

NOTIFY

12

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
Civil No. 2384CV01076

AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC.

v.

OFFICE OF THE STATE AUDITOR

**MEMORANDUM OF DECISION AND ORDER ON DEFENDANT'S MOTION
AND PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT**

Plaintiff American Civil Liberties Union of Massachusetts, Inc. ("ACLUM") brings this action against the Office of the State Auditor ("OSA") seeking the production of certain materials it requested from OSA under the Massachusetts Public Records Law, G.L. c. 66, § 10 (the "Public Records Law"). ACLUM asserts that OSA unlawfully redacted certain passages from those records pursuant to an improper invocation by OSA of the public safety exemption, as set forth in G.L. c. 4, § 7 Twenty-sixth (n).

OSA and ACLUM have each moved for summary judgment. After hearing and review of the parties' written submissions, and after also conducting a post-hearing *in camera* review of the disputed passages, the Court **DENIES** OSA's motion, **ALLOWS** ACLUM's motion, and **ORDERS** OSA to produce to ACLUM unredacted copies of the requested records.

BACKGROUND

The following undisputed facts are drawn from the parties' Consolidated Statement of Additional Facts and additional admissible evidence in the summary judgment record.

On consecutive days in March 2023, OSA issued two Official Audit Reports, titled: (1) Plymouth County Sheriff's Department – A Review of Healthcare and Inmate Deaths for the period July 1, 2019 through June 30, 2021 (dated March 15, 2023) (hereafter, the “PCSD Report”); and (2) Barnstable County Sheriff's Department – A Review of Healthcare and Inmate Deaths for the period July 1, 2019 through June 30, 2021 (dated March 16, 2023) (hereafter, the “BCSD Report”) (collectively, the “Reports”).

Each Report contains an Executive Summary describing the objectives of OSA's audit, which were the same for both Sheriff's Departments. Those objectives focused on examining each Department's provision of healthcare services to inmates in their custody as well as the Departments' compliance with regulatory requirements concerning inmate deaths.

OSA prepared two versions of each Report: (1) an unredacted version, which it transmitted to each respective Sheriff; and (2) a redacted version, which it released publicly. The unredacted PCSD Report was 13 pages in length, not including the cover page and the table of contents. The unredacted BCSD Report was 17 pages in length.

In the publicly released versions of both Reports, OSA redacted in full the last section, which comprised approximately 1 page. OSA also redacted the descriptive title for that section wherever it appeared, including in each Report's table of contents.

By letters dated March 15 and March 17, 2023, ACLUM submitted requests to OSA under the Public Records Law (the “Requests”) for copies of the unredacted versions of both Reports.

On March 29, 2023, OSA responded to the Requests by sending ACLUM copies of the publicly released versions of the Reports that identified each place in the Report where OSA had made redactions, but not the content of the text that OSA had removed. In an accompanying

transmittal email to ACLUM, OSA stated: “OSA has applied redactions in reliance on exemption (n) of the Commonwealth’s Public Records Law, Section 7(26) of Chapter 4 of the General Laws, which allows for the withholding of certain records, such as confidential and sensitive information, if their disclosure is likely to jeopardize public safety.”

On May 9, 2023, ACLUM filed its Complaint in this action, seeking declaratory and injunctive relief ordering OSA to produce the Reports in unredacted form.

In an Affidavit filed in this action on or about October 13, 2023, Joseph C. Arguijo, the Director of Judiciary and Law Enforcement Audit at OSA, averred that the redactions to the Reports at issue in this matter “were made in order to protect information about cyber security whose disclosure, in the reasonable judgment of the records access officer, would jeopardize public safety and cyber security.” Separately, in remarks quoted in articles about this lawsuit published in *The Boston Globe* and the *Cape Cod Times*, the Auditor stated: (1) the redacted information “was withheld because it relates to cybersecurity”; and (2) “Carelessly publicizing identified cybersecurity challenges found within state systems puts those systems at risk.”

Approximately seven months after the commencement of this action, both parties moved for summary judgment. The Court conducted a hearing on that motion. Following that hearing, and after further review of the parties’ written submissions, the Court issued an Order directing OSA to provide the Court with unredacted versions of the Reports for *in camera* review. OSA complied with that Order and, in the copies of the Reports that it produced, highlighted for the Court’s benefit the specific words and passages that OSA had redacted pursuant to its invocation of exemption (n).

