



OFFICE OF THE ATTORNEY GENERAL  
STATE OF ILLINOIS

**KWAME RAOUL**  
ATTORNEY GENERAL

July 6, 2021

VIA ELECTRONIC MAIL  
Mr. Kirk Allen  
*Edgar County Watchdogs*  
P.O. Box 593  
Kansas, Illinois 61933  
kirk@illinoisleaks.com

RE: Freedom of Information Act Request (078)

Dear Mr. Allen:

Thank you for writing to the Office of the Illinois Attorney General with your request for information pursuant to the Freedom of Information Act (FOIA) (5 ILCS 140/1 *et seq.* (West 2018)).

In an e-mail received on June 21, 2021, you requested the following:

1. A copy of any ransom notice or demand received in relation to the hacking of the Attorney General's computer files and website.
2. A copy of any request for a criminal investigation into the computer hacking of the Attorney General's computer files and website.
3. A copy of any communications with entities claiming responsibility for the computer hacking of the Attorney General's computer system.

On June 28, 2021, we advised that this office had conducted a search of its records, and we located no records responsive to part 2 of your request, which seeks a copy of any request for a criminal investigation into the computer hacking of the Attorney General's computer files and website.

Kirk Allen  
July 6, 2021  
Page 2

In the same response, we extended the time to respond to parts 1 and 3 of your request by five business days pursuant to sections 3(e)(i) and 3(e)(v) of FOIA (5 ILCS 140/3(e)(i), (v) (West 2019 Supp.)), because the requested records were stored at other locations than the office having charge of the requested records, and the records required further examination to determine if they were exempt from disclosure or should be released with appropriate redactions. This office has now completed its review.

Please be advised that we have located records that are responsive to Parts 1 and 3 of your request. However, your request is denied. Some of the information contained in the records is being withheld pursuant to section 7(1)(d)(i) of FOIA. 5 ILCS 140/7(1)(d)(i) (West 2019 Supp.). Section 7(1)(d)(i) of FOIA exempts from disclosure "[r]ecords in the possession of any law enforcement \* \* \* agency for law enforcement purposes \* \* \* to the extent that disclosure would unavoidably \* \* \* interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement \* \* \* agency that is the recipient of the request." The records that we have determined are exempt under this section include the ransom note and information contained in our communications with the suspected perpetrators that relates to an ongoing criminal investigation and reasonably contemplated law enforcement proceedings of this office. Accordingly, the responsive records are exempt from disclosure under section 7(1)(d)(i).

In addition, we have withheld information pursuant to section 7(1)(d)(v) of FOIA. 5 ILCS 140/7(1)(d)(v) (West 2019 Supp.). Section 7(1)(d)(v) of FOIA exempts from disclosure "unique or specialized investigative techniques other than those generally used and known \* \* \* and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request[.]" The information that we have determined is exempt under this section relates to specialized investigative techniques used in on-line discussions with the suspected perpetrators of the ransomware incident of which this office was a victim and which if made public would subject this office to additional ransomware attempts or other opportunities for a compromised computer network. Accordingly, the responsive records are exempt from disclosure under section 7(1)(d)(v).

We have also withheld information pursuant to section 7(1)(o) of FOIA. 5 ILCS 140/7(1)(o) (West 2019 Supp.). Section 7(1)(o) of FOIA exempts from disclosure "[a]dministrative or technical information associated with automated data processing operations, including but not limited to software, operating protocols, \* \* \* documentation pertaining to all logical and physical design of computerized systems, \* \* \* and any other information that, if disclosed, would jeopardize the security of the system or its data[.]" The information that we have determined is exempt under this section relates to the security of this office's network including information related to the scope of the attack and the measures taken to mitigate the harm. Accordingly, the responsive records are exempt from disclosure under section 7(1)(o).

Kirk Allen  
July 6, 2021  
Page 3

Additionally, we have withheld information pursuant to section 7(1)(v) of FOIA. 5 ILCS 140/7(1)(v) (West 2019 Supp.). Section 7(1)(v) of FOIA exempts from disclosure "[v]ulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but only to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public." Additionally, section 7(1)(v) specifies that "[i]nformation exempt under [section 7(1)(v)] may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations." The information that we have determined is exempt under this section relates to this office's response to a ransomware attack and measures taken to mitigate harm from a ransomware attack, the release of which could reasonably be expected to jeopardize the effectiveness of this office's security measures to prevent additional ransomware attempts or other opportunities for a compromised computer network. *See also Chicago Sun-Times v. Chicago Transit Authority*, 2021 IL App (1st) 192028, ¶44. Accordingly, the responsive records are exempt from disclosure under section 7(1)(v).

We have also withheld information pursuant to section 7(1)(kk) of FOIA. 5 ILCS 140/7(1)(kk) (West 2019 Supp.). Section 7(1)(kk) of FOIA exempts from disclosure "[t]he public body's credit card numbers, debit card numbers, bank account numbers, Federal Employer Identification Number, security code numbers, passwords, and similar account information[.]" Specifically, we have withheld information containing a unique security key or security code number of this office used to encrypt messages.

Similarly, we have withheld records containing a unique identifier as "private information," as that term is defined in section 2(c-5) of FOIA (5 ILCS 140/2(c-5) (West 2018)). "Private information" is exempt from disclosure under section 7(1)(b) of FOIA. 5 ILCS 140/7(1)(b) (West 2019 Supp.). Specifically, we have withheld information containing a unique security key or security code number of this office used to encrypt messages.

The persons responsible for this denial are Brent Stratton, Chief Deputy Attorney General, Matthew VanHise, Chief Privacy Officer, and the undersigned. You have a right to have the denial of your request reviewed by the Public Access Counselor (PAC) at the Office of the Illinois Attorney General. 5 ILCS 140/9.5(a) (West 2018). You may file your request for review with the PAC by writing to:

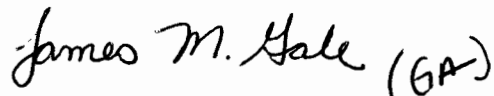
Kirk Allen  
July 6, 2021  
Page 4

Sarah Pratt  
Public Access Counselor  
Office of the Illinois Attorney General  
500 South 2nd Street  
Springfield, Illinois 62701  
Fax: (217) 782-1396  
publicaccess@atg.state.il.us

If you choose to file a request for review with the PAC, you must do so within 60 calendar days of the date of this denial letter. 5 ILCS 140/9.5(a) (West 2018). Please note that you must include a copy of your original FOIA request and of this denial letter when filing a request for review with the PAC.

You also have the right to judicial review of your denial by filing suit in the appropriate Illinois court. 5 ILCS 140/11 (West 2018).

Very truly yours,



JAMES M. GALE  
Assistant Attorney General

JMG:ga

cc: Annie Thompson, Senior Press Secretary  
Office of the Illinois Attorney General

Tori Joseph, Deputy Press Secretary  
Office of the Illinois Attorney General