pennsylvania
OFFICE OF OPEN RECORDS

FINAL DETERMINATION

IN THE MATTER OF	:	
	:	
LINDA SHECKLER,	:	
Requester	:	
	:	
v.	:	**Docket No: AP 2022-0492**
	:	
PENNSYLVANIA DEPARTMENT OF STATE,	:	
Respondent	:	

INTRODUCTION

Linda Sheckler ("Requester") submitted a request ("Request") to the Pennsylvania Department of State ("Department") pursuant to the Right-to-Know Law ("RTKL"), 65 P.S. §§ 67.101 *et seq*., seeking a copy of the Department's Statewide Uniform Registry of Electors ("SURE") Applications User Guide. The Department denied the Request, asserting that the responsive record was exempt under several of the RTKL's security-related exemptions. The Requester appealed to the Office of Open Records ("OOR"). For the reasons set forth in this Final Determination, the appeal is **denied**, and the Department is not required to take any further action.

FACTUAL BACKGROUND

On January 20, 2022, the Request was filed, seeking "a copy of the [Department's SURE] Applications Users Guide, dated January 2021 ("User Guide")." After invoking an extension of time to respond, 65 P.S. § 67.902(b), the Department, on February 15, 2022, denied the Request,

arguing that the User Guide is exempt from public disclosure under various sections of the RTKL, specifically Section 708(b)(2), the public safety exemption, Section 708(b)(3), pertaining to infrastructure security, and Section 708(b)(4), pertaining to computer security. 65 P.S. §§ 67.708(b)(2), (3), and (4). Among other things, the Department argues that disclosure of the User Guide would create a security risk and jeopardize the security of election infrastructure, including the SURE system itself.

On February 22, 2022, the Requester appealed to the OOR, challenging the denial and stating grounds for disclosure.[1] The appeal included a one-page excerpt from the January 2021 User Guide. The OOR invited both parties to supplement the record and directed the Department to notify any third parties of their ability to participate in this appeal. 65 P.S. § 67.1101(c).

After being given a brief extension of time to file its submission, the Department, on March 18, 2022, submitted a position statement arguing that Sections 708(b)(2) and (3) of the RTKL exempt the responsive record from disclosure. The Department also contends that the User Guide contains personal identification information of voters, which is exempt under Section 708(b)(6) of the RTKL. In support of its position, the Department submitted the attestations, made under the penalty of perjury, from Janelle Hawthorne, the Department's Open Records Officer, Jonathon Marks, the Department's Deputy Secretary for Elections and Commissions, and Christopher Dressler, the Information Security Officer of the Governor's Office of Administration, Office of Information Technology (OIT), Employment, Banking and Revenue Delivery Center.

[1]The Requester granted the OOR an extension to issue a final determination. *See* 65 P.S. § 67.1101(b)(1) ("Unless the requester agrees otherwise, the appeals officer shall make a final determination which shall be mailed to the requester and the agency within 30 days of receipt of the appeal filed under subsection (a)").

On May 6, 2022, in response to an inquiry from the OOR for additional information, the Department provided a supplemental attestation from Mr. Marks to address the Department's control measures related to distribution of the User Guide.

LEGAL ANALYSIS

"The objective of the Right to Know Law ... is to empower citizens by affording them access to information concerning the activities of their government." *SWB Yankees L.L.C. v. Wintermantel*, 45 A.3d 1029, 1041 (Pa. 2012). Further, this important open-government law is "designed to promote access to official government information in order to prohibit secrets, scrutinize the actions of public officials and make public officials accountable for their actions." *Bowling v. Office of Open Records*, 990 A.2d 813, 824 (Pa. Commw. Ct. 2010), *aff'd* 75 A.3d 453 (Pa. 2013).

The OOR is authorized to hear appeals for all Commonwealth and local agencies. See 65 P.S. § 67.503(a). An appeals officer is required "to review all information filed relating to the request" and may consider testimony, evidence and documents that are reasonably probative and relevant to the matter at issue. 65 P.S. § 67.1102(a)(2). An appeals officer may conduct a hearing to resolve an appeal. The decision to hold a hearing is discretionary and non-appealable. *Id.* Here, neither party requested a hearing.

