

853 (D.C. Cir. 2008). Thus, the government is required to provide "an explanation tailored to the specific information at issue," to justify withholding, rather than rely on "generic claims" of sensitivity. *See id.* (so recognizing in evaluating government's request to bar public disclosure of information in the court record of petition for review of combatant status for person detained at Guantanamo Bay). Defendant's mere invocation of "Law Enforcement Sensitive" does not overcome the public's right of access.

In any event, USCP's bald assertion that the directives at issue here are "Law Enforcement Sensitive" is a dubious one that is not supported by any record evidence. To the contrary, Plaintiff's Response Index identifies examples of federal, state, and local law enforcement agencies that have made analogous directives, manuals, statements of procedures, and other similar policy documents fully public, including ones that cover exactly the same subject matter USCP is seeking to withhold here. SMF ¶¶ 143–302; *see also* Pl.'s Resp. Index at 1–22. The practices of these law enforcement agencies in making their policies and directives publicly available is strong evidence that such documents are generally considered the opposite of "sensitive" by "the law enforcement profession." *Cf. Reps. Comm. for Freedom of the Press*, 489 U.S. at 767 (in interpreting FOIA Exemption 7(C), recognizing that "[s]tate policies, of course, do not determine the meaning of a federal statute, but they provide evidence that the law enforcement profession generally assumes—as has the Department of Justice—that individual subjects have a significant privacy interest in their criminal histories"). Considering the widespread disclosure of similar policies, and that USCP's actual assertions regarding the harms that might flow from disclosure are minimal as set forth below, the "law enforcement sensitive" label holds no water.

2. *Defendant's categorical assertion that some directives reflect "law enforcement techniques" is insufficient to overcome the public interest.*

USCP asserts that 16 directives (which do not contain "security information") may be

withheld in their entirety on the grounds that they contain "nonpublic operational methods and step-by-step procedures used by USCP personnel," and that disclosure would "enable persons to anticipate, evade, manipulate, or interfere with USCP law enforcement activities, compromise the effectiveness of investigations or other operations, or undermine procedures designed to preserve the integrity of enforcement actions and evidence." Def.'s Mem. at 9–10. As set forth in Plaintiff's Response Index, none of these hyperbolic assertions are borne out by the record. To the contrary, comparable policy documents addressing the same subject matter as the directives Defendant labels "law enforcement techniques" have been disclosed, either in full or in part, by other law enforcement agencies throughout the country. *See* Pl.'s Resp. Index at 2–11, 15, 20. Such policies typically provide basic standards for law enforcement when engaging in functions that may infringe on the public's constitutional rights rather than detailed technical procedures, and there is no evidence that these disclosures have resulted in any detriment. *See id.*

To highlight just one example, consider Directive 1060.001 (Cell Phone Recovery), which Defendant puts in the "law enforcement techniques" category. A review of comparable policy documents released by other law enforcement agencies makes clear that it is inconceivable that every word of this directive contains "nonpublic operational information" or "step-by-step procedures" that would enable would-be criminals to "circumvent" it—as Defendant contends. *Contra* Def.'s Mem. at 9. Take the U.S. Immigration and Customs Enforcement ("ICE") Directive for Border Searches of Electronic Devices: it describes the general standard for searching and seizing information from electronic devices at the border, the personnel authorized to perform such searches (and when they may request technical assistance from other agencies), and basic chain of command and data retention procedures. Veile Decl. Ex. 63. Or consider the Baltimore Police Department's Policy for mobile device searches, which requires officers to obtain a warrant to

search a cell phone and otherwise describes the process for submitting such phones to a specialized unit for examination, rather than the nuts-and-bolts of the actual data-recovery process. Veile Decl. Ex. 116. Even if USCP's policy is substantially more detailed than these policies (which there is no evidence of), the pathway to "circumvention" USCP imagines is far from clear. The Fourth Amendment requires law enforcement to obtain a warrant before searching a cell phone, and the Supreme Court has observed that after a cell phone has been seized during an arrest, there is "no longer any risk that the arrestee himself will be able to delete incriminating data from the phone," other than through use of sophisticated techniques that there is "little reason to believe" are "prevalent" or that would not be triggered by the seizure itself regardless of what procedures law enforcement might have in place. *See Riley v. California*, 573 U.S. 373, 388–90 (2014).

Defendant's suggestion that the general policy documents at issue here are analogous to the video recordings at issue in *Dhiab v. Trump*, 852 F.3d 1087 (D.C. Cir. 2017), and therefore may be withheld from the public, falls flat. The recordings in *Dhiab* were classified and depicted military personnel transporting and force-feeding detainees at Guantanamo Bay. *See id.* at 1089–90. None of USCP's policies are classified, none address force-feeding procedures for military combatants,[12] and USCP has submitted no evidence to suggest that disclosure of its basic policies for conducting preliminary investigations, enforcing traffic regulations, and searching persons would enable the development of "countermeasures." *Contra* Def.'s Mem. at 10.

