IN THE COMMONWEALTH COURT OF PENNSYLVANIA

David Osborne and Commonwealth Foundation, Petitioners	:	
v.	:	No. 1580 C.D. 2025
	:	Argued: October 13, 2026
Pennsylvania Office of the Governor (Office of Open Records), Respondent	:	

BEFORE: HONORABLE ANNE E. COVEY, Judge
HONORABLE STACY WALLACE, Judge
HONORABLE MARY HANNAH LEAVITT, Senior Judge

OPINION NOT REPORTED

MEMORANDUM OPINION
BY JUDGE WALLACE FILED: November 4, 2026

David Osborne and Commonwealth Foundation (Requesters) petition for review from the November 3, 2025 final determination of the Office of Open Records (OOR), denying Requesters' appeal from the Pennsylvania Office of the Governor's (Office) refusal to produce records they requested under the Right-to-Know Law (RTKL).[1] Upon review, we reverse, and direct the Office to disclose copies of the records consistent with this memorandum opinion.

[1] Act of February 14, 2008, P.L. 6, 65 P.S. §§ 67.101-67.3104.

BACKGROUND

In connection with the April 13, 2025 security breach and arson attack at the Harrisburg residence of Governor Joshua Shapiro, the Pennsylvania State Police (PSP) and the Office retained Jeffrey B. Miller, a former PSP commissioner (Consultant), to conduct an independent security review of the incident. Following his review, the Consultant authored a report (Report) that has not been made publicly available.

On May 22, 2025, Requesters submitted a request for records to the Office, seeking the Report and "all communications between [the Office] (including Governor Shapiro and/or his cabinet members . . .) and [the Consultant] concerning the [Report] . . . from April 1, 2025, to present." Reproduced Record (R.R.) at 9a. After receiving an extension of time to respond, the Office denied the request citing Section 708(b)(1)(ii), (2), (3)(iii), and (16)(vi)(A) of the RTKL, 65 P.S. § 67.708(b)(1)(ii), (2), (3)(iii), and (16)(vi)(A).[2] *Id.* at 4a.

---

[2] Section 708 of the RTKL provides in pertinent part:

> **(b) Exceptions.--**Except as provided in subsections (c) and (d), the following are exempt from access by a requester under this act:
>
> > (1) A record, the disclosure of which . . . (ii) would be reasonably likely to result in a substantial and demonstrable risk of physical harm to or the personal security of an individual.
> >
> > (2) A record maintained by an agency in connection with the military, homeland security, national defense, law enforcement or other public safety activity that, if disclosed, would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity . . . .
> >
> > (3) A record, the disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system, which may include . . . (iii) building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including public utility systems, structural elements, technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage and gas systems.

(Footnote continued on next page…)

On July 1, 2025, Requesters appealed to the OOR, which invited the parties to supplement the record and file position statements, and directed the Office to notify third parties of their ability to participate in the appeal process. The Office filed an affirmation by Marc Eisenstein (Eisenstein), its Open Records Officer, containing an exemption log (Log) and a separate affirmation by PSP's Deputy Commissioner of Operations, Lieutenant Colonel George L. Bivens (Lt. Col. Bivens). *Id.* at 19a-27a. Eisenstein stated the Office withheld 76 pages of documents. *Id.* at 20a. Eisenstein explained:

> 7) The withheld materials, if disclosed, are reasonably likely to result in a substantial and demonstrable risk of physical harm to or the personal security of an individual.
>
> 8) The Office withheld records maintained by an agency in connection with the military, homeland security, national defense, law enforcement or other public safety activity that if disclosed would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity, as noted in [the Log] and as further affirmed [by Lt. Col. Bivens].
>
> 9) Specifically, the withheld materials detail the security risks and exposures of the Governor's residence and detail plans and options to further develop security at the Governor's residence.
>
> 10) The withheld materials were used by the Office and agency officials to discuss and determine policies, practices and courses of action regarding implementation of security protocols, policies and physical

---

> . . . .
>
> (16) A record of an agency relating to or resulting in a criminal investigation, including:
>
> . . . .
>
> (vi) A record that, if disclosed, would do any of the following:
>
> (A) Reveal the institution, progress or result of a criminal investigation, except the filing of criminal charges.

