COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss

SUPERIOR COURT
C.A. No. 2384CV01076

AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC.,

Plaintiff,

v.

OFFICE OF THE STATE AUDITOR,

Defendant.

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

Nobody disputes that exemption (n) protects important interests, including specific technical information about current, open cyber security vulnerabilities that would permit the theft of prisoner health data. In this case, however, the Office of the State Auditor has made no attempt to show that the redactions to its audit reports shield any such information whatsoever, much less only such information. And the context of the redactions—which include not only entire sections of two audit reports, but also the sections' titles, portions of the reports' ultimate conclusions, and snippets of text interspersed throughout the other sections—strongly indicates that a much broader category of information is being improperly withheld. The Auditor's Office appears to contend that even releasing the general subject matter of the withheld section would be unacceptably risky, but it does not explain why, and, in any event, the Auditor herself has already described that information in statements to two newspapers.

Simply put, the defendant has not carried its burden to justify this extreme degree of secrecy. And prisoners, their families, legal advocates, and the public need the information in

these reports to understand whether prisoners' legal rights to medical care and medical privacy have been imperiled.

Accordingly, the Court should grant plaintiff ACLU of Massachusetts's motion for summary judgment and order production of the complete reports. Or, if not, the Court should at least conduct *in camera* review of the reports with the participation of all the parties under a protective order. Such review would permit the Court itself to identify and release all of the non-exempt text that is segregable from any specific technical information about current, open cyber security vulnerabilities that would permit the theft of prisoner health data.

FACTUAL AND PROCEDURAL BACKGROUND

The Office of the State Auditor (the "OSA") exists to conduct "audits, investigations, and studies to promote accountability and transparency, improve performance, and make government work better."[1] The OSA's broad powers include compelling the production of records from the audited agencies, issuing audit reports, and requiring agencies to respond in writing to any adverse or critical results. *See* G.L. c. 11, § 12. As the current Auditor has herself noted, "Folks are fed up. They're tired. They want access. They want to know that their officials are not playing games with their taxpayer dollars. They want to know that they can trust their elected officials."[2]

Last March, the OSA issued an audit report concerning the Plymouth County Sheriff's Department ("PCSD") entitled "Plymouth County Sheriff's Department—A Review of Healthcare and Inmate Deaths for the period July 11, 2019, through June 30, 2021" (the "Initial PCSD Report"). SOF ¶ 3; JA Ex. I. Later that same month, it issued a separate report addressing the same topic for the Barnstable County Sheriff's Office ("BCSO" and the "Initial BCSO Report").

[1] https://www.mass.gov/orgs/office-of-the-state-auditor ("About the Office of the State Auditor")

[2] https://www.wgbh.org/news/politics/2023-07-26/auditor-dizoglio-asks-for-ags-support-in-her-audit-of-the-legislature

SOF ¶ 4; JA Ex. J.

These reports are important. Sick prisoners cannot travel on their own to the doctor's office or a hospital. They are utterly dependent on the incarceration facility to provide necessary medical and psychiatric care to treat sickness and prevent death. *See, e.g.*, *Estelle v. Gamble*, 429 U.S. 97, 103 (1976) (explaining that a prisoner "must rely on prison authorities to treat his medical needs," and that failure to do so may result in "pain," "suffering," "torture," or "a lingering death"). Similarly, because prisoners must receive care through the incarceration facility, they also depend on the facility to undertake adequate precautions to protect their personal medical and psychiatric information. The information collected by the facility during the course of medical or psychiatric treatment can be excruciatingly private—indeed, in some cases, so private that the facility's duty to safeguard the information is literally a constitutional obligation or otherwise required by federal law. *See, e.g.*, *Doe v. Delie*, 257 F.3d 309, 317 (3d Cir. 2001) (recognizing prisoner's constitutional right against unnecessary disclosure of HIV-positive status); *Powell v. Schriver*, 175 F.3d 107, 112 (2d Cir. 1999) (recognizing prisoner's constitutional right against unnecessary disclosure of sexual identity); 42 CFR Part 2 (mandating heightened confidentiality protections for substance use disorder patient records).