Finally, although Defendant also seeks to rely on caselaw interpreting FOIA's Exemption 7(E) to withhold these 16 documents, Def.'s Mem. at 10, the comparison is inapt twice over. First,

[12] Notably, the U.S. Federal Bureau of Prisons' hunger strike policy is readily available to the public, illustrating that the secrecy interests at stake in *Dhiab* do not map onto domestic law enforcement policy guidance. *See* Fed. Bureau of Prisons, Policy No. P5562.05 (Hunger Strikes) (July 29, 2005), https://www.bop.gov/policy/progstat/5562_005.pdf.

the common law right of access simply operates differently than FOIA: Exemption 7(E) creates a "relatively low bar" for exempting from disclosure information that "might create a risk of circumvention" just the same as information that poses a demonstrable or actual risk of circumvention. *See Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011). By contrast, the common law right of access requires an analysis of "the ***specific*** nature of the governmental and public interests as they relate to the document itself." *WLF I*, 17 F.3d at 1452 (emphasis added). Thus, the balance of interests can still favor disclosure even if there may be some risk, so long as the public interest outweighs that risk. Such is the case here: The public interest in accessing USCP's policies for engaging in activities such as profiling members of the public, conducting searches and seizures, and processing arrestees, is substantial, and the actual risk of harm is exceedingly slight. *See* discussion *supra*, Section I.A; *see also* Pl.'s Resp. Index at 2–11, 15, 20. And second, in any event, Exemption 7(E) does not allow withholding of policy documents that describe "general methods" of policing or "publicly known investigative technique[s]" that "lack any detailed, technical analysis of these investigatory techniques," like the ones at issue here. *ACLU of N. Ca. v. Dep't of Just.*, 880 F.3d 473, 492 (9th Cir. 2018) (quotations omitted); *accord Founding Church of Scientology of Wash. D.C., Inc. v. Nat'l Sec. Agency*, 610 F.2d 824, 832 n.67 (D.C. Cir. 1979) (recognizing FOIA Exemption 7(E) "should not be interpreted to include routine techniques and procedures already well known to the public") (quotation omitted).

3. Defendant's categorical assertion that some directives reflect "administrative practices" is insufficient to overcome the public interest.

USCP has attached its "administrative practices" label to 19 directives, six of which overlap with the "internal personnel practices" label, and seven of which overlap with the "law enforcement techniques" label. USCP asserts that the revelation of the "administrative practices" directives would "reveal internal workflows, assignments of responsibilities, the personnel and

systems responsible for administering sensitive USCP functions, and other administrative practices," Def.'s Mem. at 11. Plaintiff's Response Index responds to each of these in turn. *See* Pl.'s Resp. Index at 1–9, 11–16, 20–22. But USCP's more basic problem is it has not identified harms at all, but rather descriptions of the public's interest in knowing what these directives say. For example, USCP asserts that Directive 1073.001 (Protective Body Armor), would "reveal the nature and use of protective equipment issued to USCP personnel." *See* Def.'s Index (ECF 26-4) at 3. That is exactly why the public has an interest in knowing what it says, so that it may better assess why USCP officers were not equipped with sufficient "helmets, riot gear, and shields," why the "gear was old or of poor quality," and why it was not "readily accessible" on January 6. SMF ¶ 102.

Although USCP claims that disclosure of these 19 directives "could permit outside actors to interfere with USCP's internal processes and could expose particular personnel or systems to exploitation, harassment, or disruption," Def.'s Mem. at 11, Plaintiff's Response Index shows that other agencies function while making similar policies fully available to the public—there is no evidence of "exploitation, harassment, or disruption" among them because of the publication of those policies. *See* Pl.'s Resp. Index at 1–9, 11–16, 20–22 (collecting publicly available policies for directives USCP classifies as "administrative practices"). To illustrate just how unsubstantiated USCP's assertions of harm are, consider Directive 2053.019, which USCP argues "would reveal conduct prohibited for Department employees, which could subject Department employees to extortion or interference if revealed to the public." Def.'s Index at 4. USCP does not explain what kind of "extortion" or "interference" it imagines could befall its employees if the public were entitled to learn such basic information as the "limits on employee use of social media." *See id*. By the same token, with respect to Directive 1020.001 (Bias-Based Profiling),

USCP does not explain how it could possibly be true that "reveal[ing] the methods by which the Department identifies potential bias amongst sworn employees" would "risk circumvention by criminal actors." *Id*. at 2. To the extent that USCP is attempting to argue that disclosure of these directives would risk revealing to the public how its own officers might be circumventing its own policies, that describes a benefit of accountability flowing from disclosure—not a harm.