65 P.S. § 67.708(b)(1)(ii), (2), (3)(iii), and (16)(vi)(A).

> improvements at the Governor's residence. Such materials were provided by a security consultant hired by the Commonwealth and were transmitted to the Office and executive agencies, but were not further disclosed beyond such agencies, and are therefore exempt as "records used in predecisional deliberations." 65 P.S. § 67.708(b)(10).[3]
>
> 11) With respect to materials identified as exempt records of a criminal investigation, the withheld records reveal the institution, progress or result of an investigation undertaken by the agency within its scope of authority, as indicated in [the Log]. The Office has also withheld records of criminal investigations in which criminal justice agencies provided details regarding suspects or victims of crimes. 65 P.S. § 67.708(b)(16).
>
> 12) The Office has withheld records that reveal building and technological system access information and processes. Such information, if disclosed would jeopardize physical security by revealing the location of sensitive infrastructure. In particular, the office has withheld location that public safety officials have confirmed would, if disclosed, threaten public safety and public protection activity. 65 P.S. § 67.708(b)(2), (b)(3).

Id. at 20a-21a. In addition to the Report, the Log also identified an e-mail (E-mail) sent by the Consultant to Dana Fritz, Governor Shapiro's Chief of Staff. *Id.* at 23a, 28a.

In his affirmation in support of the Office's position that the Report should not be considered a public record, Lt. Col. Bivens stated:

---

[3] It exempts, in relevant part, a record that reflects:

> [t]he internal, predecisional deliberations of an agency, its members, employees or officials or predecisional deliberations between agency members, employees or officials and members, employees or officials of another agency, including predecisional deliberations relating to a budget recommendation, legislative proposal, legislative amendment, contemplated or proposed policy or course of action or any research, memos or other documents used in the predecisional deliberations.

65 P.S. § 708(b)(10)(i)(A).

> 6. Th[e R]eport details both security risks and exposures of the Governor's residence infrastructure, systems and organization, and recommendations that detail how those risks and exposures can best be mitigated in the future.
>
> 7. Release of the records would permit individuals with malintent to determine how best to infiltrate both present and current security mechanisms in place at the Governor's residence.
>
> 8. Release of the responsive records thus jeopardizes the security of both the infrastructure of the Governor's residence, and risks the physical safety of the Governor, his family and friends, and staff who may be present at the Governor's [r]esidence.
>
> 9. Release of the records would provide building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including public utility systems, structural elements, technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage and gas systems.
>
> 10. The incident leading to the security assessment is subject to an on-going criminal investigation and any records related to the incident should not be released.

Id. at 25a-26a.

Requesters filed a position statement, seeking *in camera* "inspection of the records withheld to determine whether the records identified as responsive can be redacted and provided in limited form without any safety or security risk to the Governor or any other state official." *Id.* at 29a. Requesters argued the funding needed to "prevent any future breaches" of the Governor's residence was a matter of public importance that, to the extent possible, should be fully disclosed, and the Office should not be permitted to hide behind broad invocations of public security exemptions to avoid disclosure. *Id.* Additionally, Requesters argued records of past security breaches should not be summarily exempt if the vulnerabilities involved are

unlikely to recur or have already been addressed. *Id.* Requesters further argued information about the basic facts of, or the systems involved in, the breach, or the costs and objectives of security improvements would not necessarily reveal current security vulnerabilities at the Governor's residence. *Id.* According to Requesters, "[t]his is especially true if the breach was due to individual oversight or error that has been since addressed with a change in personnel." *Id.*