Thus, whether a correctional facility is providing adequate medical and psychiatric care to its prisoners, and whether it is properly safeguarding the highly personal information that it acquires in the process, are matters of the utmost interest to prisoners, their families, advocates who work on their behalf, and the public at large. *See, e.g.*, *Braggs v. Dunn*, 382 F. Supp. 3d 1267, 1272 (M.D. Ala. 2019) (explaining, in case concerning alleged deficiencies in correctional mental health care, that citizens "indisputably have a powerful interest in overseeing [the prison system's] performance"). In this case, the OSA's Initial PCSD Report seemingly gave PCSD a clean bill of

health, including in critical areas such as responses to prisoner deaths (there had been two deaths in the audit period), providing adequate medical screenings, and providing medical care in response to Sick Call requests. SOF ¶ 14. The Initial BCSO Report reached similar findings, but faulted that facility for delays and documentation failures in its admission medical screenings. SOF ¶ 15.

Both initial reports contained a concerning caveat, however: "Our audit of [the facility] identified one other issue, which has been omitted from this report in accordance with exemption (n) of the Commonwealth's public records law." SOF ¶ 13. And both reports were accompanied by a cover letter stating that the report was "the limited version that we are issuing publicly" and "excludes" one issue that was the subject of the audit. SOF ¶ 12. Neither the reports, nor the cover letters, gave any indication of what that issue actually was, or what (if anything) was being done to address it. SOF ¶¶ 12-13.

Concerned by these omissions, the ACLU of Massachusetts ("ACLUM") submitted public records requests for the complete reports. SOF ¶¶ 3-4. The OSA then produced what appear to be the complete versions of the reports with redactions interspersed throughout (the "Redacted PCSD Report" and the "Redacted BCSO Report"). SOF ¶¶ 5-6. Each of those reports contained an entire addition section—which was not present in the initial reports—that is completely redacted. SOF ¶ 16. Even the title of that section and any general statements about its subject matter are being withheld. *Id.* Also concerning: the redacted reports indicate that text was removed from other parts of the initial reports, without any way for the public to discern that it was missing. SOF ¶ 17. In some cases, where the initial reports had indicated satisfactory results, the redacted text appears to qualify those conclusions. SOF ¶ 18. For example, where the initial report told the public that PCSD was providing intake medical screenings with an unqualified

"Yes," the Redacted PCSD Report reveals the answer was really "Yes; [*redaction*]". *Id.*

3. Did PCSD provide medical receiving screenings to its inmates upon admission, and intake physical examinations, in accordance with Sections IV and VII of PCSD's Policy 630 (Medical Services) and Sections IV and VII of PCSD's Procedure 630 (Medical Services)?	Yes

3. Did PCSD provide medical receiving screenings to its inmates upon admission, and intake physical examinations, in accordance with Sections IV and VII of PCSD's Policy 630 (Medical Services) and Sections IV and VII of PCSD's Procedure 630 (Medical Services)?	Yes; [redacted]

Figure 1: Conclusion 3 in the Initial PCSD Report (above) and in the Redacted PCSD Report obtained by ACLUM (below)

As noted above, the OSA redacted from these reports literally everything about the missing material, including items like: the title of the missing section, any statements concerning its general subject matter, and its impact on the OSA's audit results. SOF ¶ 16. Nor did the OSA's accompanying cover emails provide any explanation of the nature of the redacted material, beyond a conclusory citation to exemption (n). SOF ¶ 19. The OSA's redacted reports and letter did not even say if the "issue" had been resolved or is still an active problem. SOF ¶ 20. Consequently, given the potentially ongoing deficiency to important prisoner health services, and faced with a final denial from the OSA, ACLUM filed this public records lawsuit for the complete report last May. *See* D.E. 1 (Complaint).

The Auditor's public response to this lawsuit reveals that the OSA *never* actually viewed at least certain information about the missing "issue" as likely to jeopardize safety or security. *See* SOF ¶¶ 21-25. The Auditor asserted in the Boston Globe that the redacted material concerns "identified cyber security challenges found within state systems" identified by the OSA's "new IT audit unit dedicated to auditing information technology with a focus on cyber security in state agencies." SOF ¶ 21, 24-25. The Auditor provided essentially identical information to the Cape Cod Times. SOF ¶ 22, 24-25.