In this category, as above, Defendant's comparison to FOIA Exemption 7(E) is misplaced because the common law requires balancing the specific disclosure harms against the specific public benefits. *See WLF I*, 17 F.3d at 1452. In any event, the cases USCP cites are distinguishable because neither involved efforts to withhold the entirety of basic law enforcement policies similar to the ones at issue here. *See Shapiro v. Dep't of Just*., 893 F.3d 796, 800–01 (D.C. Cir. 2018) (addressing withholding of records reflecting results of a specific search of a commercial database); *Citizens for Resp. & Ethics in Wash. v. DHS*, 525 F. Supp. 3d 181, 194 (D.D.C. 2021) (addressing redaction of figures and data that would tend to reveal the number of Secret Service personnel on trip to Scotland). Here, USCP is seeking to withhold documents which would inform public debate about its procedures for processing individuals it has arrested (Directives 1021.005 & 1021.006), its budget (2071.001), and the care and maintenance of protective body armor for its officers (1073.001)—all issues about which the public has a profound interest in general and as it relates to USCP's response to the events of January 6—based on nothing more than unsupported innuendo that access to these documents "may impair USCP's mission-critical functions." Def.'s Mem. at 11. These directives should be ordered released.

4. Defendant's categorical assertion that some directives reflect "internal personnel practices" is insufficient to overcome the public interest.

USCP's assertion that fourteen of the directives that remain at issue (excluding Directive 2053.013) may be withheld because they reflect "internal personnel practices" fares no better.

USCP claims that disclosure of such directives would "reveal nonpublic employee responsibilities, reporting processes, supervisory practices, and safety-related requirements," Def.'s Mem. at 12, but again, that does not describe a harm but rather a benefit of the public's right of access under the common law. And the fact that they are "nonpublic" is, of course, the point of this case.

Plaintiff's Response Index addresses each of these directives in turn. To highlight one example, Directive 2000.001 (Organizational and Management Structure of the USCP), Defendant insists that disclosure of this directive would "reveal specific personnel and their roles in the Department, subjecting them to harassment or interference with their duties." Def.'s Index at 3. These assertions are undermined, in the first instance, by the fact that USCP's organizational chart has already been revealed to the public by government oversight bodies in the wake of the January 6 attack, demonstrating both the public interest in that information and that no substantial harm has (or is likely to) flow from disclosure. Veile Decl. Ex. 2 at 16. But more to the point, the idea that personnel within USCP might prefer to avoid any public oversight should not be confused with an actual risk of "harassment" or "interference." *Contra* Def.'s Index at 3. Public accountability is a feature, not a bug, of the public's common law right to access information about the functioning of their government. *See Metlife*, 865 F.3d at 663 ("The right of public access is a fundamental element of the rule of law, important to maintaining the integrity and legitimacy"). Any other rule would eviscerate the right of common law access.

A review of Defendant's other assertions of harm demonstrate that they are, likewise, without substance. For example, Defendant asserts, presumably in reference to Directive 1000.001 (USCP Personnel-Led Tours of the Capitol) that "disclosure of Capitol-tour procedures could provide hostile actors information useful to harming tour participants or damaging the Capitol." Def.'s Mem. at 13. But it is unclear how USCP's written tour policy, by describing "the conditions

by which USCP personnel may lead tours," Def.'s Index at 2, could possibly reveal any information about Capitol tours that the "millions of individuals who visit the Capitol Complex annually" would not already know. *See* SMF ¶ 2. Defendant also expresses concern that disclosure of its policies might allow adversaries to "identify and exploit staffing trends during periods of anomalous conditions," Def.'s Mem. at 13, presumably in reference to Directive 2052.006 (Notification and Reporting for Duty During Emergency Situations). Defendant again cites FOIA Exemption 7(E) cases on this point, *see id*. at 13, but as explained above, the common law balancing test can favor disclosure even where Exemption 7(E) could conceivably apply. And, in any event, the cases Defendant cites are distinguishable in that they involved the appropriateness of redactions of information reflecting specific Secret Service detail information rather than wholesale withholding of general policy documents. *See Citizens for Resp. & Ethics in Wash. v. DHS*, 525 F. Supp. 3d at 186–87 (describing redactions); *N.Y. Times Co. v. U.S. Secret Serv.*, 17 Civ. 1885 (PAC), 2018 WL 722420, at *1–4 (S.D.N.Y. Feb. 5, 2018) (describing redactions). Moreover, USCP is not analogous to the Secret Service—USCP operates as a "traditional police department[]," with its uniformed officers "seen around the Capitol Complex" every day. Veile Decl. Ex. 2 at 16. In short, USCP's assertions of harm are insufficient to overcome the public's substantial interest in disclosure of these directives.