The Department is a Commonwealth agency subject to the RTKL that is required to disclose public records. 65 P.S. § 67.301. Records in the possession of a Commonwealth agency are presumed public unless exempt under the RTKL or other law or protected by a privilege, judicial order or decree. *See* 65 P.S. § 67.305. Upon receipt of a request, an agency is required to assess whether a record requested is within its possession, custody or control and respond within

five business days. 65 P.S. § 67.901. An agency bears the burden of proving the applicability of any cited exemptions. *See* 65 P.S. § 67.708(b).

Section 708 of the RTKL places the burden of proof on the public body to demonstrate that a record is exempt. In pertinent part, Section 708(a) states: "(1) The burden of proving that a record of a Commonwealth agency or local agency is exempt from public access shall be on the Commonwealth agency or local agency receiving a request by a preponderance of the evidence." 65 P.S. § 67.708(a)(1). Preponderance of the evidence has been defined as "such proof as leads the fact-finder … to find that the existence of a contested fact is more probable than its nonexistence." *Pa. State Troopers Ass'n v. Scolforo*, 18 A.3d 435, 439 (Pa. Commw. Ct. 2011) (quoting *Pa. Dep't of Transp. v. Agric. Lands Condemnation Approval Bd.*, 5 A.3d 821, 827 (Pa. Commw. Ct. 2010)).

The Department argues that the requested User Guide is exempt from disclosure under Sections 708(b)(3) and (4) of the RTKL. Section 708(b)(3) of the RTKL exempts the following from access:

> (3) [a] record, the disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of …infrastructure, facility or information storage system, which may include:
>
> > (i) documents or data relating to computer hardware, source files, software and system networks that could jeopardize computer security by exposing a vulnerability in preventing, protecting against, mitigating or responding to a terrorist act.
> >
> > (ii) lists of infrastructure, resources and significant special events, including those defined by the Federal Government in the National Infrastructure Protections, which are deemed critical due to their nature and which result from risk analysis; threat assessments; consequences assessments; antiterrorism protective measures and plans; counterterrorism measures and plans; and security and response needs assessments; and

> (iii) …infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including public utility systems, structural elements, technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage and gas systems.

65 P.S. §§ 67.708(b)(3)(i)-(iii). Meanwhile, Section 708(b)(4) of the RTKL exempts from disclosure, "a record regarding computer hardware, software and networks, including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security." 65 P.S. § 67.708(b)(4).

Our courts have held that "[a]n agency must offer more than speculation or conjecture to establish the [RTKL's] security-related exemptions...." *California Borough v. Rothey*, 185 A.3d 456, 468 (Pa. Commw. Ct. 2018) (internal citations omitted); *see also Mission Pa., LLC v. McKelvey*, 212 A.3d 119 (Pa. Commw. Ct. 2019) *aff'd in part*, 255 A.3d 385 (Pa. 2021). Moreover, to invoke such exemptions, the courts have also explained that an agency must show that "the disclosure of" the records -- rather than the records themselves -- would create a reasonable likelihood of the requisite harm. *See Mission Mission Pa., LLC*, 212 A.3d at 133-34.

In support of the Department's position, Mr. Marks, the Department's Deputy Secretary for Elections and Commissions, attests to the following:

> 1. I am employed by the [Department] of State as the Deputy Secretary for Elections and Commissions and have served in that position for 3 years. Prior to that, I served for nearly 8 years as Commissioner of the Bureau of Commissions, Elections, and Legislation in the Department. As part of my duties, I supervise the administration of the laws relating to voting systems. As such, I am familiar with the laws and regulations regarding voting systems certified for use within this Commonwealth. I also oversee the Department's Division of Election Security and Technology. As part of those duties, I supervise and manage the election security initiatives across the Commonwealth, voting system certification, and implementation and maintenance of technology related to [SURE]. The Department also works closely with the 67 county election boards and other stakeholders to develop and implement projects and procedures impacting election operations in the Commonwealth.