Requesters disagreed with the Office's position that the Report was part of a criminal investigation, pointing out it was commissioned as an independent security review to determine what had happened and how a similar breach of the Governor's residence could be prevented in the future. *Id.* Finally, citing *Chester Water Authority v. Pennsylvania Department of Community and Economic Development*, 249 A.3d 1106 (Pa. 2021), Requesters challenged the Office's invocation of the deliberative process exemption. R.R. at 29a. In *Chester Water Authority*, the Supreme Court held "Section 708(b)(10)(i)(A) does not serve to insulate communications exchanged between a Commonwealth agency and a private consultant from the [RTKL's] general requirement for openness." 249 A.3d at 1114.

The OOR obtained the parties' consent for an extension to file a final determination. On July 30, 2025, the OOR ordered the Office to produce unredacted copies of the records for *in camera* inspection. That same day, the Office responded to the OOR's order, stating that, although it did not object to providing the E-mail, it objected to providing the Report for *in camera* review because of its sensitive nature. The Office argued the Report would reveal "information regarding security mechanisms, protocols, infrastructure and processes that protect the Governor and his family." R.R. at 34a. The Office, therefore, declined to comply with the OOR's order, arguing *in camera* review would not add anything to the analysis. *Id.*

Requesters replied to the Office's refusal to comply with the OOR's order, urging the OOR to file a petition for enforcement of its order in this Court. *Id.* at 35a.

On August 1, 2025, the OOR issued a letter to the Office asking it to provide an attestation or sworn statement addressing the following:

> 1. Generally, describe the contents of the withheld [E-]mail —i.e. is it a transmission [E-]mail or does it address the contents of the [R]eport— and how disclosure of the [E-]mail creates a reasonable likelihood of endangerment to safety or security. Address whether redaction of the [E-]mail is [] possible and if it's not possible, generally address why.
>
> 2. Address whether there [are] any portions of the [R]eport that do not detail security risks and exposures, recommendations to mitigate those risks, or building/infrastructure plans?

Id. at 36a.

On August 18, 2025, Requesters sent a letter to the OOR, maintaining that it "insist on an *in camera* inspection of all responsive records[,]" and if the Office refuses, it should seek enforcement in this Court. *Id.* at 38a. Requesters once again stated that, even though they recognized the Office's duty "to withhold sensitive operational details related to" the Governor's security, that duty "should not be used as a blanket excuse to block transparency." *Id.* at 37a.

On August 21, 2025, the Office responded to the OOR's August 1 letter, explaining "the [E-]mail discusses the process that was used to develop the [R]eport and recommendations, and further discusses how security experts disseminated observations and recommendations to officials and those who would draw upon the [R]eport's conclusions." *Id.* at 39a. The Office further explained "[t]hese methods of developing the [R]eport and recommendations, and updating security officials on its findings, if made public, would allow bad actors to recognize and anticipate such methods, and exploit that knowledge to harm public facilities and those individuals

who inhabit or make use of those facilities." *Id.* Nonetheless, the Office conceded that, although "technically redactable, very little of the unredacted [E-]mail would contain relevant responsive information." *Id.* With respect to the Report, the Office maintained the Report did "not contain any portions that do anything other than detail and assess security risks and exposures, provide recommendations to mitigate those risks, *provide instructions for how to use the [R]eport to impellent* [sic] *recommendations*, or otherwise review, assess or recommend physical building or infrastructure plans or security plans or protocols." *Id.* (emphasis added). The Office continued to insist "[a]ll of this information, if made public, would allow individuals with malintent to use that information to overcome the security protocols that the [R]eport comments upon or recommends. Nothing within the [R]eport is severable from the sensitive security information that i[t] contains." *Id.* at 40a. The Office submitted a supplemental affirmation from Eisenstein to support its August 21 response. *Id.* at 41a-42a.