C. Defendant has failed to justify withholding the entirety of the directives it avers contain "security information."

USCP's effort to withhold the entirety of the directives it maintains contain "security information" under 2 U.S.C. § 1979 defies basic principles of statutory interpretation and common sense. At the motion to dismiss stage, this Court observed that the record lacked development as to "whether or why USCP asserts that the entirety of the 64 remaining security-information-designated directives constitute security information." *Leopold III*, 823 F. Supp. 3d at 87. Rather

than submit any meaningful evidence about what information it has deemed "security information" and why, USCP now simply reasserts its position it has "designated" the entirety of the directives as "security information," and argues that should be the end of the matter. *See* Def.'s Mem. at 14. True, in *Leopold I* this Court found that the directives in this category were "'proper[ly]' so designated." *Leopold III*, 823 F. Supp. 3d at 87 (modification in original). But that finding was made without the benefit of "a *Vaughn* index" to inform this Court's analysis. *Leopold II*, 102 F.4th at 500. Defendant's Index now does nothing to close the evidentiary gap—and Plaintiff's Response Index rebuts Defendant's designations with respect to each directive either in whole or in part and with reference to Section 1979's specific requirements.[13] Because Defendant fails to articulate any concrete harms that would flow from disclosure of these directives or the segregable portions thereof, this Court should order their release, with only narrow redactions for information that meets the statute's straightforward criteria for "security information."

1. *Section 1979 establishes at least three criteria for information to qualify as "security information," which USCP has not demonstrated are met for each of the directives it seeks to withhold.*

USCP's organizing statute grants the Capitol Police Board authority to "promulgate regulations to carry out" the release of "security information." 2 U.S.C. § 1979(c). The statute proceeds to define "security information" as information that:

[13] Because Defendant has offered little information of substance about the contents of the directives, Plaintiff is forced to guess at some of their contents. Plaintiff does not dispute, for example, that USCP's directives relating to critical incident response—such as Directives 1052.004, 1052.005, 1054.001, 1056.001, 1056.002, 1056.003—could, conceivably, contain detailed information about USCP's specific plans for responding to threats that could logically fall within Section 1979's ambit. However, these policies could also contain substantial non-sensitive information such as information about hiring, training, and maintaining personnel on USCP's teams, ensuring periodic review in developing its plans, and administrative matters like hazard pay for employees involved in such responses—all matters about which the public would have a substantial interest, and it is unclear why disclosure would result in any harm. At a minimum, USCP has failed to engage in the "line-by-line" review the common law requires with respect to these directives. *Cf. In re L.A. Times Commc'ns LLC*, 628 F. Supp. 3d 55, 62 (D.D.C. 2022).

> (1) is sensitive with respect to the policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response relating to Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds; and
>
> (2) is obtained by, on behalf of, or concerning the Capitol Police Board, the Capitol Police, or any incident command relating to emergency response.

Id. § 1979(a). Section 1979 does not give USCP or its Board the authority to preclude the release of entire documents merely by asserting that they "constitute security information," nor does it authorize them to redefine the statute to allow withholding of information that is not "security information." *Contra* Def.'s Mem. at 15–16. Rather, this provision "must be interpreted and applied by the Court." *Leopold III*, 823 F. Supp. 3d at 87. "In determining the meaning of a statutory provision, [courts] start with the text of the statute," *Teva Pharms. USA, Inc. v. Kennedy*, 187 F.4th 587, 603 (D.C. Cir. 2026) (quotation omitted), while giving "effect, if possible, to every clause and word of a statute," *id*. (quotation omitted). Here, Section 1979 contains at least three criteria that information must meet to be considered "security information": (1) it must be "sensitive," (2) it must relate to the performance of functions of "policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response," *and* (3) it must relate to the performance of those functions with respect to "Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds." 2 U.S.C. § 1979(a)(1).[14]

These criteria should be narrowly construed. Statutes that "invade the common law . . . are to be read with a presumption favoring the retention of long-established and familiar principles, except when a statutory purpose to the contrary is evident." *Metlife*, 865 F.3d at 674 (omission in original) (quoting *United States v. Texas*, 507 U.S. 529, 534 (1993)). No such purpose is evident

[14] The information must also be "obtained by, on behalf of, or concerning the Capitol Police Board, the Capitol Police, or any incident command relating to emergency response," *id.* § 1979(a)(2); Plaintiff does not dispute that the directives here concern the Capitol Police.

here—the "security information" language was added to USCP's organic statute as part of an appropriations enactment which garnered no committee reports or substantial debate, as would be expected if Congress had intended to drastically alter the scope of the public's common law rights. *See* Pub. L. No. 108-447, 118 Stat. 2809 (2004) (enacting provision); *see also* 150 Cong. Rec. E2205-03, 2004 WL 2935758 (Nov. 20, 2004) (statement of Rep. John B. Larson) (expressing concern that "several legislative provisions within the jurisdiction of the House Administration Committee found their way into this appropriations bill," including Capitol Police Board's requests); H.R. Rep. No. 108-577, at 13 (2004) (noting without comment that "Section 1002 restricts the release of security information").

