Meeting Summary

Virginia Freedom of Information Advisory Council

Phishing Study Subcommittee

October 8, 2019, at 1:00 p.m.

Pocahontas Building, House Committee Room 400A

foiacouncil.dls.virginia.gov

The Phishing Study Subcommittee (the Subcommittee) of the Virginia Freedom of Information Advisory Council (the Council) met in Richmond.[1] The meeting began with introductions and opening remarks followed by presentations and discussion. Materials presented at the meeting are accessible through the *Council's subcommittee meetings webpage*.

Presentation and Public Comment: FOIA Charges – Tolling Issue

Council Staff

Staff presented three draft bills regarding FOIA charges and the tolling issue. The first draft (LD 20100544) contains language that mimics the advanced deposit language in subsection H of § 2.2-3704, but changes "advanced deposit" to "cost estimate." It also gives a requester 30 days after the cost estimate is sent to respond to the public body before the request is deemed to be withdrawn. The second draft (LD 20100545) is almost identical to the first, except that the time period shall be tolled for the amount of time that elapses between notice of the cost estimate and *receipt of payment* from the requester. The first draft focused on receiving a *response* from the requester. The final draft (LD 20100558) is identical to the second but also clarifies later in the bill that in regard to advance deposits when an estimate exceeds $200, actual payment is required versus just the requester's agreement to pay.

During the period for public comment, it was expressed that there are concerns about "receipt of payment" being the necessary response to start the clock again on a request because companies or the media may not be able to arrange payment within the necessary 30-day period before a request is deemed withdrawn. Subcommittee member Sterling Rives III noted that from a local government perspective, he has not seen that as an issue for entities, and as such, he is in favor of the third draft bill (LD 20100558). A representative from the Department of Education noted that actually receiving payment from a request ahead of time is beneficial because the Department tends to spend a lot of time on requests for which requesters do not pay after receiving the invoice. Mr. Rives pointed out that taxpayer dollars are utilized to make sure requests are properly filled, and he made a motion to recommend LD 20100558 to the full Council. The motion was properly seconded and received unanimous consent.

[1] **Members Present:** Sandra Treadway (Chair), Lee Bujakowski, Shawri King-Casey, Sterling Rives, III, Mark Vucci

Members Absent: None

Presentation, Discussion, and Public Comment: House Joint Resolution 628 (Heretick)

Daniel Jones, Chief Information Officer, City of Portsmouth

Mr. Jones presented to the Subcommittee key points from the memo written by Portsmouth City Attorney Solomon Ashby. He noted that there is a limit to what they are trying to "keep a cap on" when it comes to protecting private data.

Members of the Subcommittee started the conversation by discussing the three major areas listed in the memo presented by Megan Rhyne of the Virginia Coalition for Open Government (VCOG) at the last subcommittee meeting. The first issue discussed was citizen personal contact information. Mr. Rives expressed that the name of a requester should be public but not their email address or cell phone number. He questioned whether there is public value in releasing personal information and whether it offsets the value to the citizen who contacts a public body. Subcommittee member Lee Bujakowski questioned whether agreeing not to disclose a requester's information would actually solve the issue of phishing. He noted that training seems to be more valuable and a better response rather than limiting the disclosure of information. Subcommittee Chair Shawri King-Casey expressed that citizens divulge personal information with the hopes of getting assistance from a public body and they often are not aware that their personal information is subject to disclosure. She noted that maybe the larger issue is whether the government has a duty to protect citizen's personal information. Dr. Sandra Treadway, another Subcommittee member, asked for confirmation on whether citizens can opt out of having their personal information shared. Mr. Rives and Mrs. King-Casey affirmed but clarified that it only applies when personal contact information is furnished to a public body for the purpose of receiving electronic mail from the public body and only if the electronic mail recipient requests that the public body not disclose such information. Subcommittee member Mark Vucci commented that this issue seems to be largely outside of the scope of HJ 628 as drafted.