2. I have reviewed the [Request] that is the subject of this appeal...

3. The U.S. Department of Homeland Security (DHS) designated Election Infrastructure (EI) part of the nation's critical infrastructure as a subsector within the Government Facilities sector in January of 2017. Critical Infrastructure is defined in the Critical Infrastructures Protection Act of 2001, as "systems or assets … so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e). The Department's SURE system is a computer database system that is the repository for voter registration data and information within the Commonwealth.

4. As identified by DHS, EI includes but is not limited to:

- Voter registration databases and associated IT systems
- IT infrastructure and systems used to manage elections (such as the counting, auditing and displaying of election results, and post-election reporting to certify and validate results)
- Voting systems and associated infrastructure
- Storage facilities for election and voting system infrastructure
- Polling places, to include early voting locations

5. The [User Guide] contains information regarding the innerworkings of the SURE system and provides instruction as to how to properly process data within it. Though the Department and the Commonwealth's information security office have robust safeguards in place to prevent unauthorized access, disclosure of the [User Guide] would potentially allow a user to manipulate the data within the SURE system if they were able to obtain access to the system.

6. Specifically, the [User Guide] contains detailed instructions of how to work and operate within the SURE system. This [G]uide and other user guides are step-by-step training and reference guides, and they are provided only to users who have been duly authorized to have access to the SURE system.

7. As the Department's Deputy Secretary, I believe that if this record is released publicly, it would create a reasonable likelihood of endangering the safety and security of the SURE system and overall election-related computer security because exposure of this information would hamper the Department's efforts in mitigating a cyber-terrorist attack. The [User Guide] provides specific details and information on how the data within the SURE system is processed and how the system operates in general. Disclosure of this type of information would provide individuals a roadmap for how to circumvent the protections within the SURE system, thus leaving the data in the system vulnerable to manipulation if the system is hacked. Because the SURE system is intimately involved in the managing of the elections held within the Commonwealth, this type of exposure would put the entire election process in the Commonwealth in jeopardy and would severely hamper the

> Department's ability to keep the SURE system safe in the event of an attack by hackers. Further, because of the pervasive nature of the information contained throughout the [User Guide], redaction would not be possible.
>
> 8. The [User Guide] contains personal information of actual registered voters within the SURE system that are used as examples for instruction. This information consists of personal information such as, partial social security numbers, a person's date of birth, home address, personal email addresses and personal phone numbers. Absent an explicit statutory mandate to make some of this information available publicly, this information should not be disclosed due to the potential danger of misuse and the potential harm it could cause the individual if their personal information is released. Furthermore, because the [User Guide] provides a roadmap of how to gain access to this type of protected data within the system, if one were to gain access to the system, the personal information of all Pennsylvania voters would be vulnerable to hacking and misuse.

In addition to the foregoing testimony, the Department also offers the attestation of Mr. Dressler, an Information Security Officer for the Governor's Office of Administration, who affirms as follows:

> 2. Over the course of my 25+ year career with the Commonwealth I have had a role in cybersecurity for the last 17 years.
>
> 3. On March 3, 2022, I was provided [RTKL] appeal 2022-0492 along with the withheld record, the January 2021 [SURE Guide] for my review.
>
> 4. In my capacity as ISO, I am familiar with the record, and its subject matter, being requested.
>
> 5. [The Department] has responsibility to implement and maintain the [SURE].
>
> 6. The SURE system electronically stores information relating to voter registration within the Commonwealth in a computer system and database that is required to be extremely secure because it contains confidential personal identification information (PII) such as date of birth, home address, partial social security numbers, and driver's license numbers.
>
> 7. In addition, the SURE system is part of the nation's critical infrastructure. The U.S. Department of Homeland Security (DHS) designated voter registration databases such as SURE as Election Infrastructure (EI) and made it part of the nation's critical infrastructure as a subsector within the Government Facilities sector in January of 2017.

8. Due to the highly confidential nature of the information stored within the database and system, [the Department] uses various technology protection measures to block and/or prevent the unauthorized access of the database and system, including, but not limited to, bad actors who would access it for fraudulent or illegal purposes.