Start with the first criterion—that the information must be "sensitive." 2 U.S.C. § 1979. Although the statute does not define "sensitive," as noted above, the practices of comparable federal and state law enforcement agencies in making their policies and directives publicly available are instructive in determining what information is generally considered non-sensitive by "the law enforcement profession." *Cf. Reps. Comm. for Freedom of the Press*, 489 U.S. at 767 (recognizing, in interpreting FOIA Exemption 7(C), that "[s]tate policies, of course, do not determine the meaning of a federal statute, but they provide evidence that the law enforcement profession generally assumes—as has the Department of Justice—that individual subjects have a significant privacy interest in their criminal histories").

In the attached Response Index, Plaintiff highlights policies addressing similar topics to the ones Defendant's assert contain "security information" that have been made public by other such agencies. *See* Pl.'s Resp. Index at 23–69. Such publications show these law enforcement entities do not consider policy documents on organizational jurisdiction and authority, demonstration activities on public property, use of force, executing arrest and search warrants, and

responding to vehicular incidents or conducting vehicular pursuits "sensitive" at all, much less so "sensitive" that the public cannot see even a word of them. *See*, *e.g.*, SMF ¶¶ 143–302 (collecting publicly available policies of, among others, USPP, DHS, HSI, TSA, MPD, NYPD, APD, the LAPD, the Maryland Capitol Police, and the California Highway Patrol (which houses a division for the California State Capitol), and the Georgia Department of Public Safety (which houses a division for the Georgia State Capitol)).

USCP itself has previously released some of the directives that it has designated "security information," including a version of Directive 1053.002 (Vehicular Pursuits). A review of this directive makes clear that USCP's policy does not contain substantially unique or detailed information to render them more "sensitive" than the policies other law enforcement agencies routinely release—nor has Defendant established that to be the case. USCP's policy, like MPD's and the USPP's policies, limits the circumstances in which USCP officers may engage in pursuits and use certain techniques, such as roadblocks, and sets forth the administrative procedures for notifying dispatch of the pursuit. *Compare, e.g.*, ECF No. 1-4 at 1, 6–8 (providing USCP may use pursuits "to affect the arrest or prevent the escape of a person who has committed a violent felony" and similar situations, prohibiting "use of rolling roadblocks . . . unless specifically authorized by a supervisor and conducted by personnel trained in this technique," and describing dispatcher procedures) *with* Veile Decl. Ex. 80 at 1, 3–6 (limiting MPD pursuits to situations where "[t]he fleeing suspect has committed or attempted to commit a crime of violence" and similar situations, prohibiting roadblocks except in "cases involving imminent threat of death or serious bodily injury," and describing dispatcher procedures) *and* Veile Decl. Ex. 43 at 3–4, 8, 11–12 (similar for USPP). And although USCP asserts the vehicular pursuits policy attached to Plaintiff's complaint was "not in effect on January 6, 2021," Def.'s SMF ¶ 5, it makes no effort to explain which

information therein it considered "sensitive" why such information was previously publicly filed in litigation with no redactions,[15] or why that previous disclosure did not render the same information non-sensitive.

Notably, the Transportation Security Administration ("TSA") makes its management directives available to the public despite the fact that it is governed by a statute which provides for the "[n]ondisclosure of security activities." 49 U.S.C. § 114(r). TSA's implementing regulations define qualifying information as "sensitive security information," 49 C.F.R. § 1520.5(a), and delineate the categories of information that it generally considers to be sensitive, including "[s]ecurity programs, security plans, and contingency plans," *id.* § 1520.5(b)(1), "Security Directives," *id.* § 1520.5(b)(2),[16] and "security measures," *id.* § 1520.5(b)(8). Nonetheless, TSA does not construe either its statute or its implementing regulations as requiring it to withhold every word of its general policy documents. To the contrary, TSA makes many of its management directives available to the public in full on its FOIA reading room. *See, e.g.*, SMF ¶¶ 162–70. This includes several that address the same topics as USCP directives that USCP has marked "security information." *Compare, e.g.*, Def.'s Index at 7, 9 (describing USCP Directives 1020.004 (Use of Force), 2022.001 (Privacy Policy for Safeguarding Sensitive Personally Identifiable Information and Sensitive Health Information), and 1040.002 (Security Screening)) *with* Veile Decl. Exs. 61, 62, & 57 (TSA Directives 3500.2 (Use of Force and Firearms), 3700.4 (Handling Sensitive Personally Identifiable Information), 100.4 (Transportation Security Searches)). Of course, the

[15] The version of Directive 1053.002 attached to Plaintiff's Complaint was filed publicly in *Anyaso v. Capitol Police*, No. 1:12-cv-01327 (ESH) (D.D.C. Dec. 16, 2013), ECF 17-5 at 16–22.

