OKLAHOMA

Steven Harpe
Chief Operating Officer

April 28, 2022

Ms. Sarah Lane
Acting Executive Director
Address: 2132 NE 36th St., Oklahoma City, OK 73111
Phone: (405) 523-4000

VIA ELECTRONIC MAIL

Director Lane:

In a letter dated March 3, 2022, on behalf of the Oklahoma Department of Veteran Affairs (ODVA), Director Kintsel requested records from the Office of Management and Enterprise Services (OMES). The requested information and OMES' response is contained herein.

ODVA Request #1:

> *"beginning December 1, 2021 through the date of this request, all Remote Control and Remote Access logs for Symantec Endpoint Management or any other remote systems management tools used by OMES or any private contractors working for or on behalf of the State of Oklahoma, including but not limited to NTT Data Services, resulting from remote access attempts by any persons other than employees of the Oklahoma Department of Veterans Affairs on the mobile devices, computers, tablets, laptops, server systems, Microsoft SharePoint folders, cloud drive folders, including but not limited to OneDrive folders, and any other shared drive folders assigned to, used by or accessible to the employees of the Oklahoma Department of Veterans Affairs (ODVA) whose place of duty is the ODVA, Central Office, located at 2132 NE 36th Street, Oklahoma City, Oklahoma 73111, namely: Lisa Acevedo, Rob Arrington, Aaron Ashworth, Rekha Asuri, Ivan Barnes, Jennifer Bloomfield, Chad Clark, Kris Dillon, Denise Figueroa, Ismael Gloria, Shena Goforth, Kim Heaton (also known as Kimberly Heaton-Wilson), Cherri Higgs, Brandon Hinton, Kristyn Hinton, Daron Hoggatt, Eulean Hollis, Josh Houston, Joel Kintsel, Shawn Kirkland, Jason LaPierre, Sarah Lane, Cami McKinney, Keith Mercer, Brint Montgomery, Kimberly Norried, Melissa Nucci, Jennifer Reeves, Stephen Rudnick, Helen Sapp, Mark Scott, Amber Seay, Jennifer Shockley, Jen Stephens, Teresa Tyler, Boni Ulik, Camilo Ulloa, Clif Wallace, Leona Watson, Lisa White, Dashon Williams and Nisha Young;"*

OMES Response #1:

OMES ISD utilizes Bomgar remote control software, and NTT Data uses rescue My PC. Both remote control software requires the end-user to visit a management website and initiate the connection. While there are limited logs, performing a forensics review of the computers would provide a full report of access/access attempts. ODVA can elect to contract with an approved vendor to provide the forensics review or have OMES perform those services.

ODVA Request #2:

"beginning December 1, 2021 through the date of this request, all records or logs of OMES employees and contract personnel employed by private contractors working for or on behalf of the State of Oklahoma, including but not limited to NTT Data Services, supporting systems assigned to ODVA who have accessed the mobile devices, computers, tablets, laptops, server systems, Microsoft SharePoint folders, cloud drive folders, including but not limited to OneDrive folders, and any other shared drive folders assigned to, used by or accessible to the employees of ODVA whose place of duty is the ODVA, Central Office, located at 2132 NE 36th Street, Oklahoma City, Oklahoma 73111, for all the same employees previously named in paragraph one (1) above;"

OMES Response #2:

In order to be responsive to your request for all records or logs of OMES employees and contract personnel employed by private contractors working for or on behalf of the State of Oklahoma, including but not limited to NTT Data Services, supporting systems assigned to ODVA who have accessed the mobile devices, computers, tablets, laptops, server systems a forensics investigation is required to provide the responsive documents. ODVA is in possession of the devices, so the devices will need to be turned over to OMES or ODVA may contract with a vendor for the performance of those services.

ODVA Request #3:

"beginning December 1, 2021 through the date of this request, a list of all mobile devices, computers, tablets, laptops, server systems, Microsoft SharePoint folders, cloud drive folders, including but not limited to OneDrive folders, and any other shared drive folders assigned to, used by or accessible to the employees of ODVA whose place of duty is the ODVA, Central Office, located at 2132 NE 36th Street, Oklahoma City, Oklahoma 73111, for all the same employees previously named in paragraph one (1) above;"

OMES Response #3:

ODVA should have all mobile devices, computers, tablets, and laptops in their possession that are required to provide the responsive documents. The devices will need to be turned over to OMES for a forensic examination or ODVA may contract with a vendor for the performance of those services. The servers are located at the OMES Data Center, Microsoft Azure, or other OMES backup/disaster recovery facilities. The file path for all ODVA user formats will be exported to ODVA in a secure method.