……

10. …The User Guide is a document that is almost 500 pages and it contains detailed information and step to step processes including screen shots that guides an authorized user to operate and navigate within the SURE system and process voter registration applications.

11. The User Guide provides insight into how the SURE system operates and sets forth step by step instructions on how the system can be used to process voter registration applications and includes screen shots of the system. Disclosure of the [Guide] would give individuals information that could be used to devise plans to circumvent the integrity and security measures of the system that is part of the U.S. Critical Infrastructure.

12. The User Guide if disclosed could be used, in whole or part, by a threat actor/attacker from a reconnaissance perspective to gain valuable information concerning the security and operation of U.S. Critical Infrastructure since the User Guide provides detailed information and insight into the Commonwealth's computer defense configuration, posture and controls, of which SURE is a vital component, placing the U.S. Critical Infrastructure and the Commonwealth's computer systems and database at risk.

13. Information and knowledge gained through the disclosure of the User Guide, in whole or part, as described above, could be used by bad actors to exploit the SURE system and database by exposing vulnerabilities within the Commonwealth's computer systems, as the User Guide details and provides screen shots on how to process information within the SURE system, which if exploited would compromise the U.S. Critical Infrastructure including the sensitive and protected information contained within the system and database.

14. In my informed professional opinion, which is based upon my extensive experience as an IT and cybersecurity professional, disclosure of [the Guide] would reasonably be likely to expose U.S. Critical Infrastructure, as defined by the Federal Government in the National Infrastructure Protection Plan, including the SURE system and database to misuse and fraud due to the ability to gain access to and manipulate the data within the SURE system and would undermine the integrity of the voter registration process while endangering the security of the information contained within the SURE system and the system itself.

> 15. Additionally, and in my informed professional opinion, this type of infrastructure record, if disclosed, would create a reasonable likelihood of endangering the safety of the SURE system by exposing the methods used in processing data within the SURE system which would lead to exposing how the system is actually configured and also what types of security protocols are in place when working within the system.
>
> 16. Based on my experience and review of the record, I have determined that the User Guide at issue in this appeal is a record regarding computer hardware, software and networks, including administrative or technical records whose disclosure would be reasonably likely to jeopardize computer security.

Under the RTKL, a statement made under the penalty of perjury may serve as sufficient evidentiary support. *See Sherry v. Radnor Twp. Sch. Dist.*, 20 A.3d 515, 520-21 (Pa. Commw. Ct. 2011); *Moore v. Office of Open Records*, 992 A.2d 907, 909 (Pa. Commw. Ct. 2010). In the absence of any evidence that the Department has acted in bad faith, "the averments in [the attestations] should be accepted as true." *McGowan v. Pa. Dep't of Envtl. Prot.*, 103 A.3d 374, 382-83 (Pa. Commw. Ct. 2014) (citing *Office of the Governor v. Scolforo*, 65 A.3d 1095, 1103 (Pa. Commw. Ct. 2013)).

Both Mr. Marks and Mr. Dressler identify the SURE system, to which the User Guide relates, as part of the national critical infrastructure. As election infrastructure, Mr. Marks indicates that the SURE system serves as a "repository for voter registration data and information" in Pennsylvania. The Department's evidence shows that the User Guide is a training or reference manual that contains step-by-step processes of how to operate the SURE system. According to Mr. Marks, disclosure of the User Guide would be reasonably likely to endanger the safety and security of the SURE system and related computer security because it would provide a "roadmap" for how to circumvent SURE system protections, which in turn would leave data in the system vulnerable to manipulation if hacked and jeopardize the electoral process in the Commonwealth. Disclosure of the User Guide, according to Mr. Marks, would also likely lessen the Department's ability to mitigate a cyber-attack should one occur and to keep the SURE system safe. Mr. Dressler

also affirms, among other things, that disclosure of the User Guide could endanger the safety of the SURE system by revealing methods of processing data which would expose how the system is configured and what types of security protocols are in place. According to Mr. Dressler, disclosure of the User Guide could expose the SURE system to fraud and misuse due to the ability to manipulate data in the system. If disclosed, Mr. Dressler states that the User Guide could be used "by a threat actor/attacker from a reconnaissance perspective to gain valuable information concerning the security and operation" of election infrastructure since the User Guide provides detailed information and insight into the Commonwealth's computer defense configuration, posture and controls, thus putting the Commonwealth's computer systems and database at risk.