Members of the public then discussed the release of personal contact information. Mr. Jones said the government is a repository for citizen information, but if that information is released, it opens citizens up to being the targets of scams or phishing attacks. He also noted that, in regard to cybersecurity concerns, training only helps after a request is made, and no amount of training will protect against every attack. Joshua Heslinga, the Legal Compliance Manager at the Virginia Information Technologies Agency (VITA), mentioned that it is up to the legislators to decide what information is ultimately protected. He also said it could be burdensome if multiple categories of information become exempt as well as if an exemption depends on the context of each individual record. Ms. Rhyne stated that contact information has never been private and there is a burden involved in trying to protect that information. Mr. Vucci noted that it will be difficult to craft an objective rule to decide what information should be protected from disclosure and that this issue is outside of the scope of the larger issue of phishing. Mr. Bujakowski agreed with Mr. Vucci and said the public's interest in knowledge is more valuable than protecting citizen contact information. Mr. Rives suggested an addition to the list of discretionary exemptions for personal contact information to give a public body the ability to protect that information. He also said it would be helpful for the full Council to hear some of the stated concerns.

Next, the Subcommittee discussed government employee work and non-work contact information. Mr. Rives said the ability of a requester to gain access to all of an employee's work contact information makes it easier for a bad actor to initiate a phishing scam. He noted that the publication of direct emails and phone numbers for government employees can also be

counterproductive because the public often needs to be redirected to the appropriate party or entity. During the period for public comment, Mr. Jones said Portsmouth receives FOIA requests for employee directory information often, including requests for employee cell phone numbers. It was discussed whether cell phone numbers are a public record if an employee uses their phone for business purposes. Staff noted that it depends on whether the public body pays for the cell phone bill and keeps records of the bill; in that case, any information included on the bill would be public information.

Members of the Subcommittee questioned what can actually be done to combat the issue of phishing. Mr. Jones suggested implementing a requirement that a requester provide a state-issued identification card if they are asking for a large body of information. Staff informed the Subcommittee members that currently the law allows for a public body to require a requester's name and legal address, but it does not require a requester to furnish a state-issued identification card. Mr. Rives suggested that there is some value in authorizing public bodies to maintain a purely internal employee directory that is not subject to disclosure under FOIA, but he said that such a provision would not prohibit an individual employee from giving out their direct email or phone line information to a citizen. Ms. Rhyne contended that while it may be inconvenient to get direct calls and emails from the public, that is simply how the public contacts the government, and if that contact information is available, it should be disclosed. Mr. Jones questioned the purpose of mandatory disclosure of directory information and asked what the public body's liability is once that information is released and potentially used for nefarious purposes.

Members of the Subcommittee then discussed a public body's potential liability and settled on the opinion that a public body is likely only to be held liable in cases of gross negligence. Mrs. King-Casey asked for the representative from the Virginia State Police (VSP) to speak briefly to the issue. The representative added that it becomes an issue when you look at the aggregate data that is requested, as some basic information gives a bad actor the first step to initiate a phishing attack. He recommended that the Subcommittee develop a definition of personally identifiable information and implement a permissive exemption over certain pieces of data that are found in employee directory lists. By having a specific definition, he argued that it would add a certain level of objectivity and make it easier for a public body to withhold the defined information from a public record. Mrs. King-Casey suggested that it may be a good idea to do some research on how other states approach this issue. Members of the Subcommittee agreed and directed staff to research the issue further to present at the first Subcommittee meeting next year.

Next Meeting

The Subcommittee will reconvene next year after the 2020 Session of the General Assembly adjourns. More detailed information will be posted on the *Council's website*.

For more information, see the *Council's website* or contact the Division of Legislative Services staff:

Alan Gernhardt, Executive Director, Virginia Freedom of Information Advisory Council, DLS
agernhardt@dls.virginia.gov
804-698-1877

Ashley Binns, Attorney, Virginia Freedom of Information Advisory Council, DLS
abinns@dls.virginia.gov
804-698-1812