ALAN WILSON
ATTORNEY GENERAL

December 11, 2017

Ms. Marci Andino
Executive Director
State Election Commission
P.O. Box 5987
Columbia, SC 29250-5987

Dear Director Andino:

Attorney General Alan Wilson has referred your letter to the Opinions section. Your letter states the following:

> The S.C. State Election Commission (SEC) respectfully seeks an opinion as to the exclusion of "[i]nformation relating to security plans and devices" under the S.C Freedom of Information Act (FOIA) and, in particular, the scope and application of this exclusion as it pertains to cybersecurity matters.
>
> ...
>
> As a result of revelations about malicious cyber activity from foreign entities targeting states' election systems in the months leading up to the 2016 presidential election, as well as the subsequent designation of election infrastructure as critical infrastructure, the SEC and county boards have seen a significant increase in the number of FOIA requests for records containing the types of information described above. Such requests often encompass numerous records thousands of pages in length.
>
> As you are aware, the definition of "public record" for purposes of FOIA contains the following language relevant to this request:
>
> > Information relating to security plans and devices proposed, adopted, installed, or utilized by a public body, other than amounts expended for adoption, implementation, or installation of these plans and devices, is required to be closed to the public and is not considered to be made open to the public under the provisions of this act.

S.C. Code § 30-4-20(c) (emphasis added). This language was added to § 30-4-20(c) as part of Act 339 of 2002, the "South Carolina Homeland Security Act."

Our concern, however, is the lack of clarification or guidance – statutory, judicial, or otherwise – as to the meaning and scope of "[i]nformation relating to security plans and devices" as used in § 30-4-20(c). Much like "medical records" which are closed to the public by § 30-4-20(c), the phrase "security plans and devices" is not defined in the statute. The "medical records" exclusion, however, has been defined and discussed at length by the S.C. Supreme Court in Perry v. Bullock, 409 S.C. 137, 761 S.E.2d 251 (2014), as well as a 2016 opinion of your Office.

In the absence of any such binding or persuasive authority clarifying the meaning and scope "information relating to security plans and devices," or unless and until legislation can be enacted specifically addressing FOIA as it relates to such critical infrastructure cybersecurity information, the SEC finds itself in a difficult position when addressing requests for the types of records discussed herein. In the past, the SEC has erred on the side of transparency by producing such records while redacting specific information deemed by staff to be a security risk if released to the public. In light of the ever growing and increasingly sophisticated threats to the infrastructure of our election systems, the continued use of such a practice could inevitably result in the inadvertent disclosure of information which could be used to compromise the security of our election systems. The risk of inadvertent disclosures is magnified when consideration is given to, *inter alia*: the number and length of the records being redacted; the time, resources, and expertise required to analyze such information for redaction; and differences of opinion amongst different public bodies possessing identical records as to the redaction of specific information.

The above concerns have caused the SEC to question the practice of redacting records concerning the infrastructure and security of our election systems. The SEC now believes the security of our election infrastructure is best served by the exclusion or withholding of such records in their entirety. Considering the Supreme Court's analysis of § 30-4-20(c) in Bullock and Opinions since issued by your Office addressing the same, the SEC seeks an opinion as to whether such a practice is supported by the exclusion of "information relating to security plans and devices" pursuant to § 30-4-20(c).

Law/Analysis

It is this Office's opinion that a court likely would find that a public body may not release records related to its cybersecurity infrastructure in response to a S.C. Freedom of Information Act (S.C. FOIA) request. Under the S.C. FOIA, "A person has a right to inspect, copy, or receive an electronic transmission of any public record of a public body, except as otherwise provided by Section 30-4-40, or other state and federal laws, in accordance with reasonable rules concerning time and place of access...." 2017 Act No. 67, § 1 (amending S.C. Code Ann. § 30-4-30). "Public body" is statutorily defined, in part, to include "any department of the State, a majority of directors or their representatives of departments within the executive branch of state government as outlined in Section 1-30-10, any state board, commission, agency, and authority, any public or governmental body or political subdivision of the State..." S.C. Code Ann. § 30-4-20(a). This Office has previously opined that the SEC is a public body. Op. S.C. Atty. Gen., 2007 WL 1651329 (May 18, 2007); see also S.C. Code Ann. § 7-3-10 (creating the State Election Commission). The S.C. FOIA defines "public record" to include:

> [A]ll books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body. Records such as income tax returns, medical records, hospital medical staff reports, scholastic records, adoption records... and other records which by law are required to be closed to the public are not considered to be made open to the public under the provisions of this act.... Information relating to security plans and devices proposed, adopted, installed, or utilized by a public body, other than amounts expended for adoption, implementation, or installation of these plans and devices, is required to be closed to the public and is not considered to be made open to the public under the provisions of this act.