On November 23, 2025, the OOR denied Requesters' appeal, concluding the disclosure of the withheld records is reasonably likely to jeopardize or threaten personal security and public safety.[4] *Id.* at 51a. In so doing, the OOR relied on the affirmations submitted by the Office. *Id.* Requesters petitioned this Court for review.

DISCUSSION

On appeal, Requesters raise three issues for our review.

> [I.] Whether the OOR committed an error of law or abused its discretion by allowing the [Office] to refuse compliance with the OOR's lawful

[4] Because the OOR denied Requesters' appeal based on security exemptions, it did not address the Office's alternative grounds for denial under Section 708(b)(10) and (16).

> order for an *in camera* inspection, then by deciding the appeal without such inspection.
>
> [II.] Whether the OOR erred by concluding—without *in camera* inspection—that the [Office] sustained [its] burden of showing that nonexempt information was wholly intertwined with exempt information and could not be released after redaction.
>
> [III.] Whether the OOR improperly shifted the burden of proof to [Requesters] where the OOR's Final Determination was based, in part, on its conclusion that [Requesters] did not "challenge the credibility" of agency attestations—despite [Requesters'] request for an *in camera* review and the absence of any hearing or other mechanism to challenge the [Office's] claims.

Requesters' Br. at 2-3.

We have summarized our standard and scope of review in RTKL appeals as follows:

> Pursuant to Chapter 13 of the RTKL, with respect to appeals relating to decisions of Commonwealth agencies, this Court is the ultimate factfinder in RTKL disputes. Section 1301 of the RTKL, 65 P.S. § 67.1301. Accordingly, we owe no deference to the OOR's legal analysis or factfinding, as our standard of review of a final determination of the OOR is *de novo*. *Bowling v. Off. of Open Recs.*, [] 75 A.3d 453, 474 ([Pa.] 2013). In addition, we are "entitled to the broadest scope of review[,]" covering all justiciable issues raised and preserved below. *Id.* at 477. *See also Payne v. Pa. Dep't of Health*, 240 A.3d 221, 225 n.6 (Pa. Cmwlth. 2020). Unlike in other administrative agency contexts, "we . . . may substitute our own findings of fact for that of the agency." *W. Chester Univ. of Pa. v. Browne*, 71 A.3d 1064, 1067 n.4 (Pa. Cmwlth. 2013). We have the discretion to conduct a hearing, or to remand to the OOR, to supplement the record. *Id.*

Pa. Off. of Governor v. Brelje (Off. of Open Recs.), 312 A.3d 928, 932 (Pa. Cmwlth. 2024) (footnote omitted).

"The enactment of the RTKL in 2008 was a dramatic expansion of the public's access to government documents" and the "objective of the RTKL 'is to empower

citizens by affording them access to information concerning the activities of their government.'" *Levy v. Senate of Pa.*, 65 A.3d 361, 381 (Pa. 2013) (quoting *SWB Yankees LLC v. Wintermantel*, 45 A.3d 1029, 1042 (Pa. 2012)). "Courts should liberally construe the RTKL to effectuate its purpose of promoting access to official government information in order to prohibit secrets, scrutinize actions of public officials, and make public officials accountable for their actions." *Off. of General Counsel v. Bumsted*, 247 A.3d 71, 76 (Pa. Cmwlth. 2021) (citations, quotation marks and brackets omitted). Thus, items are presumed to be disclosable in response to an RTKL request so long as they qualify as a public record. *Dep't of Educ. v. Massey*, 348 A.3d 339, 345 (Pa. Cmwlth. 2025). Moreover, Section 305(a) of the RTKL clarifies the presumption that a record within an agency's possession is a public record does not apply if it is proven that "the record is exempt under Section 708 [of the RTKL]." 65 P.S. § 67.305(a); *Pa. Dep't of Educ. v. Bagwell*, 114 A.3d 1113, 1122 (Pa. Cmwlth. 2015). In other words, if a record is exempt under Section 708(b), it is not a public record subject to disclosure under the RTKL. 65 P.S. § 67.102. Nonetheless, an agency has some discretion under the RTKL to release otherwise exempt records. Section 506(c)(2) of the RTKL, 65 P.S. § 67.506(c)(2).