[16] TSA Security Directives, unlike USCP Directives, are not internal policy documents issued to TSA employees; they are issued to airports, aircraft operators, or indirect carriers to "respond to a threat assessment or to a specific threat against civil aviation," by "setting forth mandatory measures" in response to particular security concerns. 49 C.F.R. §§ 1542.303, 1544.305, 1548.19.

practices of other agencies are not determinative of the meaning of Section 1979, but they are certainly illustrative of how an agency with law enforcement functions might administer a statute like Section 1979 while still balancing the public's right to know.

The second criterion of Section 1979 is that the information must relate to the performance of functions of "policing, protection, physical security, intelligence, counterterrorism actions, or emergency preparedness and response." 2 U.S.C. § 1979(a)(1). This is particularly relevant here because many of the policies USCP avers contain "security information" instead contain generic information technology policies covering such topics as handling sensitive or personally identifiable information, password policies, responding to computer security incidents, and managing USCP's internet and intranet sites.[17] Such policies could be maintained by any governmental agency and have no relationship to the performance of police, security, or emergency preparedness functions. The mere fact that USCP is a law enforcement agency cannot be enough to make its policies regarding activities so far removed from the performance of police functions sensitive with respect to the performance of such functions.

The third and final criterion is that the information must relate to the performance of the specified functions with respect to "Congress, any statutory protectee of the Capitol Police, and the Capitol buildings and grounds." 2 U.S.C. § 1979(a)(1). This criterion is relevant because USCP has categorized numerous directives as "security information," where the policies address the performance of generic law enforcement functions such as use of force, use of restraints, executing arrest warrants, and intercepting wire or oral communications.[18] Such policies are

---

[17] *E.g.*, Directives 2011.002, 2022.001, 2080.003, 2081.003, 2081.005, 2081.006, 2081.007, 2081.008, 2081.010, 2081.011, 2081.012, 2081.013, 2082.001, 2083.001, 2083.002, 2083.003, 2083.004, 2093.002, and 2081.004.

[18] That includes, for example, Directives 1020.003, 1020.004, 1022.005, 1020.011, 1021.004, 1032.002, 2093.001, 2092.002, 2092.003, 1050.001, and 1052.003.

maintained by police departments throughout the country; it is not clear why these directives would contain much, if any, information that is specific or unique to providing policing or security services to the Capitol or members of Congress, as required by the statute. Again, the mere fact that USCP's mission is somewhat unique does not mean that its generic law enforcement policies are any more sensitive than those of the numerous police departments throughout the country who make such policies fully public.

2. *Even if any of the directives contain "security information," Defendant has a ministerial duty to release all reasonably segregable information from those directives.*

As set forth above and in the attached Response Index, there is substantial reason to doubt that many of the directives at issue contain any "security information" at all. Even assuming, *arguendo*, that some or all of the directives ***did*** contain "security information," Defendant has still failed to provide any evidence explaining how it is possible "the entirety of the 64 remaining security-information-designated directives constitute security information." *See Leopold III*, 823 F. Supp. 3d at 87. Instead, USCP relies on broad and generalized assertions that it has "designated" the entirety of the directives as "security information." *See* Def.'s Mem. at 14. To be clear, the only evidence USCP has ever submitted to support its designations was a declaration in *Leopold I* that asserted a "USCP Document Review Team" had determined that the directives contained "security information." Joyce Decl. ¶ 9 (submitted in *Leopold I*, No. 1:21-cv-00465 (BAH), ECF No. 19-5). In *Leopold I*, USCP submitted no evidence regarding its assertion that these directives contained "security information" with any reference to the statute, nor did it attempt to differentiate the information contained in those directives from the information contained in the directives it conceded did not contain "security information." Instead, USCP flatly contended that "[n]one of the requested USCP directives, regardless of whether they are security information under 2 U.S.C.

§ 1979, constitute 'public records'" because, in USCP's view, they were "Law Enforcement Sensitive." Joyce Decl. ¶ 11. In this litigation, USCP's assertions are even more opaque—its declarant merely asserts that the directives "were determined to contain 'security information.'" Wilensky Decl. ¶ 5, ECF No. 26-53. That does not suffice.

