



ALAN WILSON
ATTORNEY GENERAL

July 26, 2023

Mr. Bryan P. Stirling, Director
South Carolina Department of Corrections
P.O. Box 21787
Columbia, SC 29221-1787

Dear Director Stirling:

You seek an opinion regarding “whether the South Carolina Department of Corrections (“SCDC”) is required to release, pursuant to the Freedom of Information Act (“FOIA”), photographs of inmates taken automatically while they are using their SCDC tablets.” As background information, you provide the following:

. . . eligible inmates in SCDC are now assigned tablets to use for making monitored telephone calls to their families, taking classes, reading books, subscribing to pre-approved programming, receiving messages from the institution, and other approved activities. Each inmate is assigned a Personal Identification Number (“PIN”) for tablet login, which controls their level of tablet applications. However, inmates have been known to pass off their PINs to other inmates, often resulting in criminal activity. This is prohibited by policy and is punishable as a disciplinary offense. In an effort to deter inmates from violating policy and allowing others to use their PINs, the tablets automatically take a photograph of an inmate when he or she logs on to the tablet. The tablet also takes periodic photographs of the inmate as the inmate continues to use the tablet. If a question later arises about an inmate using another inmate's PIN, SCDC staff can look up the photographs taken by the tablet at the relevant time to determine who was actually using the tablet.

SCDC has received FOIA requests for inmate tablet session records, which are generally available under FOIA. Recently, SCDC released inmate photographs along with the inmate tablet session records. After further review, SCDC now believes that although the inmate tablet session records themselves are subject to release under FOIA, the inmate photographs are not subject to release. South Carolina's FOIA enumerates several matters which are exempt from disclosure pursuant to the Act or are excluded from the Act's definition of a public record. One exclusion is under S.C. Code S.C. Code 30-4-20(c), which states that “[s]ecurity plans and devices are specifically excluded from the definition of the term ‘public record.’”

Mr. Bryan P. Stirling
Page 2
July 26, 2023

Since the inmate photographs are taken specifically for the purpose of allowing SCDC to maintain security by ensuring that inmates do not circumvent tablet access suspensions or restrictions by using another inmate's PIN, SCDC believes that the inmate photographs qualify as security plans or devices that are excluded from the definition of a public record and therefore not subject to release under FOIA. I would appreciate your opinion on whether this interpretation is correct.

Law/Analysis

As we recognized in a recent opinion, South Carolina's Freedom of Information Act was designed to require openness in government. In that opinion, dated May 14, 2021, we emphasized the following:

A. South Carolina Freedom of Information Act

South Carolina's "Freedom of Information Act requires a public body to disclose public records that are not exempt pursuant to the Act." Op. Att'y Gen., 2014WL 7210767 (S.C.A.G. Dec. 4, 2014). The preamble to the South Carolina Freedom of Information Act ("FOIA") states:

The General Assembly finds that it is vital in a democratic society that public business be performed in an open and public manner so that citizens shall be advised of the performance of public officials and of the decisions that are reached in public activity and in the formulation of public policy. Toward this end, provisions of this chapter must be construed so as to make it possible for citizens, or their representatives, to learn and report fully the activities of their public officials at a minimum cost or delay to the persons seeking access to public documents or meetings.

S.C. Code Ann. § 30-4-15 (2007). As our Court of Appeals remarked in Campbell v. Marion County Hospital District, 354 S.C. 274, 280, 580 S.E.2d 163, 166 (Ct. App. 2003), "[t]he essential purpose of the FOIA is to protect the public from secret government activity." The Supreme Court, in New York Times Co. v. Spartanburg Cty. Sch. Dist. No. 7, 374 S.C. 307, 311, 649 S.E.2d 28, 30 (2007), explained:

FOIA is remedial in nature and should be liberally construed to carry out the purpose mandated by the legislature. Quality Towing, Inc. v. City of Myrtle Beach, 345 S.C. 156, 161, 547 S.E.2d 862, 864-865 (2001). FOIA must be construed so as to make it possible for citizens to learn and report fully the activities of public officials. S.C. Code Ann. § 30-4-15 (Supp.2007).

As such, FOIA must be liberally construed to carry out its broad purpose. Also, the exceptions to disclosure must be narrowly interpreted. Op. Att'y Gen., 2006 WL 1574910 (S.C.A.G. May 19, 2006). Consistent with these principles, we have repeatedly advised, when in doubt, an agency should disclose. Op. Att'y Gen., 2017

Mr. Bryan P. Stirling
Page 3
July 26, 2023

WL 1368244 (S.C.A.G. Apr. 15, 2017). Thus, all doubt must be resolved in favor of transparency.

Pursuant to FOIA, “[a] person has a right to inspect, copy, or receive an electronic transmission of any public record of a public body,” unless it is exempt pursuant to section 30-4-40 of the South Carolina Code (2007 & Supp. 2020). S.C. Code Ann. § 30-4-30(A)(1) (Supp. 2020). Section 30-4-20(a) (2007) provides a “public body” includes “any department of the State.” Because the Department of Corrections (the “Department”) is a department of the State, it is a public body for purposes of FOIA. See also Op. Att’y Gen., 1979 WL 43200 (S.C.A.G. Dec. 6, 1979) (applying FOIA to the Department).