DISCUSSION

“Summary judgment is appropriate where there is no material issue of fact in dispute and the moving party is entitled to judgment as a matter of law.” *Adams v. Schneider Elec. USA*, 492 Mass. 271, 280 (2023).

I. The Public Records Law

Two statutes govern requests made under the Public Records Law: G.L. c. 66, § 10(a), which requires agencies, like OSA, to provide access to public records on request; and G.L. c. 4, § 7, Twenty-sixth, which defines by type and by category what documents fall within the meaning of “public records”. *See, e.g., Mack v. District Attorney for the Bristol District*, 494 Mass. 1, 9 (2024). “The primary purpose of these statutes is to provide the public ‘broad access to government records’” *Id.* Consistent with this purpose, there is a “statutory presumption in favor of disclosure, with the burden placed on the government agency to prove by a preponderance of the evidence that a record may be withheld.” *Id.* at 10.

The Legislature has specifically enumerated certain exemptions from the definition of “public records.” One of those exemptions – and the exemption at issue here – is the public safety exemption, which is set forth in G.L. c. 4, § 7, Twenty-sixth (n). (hereafter, “exemption (n)”).

Exemptions to the Public Records Law are “strictly and narrowly construed.” *Mack*, 494 Mass. at 10. “Whether an exemption applies requires a case-by-case analysis.” *Id.*

II. Exemption (n)

The public safety exemption applies to:

(n) records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or

safety of persons or buildings, structures, facilities, utilities, transportation, cyber security or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (c) of section 10 of chapter 66, is likely to jeopardize public safety or cyber security.

G.L. c. 4, § 7 Twenty-sixth (n).

The dispute at issue here involves OSA's invocation of the language in exemption (n) that shields cyber security records from disclosure. Specifically, the parties disagree over whether OSA has met its burden of establishing, by a preponderance of the evidence, that the passages it redacted from the Reports constitute "records relating to . . . cyber security . . . the disclosure of which, in the reasonable judgment of the record custodian . . . is likely to jeopardize . . . cyber security."

The Supreme Judicial Court has construed exemption (n) to require a two-part analysis. *See People for the Ethical Treatment of Animals, Inc. v. Department of Agricultural Resources*, 477 Mass. 280, 289-90 (2017) (hereafter, "*PETA*"). First, a court must assess whether the records at issue resemble the types of public safety records listed as examples in the exemption – e.g., blueprints, schematic drawings, vulnerability assessments, and the like. "The touchstone of this inquiry is whether, and to what degree, the record is one a terrorist 'would find useful to maximize damage,' . . . and in that sense jeopardize public safety." *Id.* at 289. Second, a court must decide whether the record custodian "has provided sufficient factual heft" in support of her invocation of exemption (n) for the court "to conclude that a reasonable person would agree with the custodian's determination" that disclosure of the record is "likely to jeopardize public safety." *Id.* at 290. In performing the foregoing analysis, a court is to review the custodian's determination *de novo*. *Id.* at 291.

As the parties correctly observe, at the time the Supreme Judicial Court decided *PETA*, exemption (n) did not include “cyber security” in the provision’s enumerated list of representative document types, such as blueprints, plans, policies, procedures, and the like. The Legislature amended the statutory text to insert the words “cyber security” at a later point in time. In the Court’s review, the foregoing chronology has no relevance to its decision of the parties’ Rule 56 motions. The reasoning set forth in *PETA* governs the applicability of exemption (n) to all categories of records ostensibly relating to public safety and security. There is nothing about the manner in which the Legislature inserted “cyber security” into the provision that suggests the Legislature intended for cyber security records to be treated differently from the other types of records enumerated in the exemption.

III. The OSA Redactions

The Court has conducted an *in camera* review of the passages that OSA redacted from the Reports. It has examined those passages pursuant to the two-part analysis that *PETA* defines. Having completed that review, the Court concludes – on the undisputed facts contained in the summary judgment record – that OSA has not met its burden on either prong of the *PETA* test. Despite OSA’s invocation of the protection that exemption (n) affords to “cyber security” records, the Court has found nothing in the language that OSA redacted from the Reports that might reasonably support the application of that exemption here.

As noted, the central focus of the audits was healthcare services provided to inmates, together with a review of any inmate deaths that had occurred during the audited time period. Cyber security was not listed among the audit objectives.

Nonetheless, presumably as a result of OSA’s review of the Sheriff’s Departments’ maintenance and use of electronic medical records in providing healthcare services to inmates,

OSA included a short (approximately one-page) section at the end of each Report recommending certain improvements in PCSD's and BCSD's information technology systems. It is that section which OSA has redacted, in full, from the public versions of the Reports.