Although Defendant attempts to relitigate the issue, *see* Def.'s Mem. at 16, this Court has already explained that "defendant lacks discretion as to whether to release information sought by plaintiff that is not 'security information,' if the court so orders after application of the *WLF I* test. Thus, the duty to redact appears to be ministerial, and mandamus may lie to compel it." *Leopold III*, 823 F. Supp. 3d at 89. That straightforward conclusion flowed from ample precedent confirming that "the common law duty to release judicial records exists even when the preliminary step of redaction must be taken to protect information for which good reason requires nondisclosure." *See id*. at 88 (collecting cases); *see also In re Leopold to Unseal Certain Elec. Surveillance Applications & Ords*., 964 F.3d 1121, 1133–34 (D.C. Cir. 2020) (recognizing although "the government and court must be able to redact documents in order to protect privacy and law enforcement interests," the "administrative burden" of production is not dispositive of duty to provide public access); *In re Appl. of United States for 2703(d) Order*, 548 F. Supp. 3d 31, 33 (D.D.C. 2021) ("Let there be no mistake: the government has a duty to 'mak[e] public appropriately redacted documents' after an investigation is closed." (citation omitted) (alteration in original)); *see also* Pl.'s Opp. to Def.'s Mot. Dismiss (ECF No. 12) at 21–22 (collecting cases from other circuits confirming duty to redact). In short, Defendant is incorrect that "partial disclosure remains a 'release' of security information governed by § 1979(b)." *Contra* Def.'s Mem. at 16. At the risk of stating the obvious, the release of information that is not "security information" is not a partial disclosure of "security information."

USCP's bare assertion that "no non-security information can be reasonably segregated and released without directly or indirectly disclosing security information," Wilensky Decl. ¶ 16, is conclusory and cannot be squared with the statute's narrow terms, as set forth *supra*, or common sense. These assertions are "conclusory" and "offered without any factual basis in the record," and therefore are not required to be credited, *cf. Serv. Emps. Int'l Union Nat'l Indus. Pension Fund v. Jersey City Healthcare Providers, LLC*, 358 F. Supp. 3d 12, 18 (D.D.C. 2019) (citation omitted). In any event, such assertions are fatally undermined by the fact that USCP's own OIG has made substantial information from its own reports public with redactions. *See, e.g.*, SMF ¶¶ 132–39; Veile Decl. Exs. 34–40. Although the scope of the redactions OIG has applied to these reports is not the issue before this Court, and although some of those redactions appear overbroad on their face in light of the "security information" framework described above, Plaintiff highlights that OIG Rep. 2021-I-0003-D discusses several of USCP's bureaus and divisions. Veile Decl. Ex. 38 at 2–4. In that report's discussion of USCP's Containment and Emergency Response Team (CERT), the report quotes verbatim from a portion of one of USCP's directives dated May 28, 2012 (while inexplicably redacting the name of the directive itself), as stating "the Department provides ready response for situations requiring special weapons and tactics by maintaining CERT." *See id.* at 2–3. Meanwhile, it has redacted certain information derived from a more specific document—a January 6 CERT Daily Manpower Report—about the number of employees and officers scheduled that day. *Id.* at 3. Plaintiff highlights this example to underscore that even under USCP's exceptionally broad understanding of the term "security information," general policy information contained in USCP's directives outlining the scope of its basic authorities and functions is distinguishable, and readily segregable from, the type of information that may be contained in more detailed and situation-specific records (like CERT Daily Manpower Reports)

that USCP might otherwise maintain. *Id.* at 2–3. In short, OIG's release of redacted reports makes clear that targeted redactions, rather than wholesale withholding, is entirely possible.

Defendant's brief makes reference to several cases interpreting FOIA's Exemption 3, 5 U.S.C. § 552(b)(3), which applies to records "specifically exempted by statute." Def.'s Mem. at 16–17. But that invocation does not help USCP; even in the Exemption 3 context, "a reviewing court must still assure itself that the material withheld is actually exempted by the claimed statute . . . and that the exempt material cannot be segregated from non-exempt material appearing in the same records." *Elec. Priv. Info. Ctr. v. Dep't of Just.*, 511 F. Supp. 2d 56, 66 (D.D.C. 2007) (citation omitted). As illustrated by *CIA v. Sims*, 471 U.S. 159 (1985), which Defendant cites, wholesale withholding is not the norm under Exemption 3. In *Sims*, the agency disclosed "all of the MKULTRA grant proposals and contracts" that the requestor had sought but withheld "the names of all individual researchers and 21 institutions" on the grounds those names would reveal "intelligence sources and methods." *Id.* at 163–64 (citation omitted). Here, USCP is not simply seeking to withhold names of intelligence sources or methods, it is seeking to withhold every word of its basic policy documents. And although Defendant collects a handful of Exemption 3 cases authorizing wholesale withholdings, those cases involved altogether different kinds of records and different kinds of withholding statutes than this case. *See Ass'n of Retired R.R. Workers v. U.S. R.R. Ret. Bd.*, 830 F.2d 331, 331 (D.C. Cir. 1987) (addressing request for "the names and addresses of retired workers" where identifying information was exempted by statute); *Stein v. Sec. & Exch. Comm'n*, 266 F. Supp. 3d 326, 350 (D.D.C. 2017) (addressing request for suspicious activity report where relevant statute exempted "reports"); *Rivera-Rodriguez v. Dep't of Just., Exec. Off. of U.S. Att'y*, No. 1:19-cv-02510 (APM), 2022 WL 136793, at *1 (D.D.C. Jan. 14, 2022) (addressing request for grand jury materials exempt under Fed. R. Crim. P. 6(e)); *Jud. Watch, Inc. v. Nat'l*