Of course, the OSA did not release the specific technical details of any ongoing cyber security deficiencies. There is no evidence that the OSA's reports even contain that level of technical detail. SOF ¶¶ 26-27. But, in any event, the OSA's public statements confirm that the OSA does not view the general subject matter of the redacted material (including the fact that BCSO and PCSD had or have security vulnerabilities relating to prisoner medical information), or the overall audit results, as requiring secrecy. The Auditor herself has taken that position on her agency's behalf. SOF ¶¶ 21-25.

The information released by the Auditor makes the release of the unredacted (or at least less redacted) audit reports all the more urgent. Prisoners, their families, advocates, and the public need to know (among other things) whether prisoners' private health information was exposed by cyber security failures at PCSD and BCSO, when that exposure started, whether the information was actually breached, whether the vulnerabilities are now corrected, and, if not, whether there is any plan to correct them. These are basic types of information that *everyone* deserves to know about their private health data, *see, e.g.*, 45 CFR § 164.404 (HIPAA regs recognizing need to respond to health information data breaches)—and particularly prisoners, who have no choice of health providers and must rely on the cyber security infrastructure created by the facility to which they are involuntarily assigned.

Of course the OSA should not release the technical specifics of ongoing, open cyber security vulnerabilities that would allow criminals to steal prisoner healthcare information. No party before the Court wants to see that happen. But there is simply no evidence that the OSA's redactions are concealing *any* such information, much less *only* such information. SOF ¶¶ 26-27. The OSA has not met its burden here to justify withholding redacted information from prisoners and the public under exemption (n).

LEGAL STANDARD

A court reviews a records custodian's determination whether to disclose or withhold a record de novo. *People for the Ethical Treatment of Animals v. Department of Agric. Resources*, 477 Mass. 280, 291 (2017) ("*PETA*"); G.L. c. 66, § 10A(d)(1)(ii). Exemption (n)'s "inclusion of the phrase 'reasonable judgment of the record custodian' . . . neither requires or even invites any heighted level of deference to the records custodian's initial determination." *PETA*, 477 Mass. at 291. Summary judgment is appropriate when the record shows that "there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Mass. R. Civ. P. 56(c).

ARGUMENT

I. DEFENDANT HAS NOT SATISFIED ITS BURDEN TO PROVE THAT ITS REDACTIONS ARE LAWFUL UNDER EXEMPTION (N)

The Commonwealth's public records law was first enacted in 1973 "to give the public broad access to government documents." *Georgiou v. Comm'r of Dep't of Indus. Accidents*, 67 Mass. App. Ct. 428, 431 (2006) (citing *Harvard Crimson, Inc. v. President & Fellows of Harvard College*, 445 Mass. 745, 749 (2006)). Explicit in the language of the statute is the presumption "that each record sought is public." G.L. c. 66, § 10A(d)(1)(iv). To overcome this presumption, a custodian of records has the burden to prove that one of the limited statutory exceptions applies. *Id.* These statutory exemptions "must be strictly and narrowly construed." *Boston Globe Media Partners, LLC v. Department of Pub. Health*, 482 Mass. 427, 432 (2019) (quoting *Globe Newspaper Co. v. District Attorney for the Middle Dist.*, 439 Mass. 374, 380 (2003)).

Here, to justify withholding the PCSD and BCSO Reports concerning prisoner deaths and healthcare, OSA has invoked exemption (n). Exemption (n) allows a custodian to withhold

> 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). OSA has failed to meet its burden to prove that this exemption applies.