The OOR has found the professional opinion of experts assessing the risks of security to be credible and will not substitute its judgment for that of those with far more familiarity with such issues. *See Ocasio v. Pa. Dep't of Corr.*, 183 A.3d 506, 2018 Pa. Commw. LEXIS 18 (Pa. Commw. Ct. 2018). Here, Mr. Marks has approximately eleven years as a professional in election matters, part of which includes experience with election security, and Mr. Dressler has been involved in cybersecurity, in various roles with the Commonwealth, for the past seventeen years. Combined, their attestations provide an adequate factual basis from which we can conclude that the Department has met its burden of proving, by preponderance of the evidence, that the User Guide is exempt from public access under Sections 708(b)(3) and (4) of the RTKL. *See* 65 P.S. § 67.708(a)(1).[2]

[2] *But compare Towne v. City of Philadelphia*, OOR Dkt. AP 2021-0443, 2021 PA O.O.R.D. LEXIS 503 (finding that the agency failed to meet its burden of proof under Sections 708(b)(3) and (4) of the RTKL because it failed to link the disclosure of instructions on how to use the SURE system to any particular risk or harm); *Churchwell v. Montgomery County*, OOR Dkt. AP 2021-1331, 2021 PA O.O.R.D. LEXIS 1383 (holding that the agency failed to meet its burden of proof to show that "copies of SURE operations manuals and other written guidance for staff" were exempt under Section 708(b)(3) of the RTKL and granting access to those records in accordance with the Election Code).

In her appeal, the Requester asserts that in order to be exempt from access, the User Guide would need to be a record maintained in connection with the military, homeland security, national defense, law enforcement or other public safety activity. However, the statutory language of Sections 708(b)(3) and (4) require no such relationship, and Section 708(b)(2) of the RTKL is not raised by the Department on appeal.

The Requester also implies that if the User Guide were exempt under the RTKL, then it would be categorized as classified or indicated as containing sensitive information. Nevertheless, there is no requirement that a record be identified as classified or sensitive in order for Sections 708(b)(3) or (4) of the RTKL to apply.

Next, the Requester questions how the User Guide's use and access is controlled by the Department. Such a question raises a valid point considering the record at issue is claimed to pose a security risk if disclosed. The Department's evidence, however, substantiates that the User Guide is "provided only to users who have been duly authorized to have access to the SURE system." The Department's regulations suggest that access to the SURE system is limited. *See* 4 Pa. Code § 183.4 ("[o]nly registrars or the designees of a commission may add, modify or delete information in the commission's registration records in the SURE system") and 4 Pa. Code § 183.9(b) ("[i]n addition to the training required in subsection (a), registrars and the employees and clerks of a commission who are responsible for voter registration may be required to complete additional training at other times and places as determined by the Department").

Furthermore, in his supplemental attestation, Mr. Marks verifies, under penalty of perjury, the following:

> 4. In response to the U.S. Department of Homeland Security (DHS) designation of Election Infrastructure (EI) as part of the nation's critical infrastructure in January of 2017 and because of the sensitive nature of sharing this type of information, on April 23, 2019, the Department adopted a Traffic Light Protocol

(TLP) similar to DHS and other federal agencies. The protocol requires all DOS employees to mark, handle and store all Election Infrastructure Information (EII) with a TLP designation. The TLP is a set of requirements, captured in four (4) color-coded designations, to ensure that sensitive information is only shared with appropriate stakeholders. The color-coding designation consists of four (4) colors, Red, Amber, Green and White. Information designated as TLP: RED may not be disclosed to any parties outside of a specific exchange or meeting; TLP: AMBER is of limited distribution; TLP: GREEN can be circulated within a business community; and TLP: WHITE may be distributed freely. Each of these colors and stamps requires different handling and treatment and is based upon the risk that unprotected disclosure of that piece of information could cause to our EI.