The RTKL permits redaction of "the information which is not subject to access." Section 706 of the RTKL, 65 P.S. § 67.706. As we explained in *Commonwealth Department of Labor and Industry v. Simpson*, 151 A.3d 678 (Pa. Cmwlth. 2016):

> If a record is not exempt from disclosure, but contains information that is not subject to access, the agency may discharge its duty by providing redacted records. . . . Conversely, if a record is exempt from disclosure under the RTKL and thus is not a public record, it need not be redacted in accordance with Section 706 of the RTKL.

Id. at 682 (citation omitted). Section 708(a)(1) of the RTKL requires the agency that is receiving the RTKL request to bear the burden to prove, by a preponderance of the evidence, that the requested record is exempt from public access. 65 P.S. § 67.708(a)(1). The exceptions to disclosure of public records must be narrowly construed given the RTKL's remedial nature. *California Borough v. Rothey*, 185 A.3d 456, 465 (Pa. Cmwlth. 2018).

As we explained in *McGowan v. Pennsylvania Department of Environmental Protection*, 103 A.3d 374 (Pa. Cmwlth. 2014),

> [t]estimonial affidavits found to be relevant and credible may provide sufficient evidence in support of a claimed exemption. Affidavits are the means through which a governmental agency justifies nondisclosure of the requested documents under each exemption upon which it relied upon. The affidavits must be detailed, nonconclusory, and submitted in good faith. Absent evidence of bad faith, the veracity of an agency's submissions explaining reasons for nondisclosure should not be questioned.

Id. at 381 (citations, quotation marks, and ellipsis omitted).

Here, the OOR denied Requesters' appeal based on security exemptions under Section 708(b)(1)(ii), (2) and (3)(iii) of the RTKL.[5] To establish the personal

[5] The Office also asserted two additional exemptions: the deliberative process exemption, and the criminal investigation exemption. We reject Requesters' argument that the Office waived the deliberative process exemption by failing to assert it in its initial response denying their records request. *See Levy*, 65 A.3d at 380 (holding an agency does not waive reasons for non-disclosure simply because they were not addressed in the initial written response). Nonetheless, as Requesters correctly note, the deliberative process exemption does not apply to the Report. In *Chester Water Authority*, our Supreme Court determined the plain language of the deliberative process exemption under the RTKL did not extend the exemption to consultants contracted with an agency. 249 A.3d at 1111-14. Here, the Office and PSP retained the Consultant as a contractor to conduct an independent security review. The criminal investigation exemption under Section 708(b)(16)(vi)(A) of the RTKL prevents the disclosure of a record if it would reveal the institution, progress or result of a criminal investigation. 65 P.S. § 67.708(b)(16)(vi)(A). The criminal investigation exemption, however, is inapplicable. Our review of the unredacted records
(Footnote continued on next page…)

security exemption under Section 708(b)(1)(ii), "an agency must show: (1) a 'reasonable likelihood' of (2) 'substantial and demonstrable risk' to an individual's security if the information sought is not protected." *Carey v. Pa. Dep't of Corr.*, 61 A.3d 367, 373 (Pa. Cmwlth. 2013) (citation omitted). We have "defined substantial and demonstrable as actual or real and apparent . . . [and m]ore than mere conjecture is needed." *Id.* at 373-74 (internal quotation marks and citation omitted). Importantly, "[g]eneral, broad-sweeping conclusions will not be a substitute for actual evidence of the likelihood of a demonstrable risk to the individuals involved posed by a particular disclosure." *Governor's Off. of Admin. v. Pennsylvanians for Union Reform, Inc.*, 105 A.3d 61, 66 (Pa. Cmwlth. 2014) (citation omitted).