S.C. Code Ann. 30-4-20(c) (Supp. 2016) (emphasis added). The underlined portion of the "public record" definition was added by the "South Carolina Homeland Security Act," 2002 Act No. 399, § 17. In relevant part, the Act is titled as "AN ACT TO...AMEND SECTION 30-4-20, RELATING TO DEFINITIONS FOR PURPOSES OF THE FREEDOM OF INFORMATION ACT (FOI), SO AS TO PROVIDE THAT INFORMATION REGARDING THE SECURITY PLAN OF A PUBLIC BODY IS NOT OPEN TO THE PUBLIC." As noted in the request letter above, the meaning of "security plans" is not statutorily defined within the S.C. FOIA. Therefore, to determine whether the SEC's and county boards' cybersecurity infrastructure information is closed to the public as "information relating to security plans," we must examine the rules of statutory interpretation and the opinions or of our state courts.

Statutory interpretation of the South Carolina Code of Laws requires a determination of the General Assembly's intent. Mitchell v. City of Greenville, 411 S.C. 632, 634, 770 S.E.2d 391, 392 (2015) ("The cardinal rule of statutory interpretation is to ascertain and effectuate the legislative intent whenever possible."). Where a statute's language is plain and unambiguous,

"the text of a statute is considered the best evidence of the legislative intent or will." Hodges v. Rainey, 341 S.C. 79, 85, 533 S.E.2d 578, 581 (2000). "A statute as a whole must receive a practical, reasonable and fair interpretation consonant with the purpose, design, and policy of lawmakers." State v. Henkel, 413 S.C. 9, 14, 774 S.E.2d 458, 461 (2015), reh'g denied (Aug. 5, 2015).

In Perry v. Bullock, 409 S.C. 137, 761 S.E.2d 251 (2014), the South Carolina Supreme Court addressed a similar issue of statutory construction. The Court considered whether autopsy reports are considered "medical records" as used in the same S.C. FOIA definition of "public record." The Court analyzed the matter as follows:

> The FOIA requires public bodies to disclose public records upon request and defines public records as "all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body." S.C. Code Ann. § 30–4–20. However, "[r]ecords such as ... medical records ... and other records which by law are required to be closed to the public are not considered to be made open to the public under the provisions of [the FOIA].... " Id.
>
> The phrase "medical records" is not defined within the statute and therefore, we turn to its normal and customary meaning. See, e.g., Branch v. City of Myrtle Beach, 340 S.C. 405, 409–10, 532 S.E.2d 289, 292 (2000) ("When faced with an undefined statutory term, the Court must interpret the term in accord with its usual and customary meaning."). Merriam–Webster defines a medical record as "a record of a patient's medical information (as medical history, care or treatments received, test results, diagnoses, and medications taken)." Merriam–Webster Online, http://www.merriam-webster.com/medical/medical%20records. Thus, plainly stated, medical records are those records containing medical information.
>
> We find autopsy reports fit neatly within that general understanding of medical records. Section 17–5–5(1) of the South Carolina Code (2014) defines an autopsy as "the dissection of a dead body and the removal and examination of bone, tissue, organs, and foreign objects for the purpose of determining the cause of death and manner of death." Although the objective of an autopsy is to determine the cause of death, as the statute indicates, the actual examination is comprehensive. Thus, the medical information gained from the autopsy and indicated in the report is not confined to how the decedent died. Instead, an autopsy, which is performed by a medical doctor, is a thorough and invasive inquiry into the body of the decedent which reveals extensive medical information, such as the presence of any diseases or medications and any evidence of treatments received, regardless of whether that information pertained

> to the cause of death. Accordingly, we find an autopsy report falls within the definition of a medical record as that term is commonly understood.
>
> ...

409 S.C. at 141–42, 761 S.E.2d at 253. The Court held that autopsy reports are "excluded from disclosure under the FOIA as medical records." 409 S.C. at 144, 761 S.E.2d at 255.

As to the present question regarding the meaning of "security plans," we likewise examine its normal and customary meaning for guidance on interpreting the undefined term. Merriam–Webster defines **security** as:

"b (1): measures taken to guard against espionage or sabotage, crime, attack, or escape." Merriam–Webster Online, https://www.merriam-webster.com/dictionary/security; see also Dictionary.com, http://www.dictionary.com/browse/security ("precautions taken to guard against crime, attack, sabotage, espionage, etc."); The American Heritage Dictionary 1233 (3rd ed. 1993) (security defined as "measures adopted by a government to prevent espionage, sabotage, or attack.").