5. The policy requires any information that directly or indirectly contains or discusses the vulnerabilities or internal functioning of EI or EII, or which provides information concerning the election processes in any election district within the Commonwealth, shall be processed and handled by DOS employees, contractors, consultants, and others with access to EI using the TLP, including applying markings and using internal security measures in handling and sharing such information. EII shall be presumed TLP: RED unless expressly designated as one of the other categories. Any EII pre-dating this policy may be designated retroactively under the TLP protocol.

6. As previously stated, the [User Guide] contains information regarding the innerworkings of the SURE system and provides instruction as to how to properly process data within it and, as such, it would be designated as TLP: AMBER. Distribution of the [User Guide] is limited to only those individuals that have been duly authorized to have working access to the SURE system, specifically county election personnel, who are required to treat it as if they were employees of the Department and to adhere to the TLP policy when handling the User Guide. Distribution of the [User Guide] is very infrequent and only happens if an update to the SURE system requires it to be amended.

The Department's evidence verifies that county election personnel with access to the User Guide are required to treat the record as if they were employees of the Department and adhere to the Department's TLP policy when handling it. While the Department's TLP policy in and of itself does not supersede the requirements of the RTKL, the use of the policy and protocols related thereto show that the Department has taken affirmative steps to restrict disclosure of and use of the User Guide. Given those restrictions, along with the Department's foregoing evidence concerning the likelihood of resulting harm if the User Guide were disclosed to the public, the

Department has met its burden of proof in this matter. The limited disclosure of the User Guide to authorized individuals outside the Department is not significant enough, in this instance, to outweigh the potential security risks associated with disclosure of the User Guide to the public at large.

Lastly, the Requester seems to suggest that the Department can extract sensitive information in the User Guide and provide a redacted version of the record to her. Because the Department has proven that the User Guide is exempt under Sections 708(b)(3) and (4), however, it is not required to redact the record. 65 P.S. § 67.706 (Section 706 requires an agency to redact non-public information from a record that is a "public record").[3]

CONCLUSION

For the foregoing reasons, the appeal is **denied**, and the Department is not required to take any further action. This Final Determination is binding on all parties. Within thirty days of the mailing date of this Final Determination, any party may appeal to the Commonwealth Court. 65 P.S. § 67.1301(a). All parties must be served with notice of the appeal. The OOR also shall be served notice and have an opportunity to respond as per Section 1303 of the RTKL. 65 P.S. § 67.1303. However, as the quasi-judicial tribunal adjudicating this matter, the OOR is not a proper party to any appeal and should not be named as a party.[4] This Final Determination shall be placed on the OOR website at: http://openrecords.pa.gov.

[3] The Requester's appeal correspondence appears to seek additional information from the Department. However, to the extent that the Requester wishes to modify the Request underlying this appeal, such is impermissible. A requester may not modify, explain or expand a request on appeal. *See PSP v. Office of Open Records*, 995 A.2d 515, 516 (Pa. Commw. Ct. 2010); *Michak v. Pa. Dep't of Pub. Welfare*, 56 A.3d 925 (Pa. Commw. Ct. 2012) (holding that "where a requestor requests a specific type of record … the requestor may not, on appeal argue that an agency must instead disclose a different record in response to the request"). If the Requester wishes to submit a new RTKL request to the Department, such can and should be accomplished by the appropriate methods outside of this appeal proceeding.

[4] *Padgett v. Pa. State Police*, 73 A.3d 644, 648 n.5 (Pa. Commw. Ct. 2013).

FINAL DETERMINATION ISSUED AND MAILED: May 13, 2022

/s/ Angela Edris

_____
APPEALS OFFICER
ANGELA EDRIS, ESQ.

Sent via email to: Linda Sheckler;
Jason McMurry, Esq.;
Janelle Hawthorne, AORO