An agency establishes the public-safety exemption under Section 708(b)(2) when it shows by a preponderance of the evidence "that (1) the record at issue relates to a law enforcement or public safety activity; and (2) disclosure of the record would be 'reasonably likely' to threaten public safety or a public protection activity." *Rothey*, 185 A.3d at 468 (citation omitted). Our Supreme Court has further expounded on this exception.

> There can be no question that law enforcement agencies require the ability to protect documents that would reveal methods, protocols, identities, and other information the secrecy of which is essential to the agencies' ability to ensure public safety. Thus, even while construing the public safety exception strictly, courts should proceed with care not to narrow its application so much that public safety is compromised.

Am. C. L. Union of Pa. v. Pa. State Police, 232 A.3d 654, 666 (Pa. 2020).

To establish the infrastructure safety exemption under Section 708(b)(3)(iii), an agency must establish the disclosure of records creates a reasonable likelihood of

---

demonstrates the E-mail and the Report do not discuss the institution, progress, or result of such investigation. Thus, our review is limited to the application of the Office's security exemptions.

endangering the safety or physical security of a building. *Allegheny Cnty. Dist. Att'y's Off. v. Wereschagin*, 257 A.3d 1280, 1299 (Pa. Cmwlth. 2021). Similar to the public safety exemption, "more than mere speculation is necessary for an agency to meet its burden." *Id.* (citation and quotation marks omitted).

a. In Camera Review

With the foregoing in mind, we now address Requesters' first issue that the OOR abused its discretion in failing to enforce its order directing the Office to submit the records for *in camera* review when the Office declined to comply with that order. According to Requesters, the Office's noncompliance and the OOR's failure to enforce its order renders "meaningless" the OOR appeal process because "any agency could prevent neutral adjudication by refusing to submit records for inspection." Requesters' Br. at 9. Consequently, Requesters urge this Court to conduct *in camera* inspection of the records.

Generally, when "an agency sufficiently explains the basis for nondisclosure through an affidavit, a log or *in camera* review may not be necessary." *UnitedHealthcare of Pa., Inc. v. Pa. Dep't of Hum. Servs.*, 187 A.3d 1046, 1060 (Pa. Cmwlth. 2018). However, *in camera* review is both available and, in certain circumstances, helpful in resolving RTKL matters. *See McKelvey v. Pa. Dep't of Health*, 255 A.3d 385, 413 (Pa. 2021) ("[I]t was incumbent upon the OOR, and, ultimately, the Commonwealth Court, to consider the alleged exemptions applicable to such financial information, to review the information at issue–*in camera* if beneficial–and to fully consider the reasons proffered to support exemption from disclosure."). This is one such case.

Here, as Requesters aptly point out, the Office's statements and affirmations "sound evasive, overly vague, and conclusory." Requesters' Br. at 9. The Office's

statements for withholding the E-mail and the Report largely track the language of the exemptions it asserted. Additionally, the Office's own statements undercut its position that the E-mail and the Report should be withheld. In response to the OOR's August 1, 2025 letter, the Office conceded the E-mail may be redactable. Tellingly, undermining its asserted security concerns, the Office offered seemingly contradictory statements concerning the Report. On the one hand, it argued "[n]othing within the [R]eport is severable from the sensitive security information that i[t] contains," and on the other hand, it conceded some portions of the Report simply provide instructions on how to use and implement the Report. R.R. at 40a. Accordingly, further review of the records was warranted. The OOR, therefore, abused its discretion in failing to enforce its *in camera* order.[6]

b. This Court's Review

Given our role as the ultimate finder of fact and our clear authority to expand the record in appeals from final determinations of the OOR, and to provide finality to the parties, we ordered the Office, on September 23, 2026, to file physical copies of the unredacted records responsive to Requesters' May 22, 2025, RTKL request for *in camera* inspection. Without unredacted records, we would be unable to conduct a meaningful review of Requesters' claims based on the present record, and we could not properly consider and assess the applicability of the Office's asserted exemptions. The Office complied.