Further, Merriam–Webster defines **plan** as:

"2: a: a method for achieving an end; b: an often customary method of doing something: procedure; c: a detailed formulation of a program of action; d: goal, aim; 3: an orderly arrangement of parts of an overall design or objective; 4: a detailed program." Merriam–Webster Online, https://www.merriam-webster.com/dictionary/plan; see also Dictionary.com, http://www.dictionary.com/browse/plan?s=t ("a scheme or method of acting, doing, proceeding, making, etc., developed in advance"). When read in combination, these definitions suggest the Legislature likely intended for "information relating to security plans and devices" to mean the methods, procedures, and detailed formulations proposed, adopted, installed, or utilized to guard against espionage or sabotage, crime, attack, or escape.

Next, we examine the normal and customary meaning of "cybersecurity" to determine whether it "fit[s] neatly within that general understanding" of information relating to security plans. Bullock, supra. Merriam–Webster defines cybersecurity as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack." Merriam–Webster Online, https://www.merriam-webster.com/dictionary/cybersecurity; see also Dictionary.com, http://www.dictionary.com/browse/cybersecurity?s=t ("precautions taken to guard against crime that involves the Internet, especially unauthorized access to computer systems and data connected to the Internet."). The normal and customary meaning of cybersecurity, as stated in the definitions above, includes the similar element of guarding against attack which is central to the normal and customary meaning of security plans. Additionally, Sections 9-12 of the South Carolina Homeland Security Act define "computer crime offenses," criminal penalties, civil remedies, as well as venue for such offenses. Included within the definitions in Section 9, "computer contaminant" lists "viruses", "worms", "Trojans", and

"Trojan Horses" as being commonly designed to "compromise computer security." While no specific link is made between the computer crime offenses in Sections 9-12 and the exclusion from the public record definition in the S.C. FOIA, it is a "fair interpretation consonant with the purpose, design, and policy" of the Legislature that "information relating to security plans" is meant to include information related to computer security or cybersecurity. State v. Henkel, supra. Therefore, it is this Office's opinion that cybersecurity infrastructure information is included within the broad set of information encompassed by "information relating to security plans."

We next address whether the SEC's proposed method of the exclusion or withholding of [cybersecurity infrastructure] records in their entirety is permissible under the S.C. FOIA. It is this Office's opinion that a court likely would find that the exclusion or withholding of cybersecurity infrastructure records in response to a S.C. FOIA request is consistent with the express terms of the act and legislative intent. As the South Carolina Supreme Court described in Beattie v. Aiken Dept. of Social Services, 319 S.C. 449, 462 S.E.2d 276 (1995), the right to inspect and copy records of a public body are limited in two distinct circumstances; when records are specifically exempted from the FOIA and when records are closed to the public by law. The Court explained as follows:

> FOIA provides the right to inspect or copy any public record of a public body. S.C. Code Ann. § 30–4–30(a) (Supp.1994). However, the FOIA enumerates certain exemptions, including information of a personal nature and work product of legal counsel. S.C. Code Ann. § 30–4–40(a)(2) and (a)(7) (1991 and Supp.1994). Moreover, those records which are required by law to be closed to the public are not subject to the FOIA. S.C. Code Ann. § 30–4–20(c) (1991); S.C. Code Ann. § 30–4–40(4) (1991). Notwithstanding, these exemptions for the FOIA do not provide a blanket prohibition of disclosure of the entire record containing exempt material. Rather, the exempt and nonexempt material shall be separated and the nonexempt material disclosed. See Newberry Publ. v. Newberry Co. Comm'n A.D.A., 308 S.C. 352, 417 S.E.2d 870 (1992).

319 S.C. at 453, 462 S.E.2d at 279 (emphasis added). The Bullock Court's holding that autopsy reports are included within the category of records which are closed to the public because they "are excluded from disclosure under the FOIA as medical records" would be equally applicable to cybersecurity infrastructure records as information relating to security plans. 409 S.C. at 144, 761 S.E.2d at 255. Both medical records and information relating to security plans are "closed to the public are not considered to be made open to the public under the provisions of this act." S.C. Code Ann. 30-4-20(c).[1] Indeed, this conclusion is further supported by the title of the "South

[1] See Op. S.C. Atty. Gen., 2016 WL 1167292, at 10 (February 24, 2016).