Archives & Recs. Admin., 214 F. Supp. 3d 43, 65 (D.D.C. 2016) (similar).

Plaintiff seeks access to basic documents reflecting USCP's basic policies, which would reveal a great deal about USCP's fulfillment of its mission generally and with respect to the extraordinary events of January 6 in particular. It may be true that courts sometimes permit the withholding of "superficially innocuous" information, *Sims*, 471 U.S. at 178, but that does not salvage USCP's argument here, where it has submitted nothing to demonstrate that its directives contain anything more than "seemingly benign text," Def.'s Mem. at 19. In short, USCP has submitted utterly no evidence explaining why it "asserts that the entirety of the 64 remaining security-information-designated directives constitute security information." *Leopold III*, 823 F. Supp. 3d at 87. Defendant has also not attempted to assert any harm that would flow from disclosure as to the directives it maintains contain security information. Accordingly, the *WLF I* balancing test clearly and indisputably favors disclosure.

II. The other mandamus factors favor issuance of the writ to enforce the public's common law right to access these directives.

For the reasons set forth above, the two-step *WLF I* test is clearly and indisputably satisfied with respect to the directives at issue here, and Defendant therefore has a "nondiscretionary duty to make . . . records available to the public." *Leopold III*, 823 F. Supp. 3d at 84 (quotations omitted) (omission in original). Although Defendant does not raise them, the remaining mandamus factors are also readily satisfied here such that mandamus relief should issue. In light of Defendant's representation that the version of Directive 2053.013 that Plaintiff possesses was in effect on January 6, Plaintiff agrees no further relief is necessary. As for the remaining 99 directives, "there are no other adequate means to attain the relief sought." *Leopold III*, 823 F. Supp. 3d at 78–79 (citation and quotation omitted). No statutory disclosure regime applies to the records Plaintiff seeks. *See* Def.'s Mem. at 5 (agreeing USCP is "not subject to FOIA"). The parties appear to

agree, then, that Congress has not "spoken directly to the issue at hand." *Ctr. for Nat'l Sec. Studies v. Dep't of Just.*, 331 F.3d 918, 937 (D.C. Cir. 2003). The common law provides the only adequate means for Plaintiff to obtain relief.

For much the same reasons that the common law balancing test conclusively favors disclosure here, issuance of mandamus relief is also "appropriate under the circumstances" of this case. *Leopold III*, 823 F. Supp. 3d at 78–79 (citation and quotation omitted). The public has a powerful interest in disclosure, and USCP has utterly failed to demonstrate that the "specific interests favoring secrecy outweigh the general and specific interests favoring disclosure." *WLF I*, 17 F.3d at 1451–52 (citation and quotation omitted). USCP has refused to comply with its obligation to produce these records under the common law for over five years. Because Defendant, in his official capacity as Chief of USCP, is "simply defying" the common law right of access "without any legal basis," mandamus is appropriate to make clear that Defendant must comply with his obligations under the common law, and that USCP is not immune to public oversight over its functions. *See In re Aiken Cnty.*, 725 F.3d 255, 266–67 (D.C. Cir. 2013) (issuing mandamus where agency had been "disregard[ing] federal law" for two years).

CONCLUSION

Plaintiff respectfully requests that the Court deny Defendant's motion for summary judgment as to the 99 directives that remain at issue, grant Plaintiff's cross-motion for summary judgment, and enter an order requiring Defendant to produce to Plaintiff those 99 directives, with only narrow redactions for information (if any) that the Court determines properly consist of "security information," as that term is defined by 2 U.S.C. § 1979.

Dated: November 9, 2026

Respectfully Submitted,

/s/ Allyson Veile
Allyson Veile
D.C. Bar No. 1766038

Adam A. Marshall
D.C. Bar No. 1029423
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1020
Washington, DC 20005
Phone: 202.800.3534
Facsimile: 202.795.9310
Email: aveile@rcfp.org
Email: amarshall@rcfp.org

Counsel for Plaintiff