In its papers, the OSA references a May 19, 2023 decision by the Supervisor of Records, apparently in response to a similar request by a Mr. Coleman Herman for the complete PCSD Report.[3] To be clear, ACLUM was not part of any proceeding before the Supervisor concerning these reports. Indeed, although the Supervisor issued its letter last May, the OSA didn't even inform ACLUM of that proceeding or resulting letter until it served its summary judgment papers the following October. In any event, the Supervisor's decision does not have preclusive effect on ACLUM, which was not a party in that matter and had no opportunity to present any evidence or arguments. *See, e.g.*, *Heacock v. Heacock*, 402 Mass. 21, 23-25 (1988) (claim and issue preclusion operate on same parties or their privies). Moreover, regardless of what the Supervisor might have concluded, this Court is required by the public records statute to consider the matter de novo and reach its own conclusions. *See* G.L. c. 66, § 10A(d)(1)(ii) ("[T]he superior court shall determine the propriety of any agency or municipal action de novo . . . .").

A. The Two-Part Inquiry Set Forth by the Supreme Judicial Court in *PETA* Governs the Application of Exemption (n)

The Supreme Judicial Court (SJC) held in *PETA* that a two-part inquiry governs the

[3] Mr. Herman appears to be a journalist for various New England publications: https://muckrack.com/colman-m-herman/articles.

application of exemption (n). Per the Court,

> [t]he first prong of exemption (*n*) probes whether, and to what degree, the record sought resembles the records listed as examples in the statute. 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. The second prong of exemption (*n*) probes the factual and contextual support for the proposition that disclosure of the record is "likely to jeopardize public safety." Because the records custodian must exercise "reasonable judgment" in making that determination, the primary focus on review is whether the custodian has provided sufficient factual heft for the supervisor of public records or the reviewing court to conclude that a reasonable person would agree with the custodian's determination given the context of the particular case.

PETA, 477 Mass. at 289-290 (citations omitted). The SJC reached this holding after examining the legislative history of exemption (n), which revealed that the exemption "was enacted as one of twelve sections in 'An Act providing protections against terrorism'" that was passed by the Legislature on the one-year anniversary of September 11, 2001. *Id.* at 288.

While OSA asks the Court to disregard the *PETA* standard due to amendments to exemption (n) that had not yet taken effect at the time of the SJC's decision, *see* Defendant's Br. at 5 (arguing that "the risk posed by disclosure of documents relating to cyber security . . . requires consideration through a different lens"), that argument is foreclosed by the *PETA* case itself and its progeny. According to OSA, the *PETA* analysis should not apply because the SJC's decision was based on an "earlier iteration" of exemption (n) that did not include the phrase "cyber security." *Id.* It is true that in 2016 the Legislature added "cyber security" to the "any other records" clause of exemption (n), and added "cyber security" after "public safety" in the "likely to jeopardize" clause. *See* St. 2016, c. 121, §§ 1-3. But the SJC's decision in *PETA* was issued *after* that revision, and the SJC specifically stated in *PETA* that it appeared that the insertion of the phrase "cyber security" into exemption (n), and other more "substantial" revisions to the public records law that took effect in 2017, would not "significantly alter [the Court's] analysis as to the

exemptions and their application." 477 Mass. at 281, n.3. Then again in 2020, the SJC "st[ood] by" this conclusion in *Rahim v. District Attorney for the Suffolk District* after examining the legislative history of the amendments. 486 Mass. 544, 553 (2020); *see also id.* at 554, n.14 (noting that the Legislature's intent was "to improve and strengthen and modernize the law, not to change the scope of the law") (quoting Sen. Jason M. Lewis).

While this Court need not look to the legislative history of exemption (n) given the pronouncements by the SJC and the lack of ambiguity in the statute, the legislative history shows that the addition of "cyber security" was merely intended to clarify that cyber security fell within the scope of the existing exemption, not change its scope. The Senate Committee on Ways and Means' summary of the draft bill that ultimately amended exemption (n) stated that the bill "*[c]larifies* that records relating to the cyber-security of systems in the commonwealth may be exempted from classification as public records." SOF ¶ 10 (emphasis supplied). On the day that the draft bill was announced, Senator Karen E. Spilka, Chair of the Senate Committee on Ways and Means, stated that even without the addition of the phrase "cyber security," exemption (n) "probably . . . would have included" cyber security within the meaning of the term "security," but "there were some folks and state agencies that asked to make it clearer." SOF ¶ 11. Thus, contrary to OSA's assertion, the addition of cyber security was not so "significant" so as to provide any basis for this Court to depart from the analysis directed by the Supreme Judicial Court in *PETA*, and much less to "defer to the agency's decision" in a manner contrary to the SJC's directives. Defendant's Br. at 6, n.1.