> In particular, while our prior opinions as well as Section 30-4-40 explain that public bodies may disclose public records fitting within the category of an exemption, because FOIA's applicability is limited to "public records" and, pursuant to our conclusion above, a toxicology report is a

Carolina Homeland Security Act" which, again, states the definition of "public record" was amended "TO PROVIDE THAT INFORMATION REGARDING THE SECURITY PLAN OF A PUBLIC BODY IS NOT OPEN TO THE PUBLIC." 2002 Act No. 399. Therefore, it is this Office's opinion that records which relate to a public body's cybersecurity infrastructure are not subject to disclosure under the S.C. FOIA as a public record.

Please note however, that the "amounts expended for adoption, implementation, or installation of these plans and devices" related to cybersecurity infrastructure, as information relating to a security plan, are not specifically closed to public disclosure. A public body should treat a request for such information as a public record.

Conclusion

It is this Office's opinion that a court likely would find that a public body may not release records related to its cybersecurity infrastructure in response to a S.C. Freedom of Information Act (S.C. FOIA) request. Under the S.C. FOIA, "A person has a right to inspect, copy, or receive an electronic transmission of any public record of a public body, except as otherwise provided by Section 30-4-40, or other state and federal laws, in accordance with reasonable rules concerning time and place of access...." 2017 Act No. 67, § 1 (amending S.C. Code Ann. § 30-4-30). However, the "South Carolina Homeland Security Act," 2002 Act No. 399, § 17, amended the statutory definition of "public record" to read, in relevant part, "information relating to security plans and devices... is required to be closed to the public and is not considered to be made open to the public under the provisions of this act." While the term "security plans" is not statutorily defined, it is this Office's opinion that a court would likely find the common and ordinary meaning of information relating to security plans, discussed above, includes information pertaining to cybersecurity infrastructure. The South Carolina Supreme Court's analysis in Beattie v. Aiken Dept. of Social Services, 319 S.C. 449, 462 S.E.2d 276 (1995) and Perry v. Bullock, 409 S.C. 137, 761 S.E.2d 251 (2014) suggests that cybersecurity

---

"medical record" and therefore closed for purposes of FOIA, it appears FOIA, because it applies only to "public records" was not intended to protect a public body should it release a closed record. In other words, because we believe a toxicology report is a closed record as opposed to a public record subject to Section 30-4-40's disclosure exemptions, FOIA's protections permitting the disclosure of an exempt record do not apply to the disclosure of a closed record.

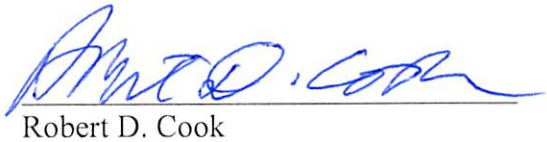
As detailed above, "analysis of the FOIA's application turns on whether the information requested (1) is held by an entity that classifies as a 'public body'; (2) falls under the definition of a 'public record'; and (3) is not exempt from disclosure." Op. S.C. Att'y Gen., 2014 WL 7210767 (December 4, 2014). This is important because, in the words of our Supreme Court, "records which are required by law to be closed to the public are not subject to the FOIA." Beattie v. Aiken County Dept. of Social Servs., 319 S.C. 449, 453, 462 S.E.2d 276, 279 (1995) (emphasis added). Thus, both this Office, as well as our Supreme Court, clearly recognize the distinction between closed records and public records which are exempt from disclosure pursuant to the terms of Section 30-4-40.

infrastructure records, as information relating to security plans, would be regarded as closed records. See also Op. S.C. Atty. Gen., 2016 WL 1167292 (February 24, 2016) (discussing distinction between exemptions from disclosure of public records in S.C. Code Ann. § 30-4-40 and records closed to the public which are not subject to the FOIA). In light of the S.C. FOIA's mandate of liberal construction in favor of disclosure, this Office has consistently advised public bodies concerning the applicability of Section 30-4-40 exemptions to disclosure, "when in doubt, disclose ..." Op. S.C. Atty. Gen., 2015 WL 4699336 (July 27, 2015). However, when a record is required by law to be closed to the public, there is no doubt that a public body cannot disclose such a record under the S.C. FOIA. Therefore, it is this Office's opinion that a court likely would find that the exclusion or withholding of cybersecurity infrastructure records in response to a S.C. FOIA request is consistent with the Act.

Sincerely,

Matthew Houck
Assistant Attorney General

REVIEWED AND APPROVED BY:



Robert D. Cook
Solicitor General