[6] Given our disposition of Requesters' first issue, we need not address their remaining issues.

c. The E-mail

Although it contains limited personal information (e.g., e-mail addresses of sender and recipient, and cell phone number of sender),[7] the E-mail does not appear to discuss the process used to develop the Report and recommendations contained therein. The E-mail merely transmits the Report as an attachment to the Office. Without providing any specific or sensitive information, the E-mail generally references the entities and individuals who would draw upon the Report's conclusions. Thus, contrary to the Office's assertion, the E-mail does not pose safety concerns, and therefore, is not subject to the security exemptions. Accordingly, the E-mail must be disclosed.

d. The Report

As for the Report, we agree with the Office that significant portions of it implicate security exemptions set forth in Section 708(b)(1)(ii), (2) and (3)(iii). To highlight the security risks following from the Report's disclosure, the Office references several attacks on government officials. Office's Br. at 8-11. For instance, the Office mentions the Federal Bureau of Investigation's October 2020 arrest of 14 people charged with plotting to kidnap Michigan Governor Gretchen Witmer; the October 28, 2022 break-in at then-Speaker Nancy Pelosi's California residence and the subsequent hammer attack on her husband; the June 14, 2025 shooting of four Minnesota state legislators and their spouses at their homes; and the January 5, 2026 attack on Vice President JD Vance's Cincinnati, Ohio, residence.

[7] The Office does not assert the personal information exemption under Section 708(b)(6)(i)(A) of the RTKL. *See* 65 P.S. § 67.708(b)(6)(i)(A) (exempting "[a] record containing all or part of a person's Social Security number, driver's license number, personal financial information, home, cellular or personal telephone numbers, personal e-mail addresses, employee number or other confidential personal identification number").

Without even having to examine the 75-page Report line by line, as we did here, to determine which portions contain exempt content, the Report's structure and content make clear that it contains both exempt and non-exempt information. Stated otherwise, the Report not only contains specific information threatening the safety and security of the Governor, but also broad, general information that does not bear any relation to public safety. Our review of the unredacted records reveals that page 1 of the Report is a cover page. Specifically, it identifies the title of the Report, site name, owner, site operator, security operator, report recipient, site address, website, and site type. The bottom of the cover page identifies the name and company of the author. This information does not fall under the Office's asserted security exemptions.

Similarly, page 2 of the Report identifies the names, positions and contact information of the individuals who performed the security review of the incident, and the names, positions and contact information of the facility contacts. This information is not subject to the asserted security exemptions, and the Office otherwise does not assert the personal information exemption under Section 708(b)(6) of the RTKL. Thus, page 2 of the Report must be disclosed.

Pages 3 and 4 contain a table of contents. Starting with "Table of Contents" at the top of page 3 until the subheading "Limitations," the information is not subject to any asserted exemptions. The remaining subheadings under "Executive Summary – General" must be redacted based on the asserted security exemptions.

Next, the heading "Executive Summary – Findings" on page 3 is also not subject to the asserted security exemptions. However, all ensuing subheadings under "Executive Summary – Findings" on page 3 implicate the asserted security exemptions, and must therefore be redacted.

The information, starting with "Facility Overview" through the subheading "Most Recent Renovations" on page 3, is not subject to the exemptions. Similarly, the subheading "Crime Data" on page 4 also does not satisfy any of the exemptions. The remaining subheadings under "Facility Overview" on pages 3 and 4 implicate the security exemptions and must therefore be redacted.

Finally, except for the heading "Security Operations – Assessment Specifics" on page 4, the remaining subheadings are subject to redactions because of asserted security exemptions.