B. OSA's Conclusory Evidence and Arguments Fail to Satisfy Its Burden Under Exemption (n)

i. OSA Has Not Demonstrated that the Records Are Records a Terrorist Would Find Useful to Maximize Damage

As noted above, the first prong of exemption (n) examines "whether, and to what degree, the record sought resembles the records listed as examples in the statute," and the "touchstone of this inquiry is whether, and to what degree, the record is one a terrorist 'would find useful to maximize damage.'" *PETA*, 477 Mass. at 289-90 (citation omitted). The conclusory affidavit submitted with OSA's motion (JA Ex. G), which does little more than recite the words of the statute, fails to address these questions, and cannot meet the OSA's burden to prove that the exemption applies. *See* G.L. c. 66, § 10A(d)(1)(iv); *In re Subpoena Duces Tecum*, 445 Mass. 685, 688 (2006) (record custodian has the burden "to prove with specificity" that an exemption applies).

OSA has not presented any evidence that the redactions conceal information that a terrorist would find useful in maximizing damage. As noted above, OSA has redacted an entire section of each report, including the section's title, any general description of the section's subject matter and findings, and even items as innocuous as the entry in the table of contents and short snippets of text elsewhere in the report. SOF ¶¶ 16-17. OSA has not argued, much less proven by a preponderance of the evidence, that such general information would be useful to a terrorist. OSA has similarly failed to present evidence that the audit reports contain specific technical information about cyber security vulnerabilities that a terrorist could theoretically exploit. SOF ¶ 26. And even for such specific technical information to be useful, it would have to concern vulnerabilities that currently exist—*i.e.*, vulnerabilities that have not been corrected at the facilities since the audits. OSA has not presented any evidence of that, either. SOF ¶ 27. As a result, OSA has not shown that the records are likely to be helpful to terrorists, such that exemption (n) cannot be

applied. And even if the Court did conclude that the OSA has met its burden at this first step (which it should not), the extraordinary weakness of OSA's showing on the first prong would mean that its burden for demonstrating the second prong—that a "reasonable person" would agree that that disclosure of the records is "likely to jeopardize public safety or cyber security"—is "at its highest." *PETA*, 477 Mass. at 290-291.

ii. OSA Has Not Demonstrated that Disclosing the Redacted Material Is Likely to Jeopardize Public Safety or Cyber Security

OSA has not provided "sufficient factual heft" for the Court to conclude that a reasonable person would agree that disclosure of the redacted material is likely to jeopardize public safety or cyber security. *PETA*, 477 Mass. at 289-90. The affidavit submitted with OSA's motion contains four paragraphs, only one of which states, in the most conclusory terms, that "[t]he redactions 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." JA Ex. G. OSA asserts in its brief that it "affirmed" in the separate Supervisor of Records appeal that "the redactions are of a nature that a terrorist would find useful to maximize damage to public safety."[4] Defendant's Br. at 6. But as for "factual heft," OSA offers nothing.

In fact, it is evident that OSA did not reasonably believe that the mere fact that it performed cyber security audits, or the general subject matter of those audits, or the general findings of those audits that PCSD and BCSO have cyber vulnerabilities relating to prisoner health information, is the type of information that "a terrorist 'would find useful to maximize damage." *PETA*, 477 Mass. at 289. If OSA is willing to say that to media outlets (as it has, SOF ¶¶ 21-25), then there is no reason not to release similar information contained in the audit reports.

[4] As explained above, ACLUM was not part of that Supervisor of Records appeal, and that appeal has no impact on this case.