As a public body, the Department must thus comply with requests for public records under FOIA. “Public records” include “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(c) (2007). Pursuant to section 24-9-35 of the South Carolina Code (Supp. 2020), the Jail and Prison Inspection Division of the Department of Corrections is required to retain a permanent record of deaths and the circumstances surrounding such deaths of persons incarcerated or in the custody of a municipal, county, multijurisdictional jail, county prison camp, or state correctional facility. Accordingly, we believe a list of the inmates who have died in custody and their causes of death is likely something the Department would possess or maintain for purposes of FOIA. Further, in requiring such records be kept or maintained, the Legislature could easily have required they be confidential or not open to disclosure. Yet, even though section 24-9-35 has been amended on several occasions, the Legislature did not expressly require such records be confidential.

Section 30-4-20(c) lists records that are not open to the public pursuant to FOIA, including “[r]ecords such as ... medical records ... and other records which by law are required to be closed to the public” We understand from your letter you are particularly concerned as to whether information pertaining to inmate deaths is a medical record which would be closed to the public. Our Supreme Court addressed the medical record exemption under FOIA in Society of Professional Journalists v. Sexton, 283 S.C. 563, 566, 324 S.E.2d 313, 314 (1984), finding: “It is true that death certificates contain a medical certification of the cause of death. However, they are not medical records in the normal sense but are statements of conclusion by persons required by law to make such findings after the death of a citizen of the state.”

In Perry v. Bullock, 409 S.C. 13 7, 761 S.E.2d 251 (2014), the Court considered whether an autopsy report is a medical record exempt from disclosure pursuant to FOIA. Id. Finding FOIA did not define “medical record,” the Court followed the rules of statutory interpretation and turned to the normal and customary meaning of the term. The Court stated: “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.” Id. at 141, 761 S.E.2d at 253. The Court determined an autopsy report falls within the definition of a medical record, reasoning

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.

Id. at 142, 761 S.E.2d at 253 (emphasis added).

The Court in Perry differentiated between autopsy reports and death certificates, which it previously ruled are not medical records “simply because they contain medical information.” Id. at 143, 761 S.E.2d at 254 (citing to Society of Professional Journalists, 283 S.C. at 563, 324 S.E.2d at 313). The Court explained:

A death certificate includes no more than the cause of death, if known. In contrast an autopsy is a comprehensive medical examination of a body designed to reveal not only the cause of death, but also the decedent's general medical condition at the time of death including information unrelated to the cause of death. This is the type of information that would necessarily be contained in medical records when a person is alive. We decline to allow a person's death to change the nature of the record into one subject to disclosure under the FOIA.

Id.

Op. S.C. Att’y Gen., 2021 WL 2181992 (May 14, 2021). Thus, absent a clear exclusion or exception, SCDC must “when in doubt, disclose” pursuant to FOIA.

Your specific question deals with that portion of § 30-4-20(c) which provides that “[i]nformation relating to “security plans and devices” are not “public records” under FOIA. Such provision states that “[i]nformation 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.” This form of exclusion differs from exemptions under FOIA (§ 30-4-40) in that an exclusion under § 30-4-20(c) is mandatory. SCDC deems inmate tablet photographs as subject to § 30-4-20(c) and the means for maintaining security by “ensuring that inmates do not circumvent tablet access suspensions or restrictions by using another inmate’s PIN. . . .” We believe a court would likely defer to SCDC’s judgment and rationale inasmuch as security measures to ensure that inmates do not circumvent prison rules and regulations are generally upheld.

In Op. S.C. Att’y Gen., 2017 WL 6548004 (Dec. 11, 2017), we addressed the “security plans and devices” exclusion required by § 30-4-20(c). There, it was noted that the language “was added to § 30-4-20(c) as part of Act 339 of 2002, the ‘South Carolina Homeland Security Act.’” The question before us in that 2017 opinion was the “scope and application of this exclusion [“security plans and devices”] as it pertains to cybersecurity matters.” We analyzed the issue as follows:

[a]s 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). [] Indeed, this conclusion is further supported by the title of the “South 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

Mr. Bryan P. Stirling
Page 7
July 26, 2023

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.

In addition, in Flaherty-Ortega v. Horry County, et al., 2021 WL 5495362 (D.S.C. 2021), the Magistrate Judge there addressed the issue of whether certain “‘photos and videos at issue contain clear depictions of the [Horry County] Detention Center itself, . . . and the transport van at issue’ and are protected from disclosure pursuant to South Carolina’s Freedom of Information Act (‘FOIA’) . . . and the South Carolina’s expungement statute, S.C. Code Ann. § 17-1-40.” The surveillance video and photos there “‘depict[ed] the inside of the Detention Center’s secure areas.’” The argument by the Horry County Sheriff’s Office was that the surveillance video and photos were not “‘public records’” pursuant to § 30-4-20(c).