Pages 5 through 10 of the Report contain an "Executive Summary – General." On page 5, the information under the subheadings "Purpose," "Disclaimer," "Information and Report Sharing," and "Forms – General" is not subject to the asserted security exemptions. Specifically, the information consists of general introductory material explaining how to use the Report and would not pose a security threat or a safety risk. Likewise, the information under the subheadings "Report Structure," and "Limitations" on page 6 is not subject to the exemptions.

However, the information following the "Limitations" sections starting at the bottom of page 6 and ending at the bottom of page 10 satisfies the asserted security exemptions. It therefore must be redacted.

Next, except for the heading "Executive Summary – Findings," all information contained on pages 11 through 20 of the Report concerns public safety and is thus subject to redaction because of the exemptions. The information immediately under the heading "Facility Overview," and subheadings "Facility Description – Relational," "Facility Description – General," and "Most Recent Renovations," from page 21 through the link to Pennlive.com on page 23, is not subject to the security asserted exemptions. The information in these sections

appears to come from publicly available sources, including Google Earth, www.pa.gov, and PennLive.com. Specifically, these sections provide general geographic information about the location of the Governor's Residence, its size, visitor hours, and recent non-security renovations to public spaces. Accordingly, the Office's asserted security exemptions are not implicated.

Following the PennLive link on page 23 through the bottom of page 28 of the Report, all information concerns public safety and is therefore subject to the asserted security exemptions. This information must be redacted.

The information under the subheading "Crime Data" on page 29 though the end of the first paragraph on page 31, which generally relates to the City of Harrisburg, is not subject to any exemptions. The data and statistics are publicly available on the Pennsylvania Uniform Crime Reporting System. Additionally, the Report examined data on the FBI's Crime Data Explorer website. Finally, from the subheading of the second paragraph on page 31 through the end of the Report on page 75, all information is subject to security exemptions and redactions. However, the heading "Security Operations – Assessment Specifics" on page 32 is disclosable.

Thus, narrowly construing the asserted security exemptions, we conclude the Office must disclose a redacted copy of the Report consistent with this memorandum opinion.[8] *Cf. Myers v. Pa. Dep't of Corr.* (Pa. Cmwlth., No. 268 C.D. 2024 filed Feb. 24, 2024), slip op. at 5 (ordering disclosure of the Department of Corrections' policy

[8] This case is distinguishable from *Simpson*, where the Court held information requested was exempt from disclosure in its entirety because all requested information related to individuals' claims for workers' compensation benefits under Section 708(b)(28)(ii)(B) of the RTKL. *Simpson*, 151 A.3d at 683-85. The security exemptions asserted here depend on "the consequences of disclosure." *Id.* at 683 n.11.

with limited redactions, concluding it contained broad, general information and did not threaten public safety).[9]

CONCLUSION

In light of the foregoing, upon careful review of the unredacted records, we reverse the OOR's final determination, and direct the Office, consistent with this memorandum opinion, to disclose to Requesters a copy of the E-mail and a redacted copy of the Report within 14 days of this Court's Order.

_____
STACY WALLACE, Judge

[9] An unreported panel decision of this Court, "issued after January 15, 2008," may be cited "for its persuasive value[.]" Section 414(a) of the Commonwealth Court's Internal Operating Procedures, 210 Pa. Code § 69.414(a).

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

David Osborne and Commonwealth Foundation, Petitioners	:	
v.	:	No. 1580 C.D. 2025
Pennsylvania Office of the Governor (Office of Open Records), Respondent	:	

O R D E R

AND NOW, this 4th day of November 2026, the November 3, 2025 final determination of the Office of Open Records is hereby **REVERSED**, and the Pennsylvania Office of the Governor is **DIRECTED** to disclose to David Osborne and Commonwealth Foundation redacted copies of the records responsive to their May 22, 2025 Right-to-Know Law[10] request, consistent with the foregoing memorandum opinion, within 14 days of the date of this Order.

_____
STACY WALLACE, Judge

[10] Act of February 14, 2008, P.L. 6, 65 P.S. §§ 67.101-67.3104.