Further, OSA has not met its burden to show that the reports contain the types of information that could conceivably jeopardize public safety or cyber security if released. *PETA*, 477 Mass. at 290. As noted above, OSA has not presented any evidence that the reports contain technical specifics of ongoing, open cyber security vulnerabilities that would allow criminals to steal prisoner healthcare information. SOF ¶ 27. There is no evidence that the reports contain *any* technical specifics of vulnerabilities at all. SOF ¶ 26. Even if there were, there is no evidence that *any* such vulnerabilities remain uncorrected such that a terrorist could actually exploit them at the facility. And, even if that information were included, there is no evidence that the redacted material contains *only* such information. Indeed, given that OSA redacted an entire section of the reports (including the title), it is highly probable that more general information is being concealed, that such information is segregable from any technical details, and that such information could therefore be released. *See Reinstein v. Police Comm'r of Bos.,* 378 Mass. 281, 290 (1979) ("That some exempt material may be found in a document . . . does not justify cloture as to all of it.").

OSA seeks to absolve itself from its statutory-mandated burden to prove that its redactions are proper by asserting that "there is no way to demonstrate the reasonableness of the record custodian's decision without disclosure of the redactions themselves" and asking the Court to conduct *in camera* review of the unredacted reports. Defendant's Br. at 6. As the Supreme Judicial Court has explained, *in camera* inspection is an "unhappy" solution "because it forfeits bilaterality," and it is "to be used only in the last resort." *Reinstein v. Police Comm'r of Bos.*, 378 Mass. at 294-95. Here, where OSA has provided no factual support for its contention that disclosing the redacted material is likely to jeopardize public safety or cyber security, the Court would be justified in simply ordering the production of the unredacted PCSD and BSCO Reports.

C. If the Court Proceeds with *In Camera* Review, It Should Permit ACLUM's Counsel to View the Records and Participate in the Resulting Discussion of Their Contents

ACLUM understands that *in camera* review may be appealing in this particular case given the importance of protecting prisoner healthcare information. But if the Court elects to grant OSA's request for *in camera* review, ACLUM should at least have an opportunity to participate in the process and argue the implications of the reviewed material. The Court is empowered to do that with an appropriate protective order that provides ACLUM access to the unredacted reports strictly for the purposes of this case and enables ACLUM to have an informed discussion about the records with the Court and the agency. *See, e.g.*, *Worcester Telegram & Gazette Corp. v. Chief of Police of Worcester*, 436 Mass. 378, 385 (2002) (explaining that a judge may "permit counsel for the custodian and counsel for the party seeking production to have access to the documents subject to an appropriate protective order" to enable the parties to "particularize their arguments to the judge, citing specific materials, or portions of materials, that are exempt or subject to disclosure" and "relieve the judge from a tedious examination of materials against generalized claims that exemptions are applicable") (citation omitted). If the Court were to adopt this approach, it need not order the document be transmitted to ACLUM, but rather could authorize ACLUM to review it at the offices of the Attorney General, with the AGO maintaining physical custody of the document at all times.

CONCLUSION

For the foregoing reasons, ACLUM respectfully asks the Court to deny OSA's motion for summary judgment, grant ACLUM's cross-motion for summary judgment, and order OSA to produce the PCSD and BSCO Reports unredacted. In the alternative, if the Court adopts the approach of *in camera* review, ACLUM asks the Court to order OSA to permit ACLUM access to

the unredacted PCSD and BSCO Reports subject to an appropriate protective order, such that both parties can brief and argue the implications of its content through an appropriate adversarial process.

Dated: November 17, 2023

Respectfully submitted,

/s/ Natalie F. Panariello

Christopher E. Hart (BBO #625031)
Natalie F. Panariello (BBO #707579)
Foley Hoag LLP
155 Seaport Boulevard
Boston, MA 02210
(617) 832-1000
chart@foleyhoag.com
npanariello@foleyhoag.com

Daniel L. McFadden (BBO #676612)
American Civil Liberties Union
Foundation of Massachusetts, Inc.
One Center Plaza, Suite 850
Boston, MA 02108
(617) 482-3170
dmcfadden@aclum.org

Counsel for Plaintiff

CERTIFICATE OF SERVICE

I, Natalie F. Panariello, hereby certify that, on November 17, 2023, a true and accurate copy of the foregoing document was served by email on the following:

Samuel Furgang
samuel.furgang@mass.gov

/s/ Natalie F. Panariello
Natalie F. Panariello (BBO # 707579)