According to the Magistrate Judge, these videos and photos were immune from release pursuant to the “‘common-sense protection these videos are provided by FOIA. . . .’” Id. at * 3. Likewise, photos and video of the transport van were not subject to release in accordance with § 30-4-20(c). In the words of the Magistrate,

Defendants are especially protective regarding information about the security devices and plans related to the transport of inmates as the transport process represents the most risk of inmate escapes, given that multiple inmates may be transported outside the secure perimeter of the Detention Center by only 1 or 2 officers. Just as the videos and photos of the inside of the secure areas of the Detention Center are not publicly available for the common-sense protection of the integrity of the security devices depicted within the Detention Center, so [too] is similar information regarding the secure areas of the transport vehicles used by HCSO officers. . . .

Id. at * 4.

Flaherty-Ortega rejected Plaintiff’s argument that “‘the limited video surveillance from the decedent’s unit . . . has no relation to ‘security plans and devices. . . .’” According to the Magistrate, “‘HCSO Defendants have sufficiently articulated safety concerns and statutory protections connected to this category of documents.’” (citing Dang by and through Dang v. Eslinger, 2015 WL 13655675) (“The details of how a jail’s video surveillance system operates is plainly information that is best kept confidential.”) See also Stahl v. Dept. of Justice, 2021 WL 1163154, at * 5-6 (E.D.N.Y. 2021) (finding that portions of videos documenting procedures for removing prisoners from their cells, including the types of gear and equipment employed are exempt from disclosure; “[d]isclosing this information would enable inmates to circumvent the procedures, threatening the BOP’s ability to perform them safely. . . .”).

As the United States Supreme Court has noted, judgments regarding prison security “are peculiarly within the province and professional expertise of corrections officials, and in the absence of substantial evidence in the record to indicate that the officials have exaggerated their

response to these considerations, courts should ordinarily defer to their expert judgment in such matters.” Pell v. Procunier, 417 U.S. 817, 827 (1974). While this Office strongly supports FOIA and openness in government, and will continue to do so, the issue of prison security is primarily one for prison officials and we do not question their exercise of judgment unless there is little or no support for such position. Based upon the information provided, we cannot so conclude.

Conclusion

As we determined in our 2017 opinion, referenced above, “[w]hile 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 . . . includes information pertaining to cybersecurity infrastructure.” Op. S.C. Att’y Gen., 2017 WL 6548004 (Dec. 11, 2017). Based upon the information provided, the materials in question fit this definition. Moreover, “. . . courts, as a general rule, do not intervene in matters of prison discipline, security, or safety, except in most extraordinary of circumstances.” Op. S.C. Att’y Gen., 1984 WL 159913, Op. No. 84-106 (August 28, 1984). The judicial branch usually deems security measures designed to prevent circumvention of rules and regulations governing prisons and correctional institutions as not subject to public disclosure.

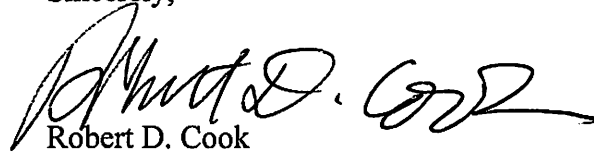
While this Office strongly supports FOIA and openness in government, the issue of prison security is primarily one for prison officials to determine, and we do not question their exercise of judgment unless there is no support for such position.

Here, the SCDC takes the position that “inmate photographs are taken specifically for the purpose of allowing SCDC to maintain security by ensuring that inmates do not circumvent tablet access suspensions or restrictions by using another inmate’s PIN. . . .” Thus, SCDC contends that “the inmate photographs qualify as security plans or devices that are excluded from the definition of a public record and therefore not subject to release under FOIA.”

Based upon our research, as set forth above, we believe a court would likely defer to SCDC’s judgment and uphold its conclusion that inmate photographs constitute “security plans or devices” for purposes of § 30-4-20(c). Moreover, another basis for this is that photographs of a prisoner in his or her prison cell could be deemed by a court to compromise prison security. See Flaherty-Ortega, supra [“Just as the videos and photos of the inside of the secure areas of the Detention Center are not publicly available for the common-sense protection of the integrity of the security devices depicted within the Detention Center, so [too] is similar information regarding the secure areas of the transport vehicles used by the HCSO officers. . . .”]. Inasmuch as our opinion cannot make factual findings, we accept SCDC’s position as governing. Accordingly, based upon the information presented, we believe a court would likely uphold SCDC’s position that § 30-4-20(c) deems the material in question not to be a “public record.”

Mr. Bryan P. Stirling
Page 9
July 26, 2023

Sincerely,

A handwritten signature in black ink, appearing to read "Robert D. Cook". The signature is fluid and cursive, with a large initial "R" and a long, sweeping tail.

Robert D. Cook
Solicitor General