The Court has carefully reviewed the unredacted text. It contains no mention of any vulnerabilities in either Department's information technology systems that a reasonable person could conclude risks jeopardizing the safety or security of those systems if disclosed. Examples of such issues – if they were mentioned, which they are not – might include things such as the failure to timely apply certain security patches to the Department's servers (with perhaps a list providing specific examples of unapplied patches), or a caution regarding vulnerabilities identified by OSA in remote access VPNs being utilized by Department employees to access Department servers from outside the office. It is conceivable that such issues, if discussed with sufficient particularity and if unrectified despite the passage of more than one year since the Reports were released, might provide bad actors with insight into how they might gain unauthorized access to BCSD's or PCSD's IT systems.

The redacted passages from the Reports, however, contain no information remotely like this. To the contrary, they do little more than set forth – at a high level of generality – OSA's recommendation that the Departments develop additional written IT policies and procedures and provide more IT training to their employees.

Mindful of OSA's right to appeal this decision, the Court will refrain from discussing further the types of policies and training that OSA recommended. Suffice it to say, however, that the Court finds none of the recommendations to be particularly revelatory.

As just one illustration, the Court took note of a response that BCSD provided to OSA's recommendation regarding additional employee training. In that response, which is reproduced

in the short section at the end of the BCSD Report that OSA redacted in its entirety, BCSD advised that it was in the process of seeking funding from a particular grant program to be able to provide that training. BCSD identified the grant program by name; it identified the specific state agency that administered the program; and it described, in very general terms, the type of training that it hoped to conduct if it obtained grant funding.

As part of the Court's effort to assess what cyber security risk, if any, might result from ordering the disclosure of the foregoing information, the Court looked to see how much of it might already be out in the public domain. The results of that research were illuminating. The Court located a detailed description of the grant program on the public website of the Massachusetts Executive Office of Technology Services and Security ("EOTSS"). On that same public website, the Court found links to the complete contents of a 15-chapter EOTSS Handbook titled "Enterprise Information Security Policies and Standards." In the "Overview" to that Handbook, EOTSS states: "The EOTSS Enterprise Risk Management Office is responsible for writing, publishing, and updating all Enterprise Information Security Policies and Standards that apply to all Executive Department offices and agencies. This is a compilation of those policies and standards." The Court's review of the Handbook's chapter titles shows that the standards cover a wide range of cyber security topics, including access management, business continuity and disaster recovery, communication and network security, cryptographic management, information security risk management, physical and environmental security, secure system and software lifecycle management, and more. The full content of every chapter is accessible to the public on the EOTSS website.

If the state office responsible for technology security across the Commonwealth's entire executive branch has concluded, as it presumably has, that making the foregoing material

available on its public website does not “jeopardize” the security of the Commonwealth’s IT systems, the Court sees nothing in the passages that OSA redacted from the Reports that comes remotely close to creating any cyber security risk. The redacted passages list – by name only – a handful of IT policies and training programs that OSA recommended be implemented. By comparison, EOTSS’s public website contains not just the names but also the full text of every enterprise information security policy and standard applicable to executive branch offices and agencies.

Finally, although there is no need to go further, the Court notes that BCSD’s audit response – which OSA redacted – states that BCSD has adopted policies and procedures responsive to all of OSA’s recommendations. To the extent that any concern might exist about the risk of publicly revealing the names of IT policies that OSA concluded the Departments were lacking, the fact that BCSD adopted those policies more than a year ago surely reduces that risk – already minimal – to zero.

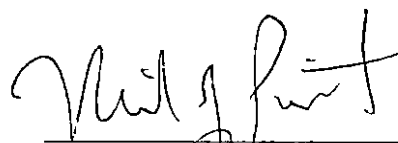
In sum, OSA has not met its burden to justify – under exemption (n) or otherwise – the passages from the Reports that it has withheld from ACLUM.

CONCLUSION AND ORDER

For the reasons set forth above, the Court **ALLOWS** ACLUM’s motion for summary judgment, **DENIES** OSA’s motion for summary judgment, and **ORDERS** OSA to produce unredacted copies of the Reports to ACLUM within thirty days from the date of issuance of this Order.

SO ORDERED.

Dated: May 31, 2024



Michael J. Pineault
Associate Justice of the Superior Court