Please reference folder "questions 3" list of shares/folder permission.

- **"All -Users-ODVA_2022-3-24.csv"**
- **"ODVA Sharepoint.xlsx"**
- **"ODVA Clinton File access.csv"**
- **"ODVA_Ardmore_Shared_Permissions.csv"**
- **"odva_Claremore_SHARED_PERMISSIONS.csv"**
- **"ODVA_Lawton_Shared_Permissions.csv"**
- **"odva_Norman_SHARED_PERMISSIONS.csv"**
- **"odva_OKC_SHARED_PERMISSIONS.csv"**
- **"odva_Sulphur_SHARED_PERMISSIONS.csv"**
- **"odva_Talihina_SHARED_PERMISSIONS.csv"**

ODVA Request #4:

"beginning December 1, 2021 through the date of this request, disclosure of all types of remote connection methods including but not limited to "Shared Remote Control," "Private Remote Control," "Remote PowerShell" and "Remote File Access" or any other equivalent methods of remote connection used by any persons other than employees of the Oklahoma Department of Veterans Affairs to access the mobile devices, computers, tablets, laptops, server systems, Microsoft SharePoint folders, cloud drive folders, including but not limited to OneDrive folders, and any other shared drive folders assigned to, used by or accessible to the employees of ODVA whose place of duty is the ODVA, Central Office, located at 2132 NE 36th Street, Oklahoma City, Oklahoma 73111 and who are the same employees previously named in paragraph one (1) above;"

OMES Response #4:

Zscaler ZPA, DFS, SMB (CIFS), using transport methods TCP, NBT, UDP, MDF, WinRM PowerShell, HTTP, HTTPS

ODVA Request #5:

"beginning December 1, 2021 through the date of this request, the names of the OMES employees and contract personnel employed by private contractors working for or on behalf of the State of Oklahoma or OMES, including but not limited to NTT Data Services, and any other persons or entities other than employees of the Oklahoma Department of Veterans Affairs who have been allowed or given access along with their remote management usernames utilized to initiate connection with the mobile devices, computers, tablets, laptops, server systems, Microsoft SharePoint folders, cloud drive folders, including but not limited to OneDrive folders, and any other shared drive folders assigned to, used by or accessible to the employees of ODVA whose place of duty is the ODVA, Central Office, located at 2132 NE 36th Street, Oklahoma City, Oklahoma 73111 and who are the same employees previously named in paragraph one (1) above;"

OMES Response #5:

Spreadsheet "All-Users-ODVA_2022-3-24.csv includes all OMES/NTT users who have elevated permission on ODVA resources. See folder "question 3."

ODVA Request #6:

"beginning December 1, 2021 through the date of this request, except for helpdesk or work tickets initiated by employees of the Oklahoma Department of Veterans Affairs, a copy of the helpdesk or work tickets from the OMES Cherwell, Ivanti or other ticketing systems which prompted the need for any instances of remote access into the mobile devices, computers, tablets, laptops, server systems, Microsoft SharePoint folders, cloud drive folders, including but not limited to OneDrive folders, and any other shared drive folders assigned to, used by or accessible to the employees of ODVA whose place of duty is the ODVA, Central Office, located at 2132 NE 36th Street, Oklahoma City, Oklahoma 73111 and who are the same employees previously named in paragraph one (1) above;"

OMES Response #6:

No responsive documents found.

ODVA Request #7:

"except for e-mails sent or received by employees of the Oklahoma Department of Veterans Affairs, copies of all e-mails in the possession of the State of Oklahoma referencing achievement of remote access or referencing attempts to gain remote access to the mobile devices, computers, tablets, laptops, server systems, Microsoft SharePoint folders, cloud drive folders, including but not limited to OneDrive folders, and any other shared drive folders assigned to, used by or accessible to the employees of ODVA whose place of duty is the ODVA, Central Office, located at 2132 NE 36th Street, Oklahoma City, Oklahoma 73111 and who are the same employees previously named in paragraph one (1) above;"

OMES Response #7:

Overly broad. Initial searches have pulled an unreasonable amount of data for OMES to review for request # 7 while effectively avoiding excessive disruption to OMES essential functions.

ODVA Request #8:

"all documentation and findings resulting from or relevant to the "forensic examination" of the laptop and OMES network account of Ms. Jennifer Shockley, State Human Resources Manager, arising from allegations of an unauthorized intrusion witnessed by multiple persons. Initiated by ticket number 2319958 and any other tickets related to or relevant to the matter; and"

OMES Response #8:

Forensic report is completed. Please reference folder "Question 8" for the records.

ODVA Request #9:

"copies of all e-mails referencing or relevant to ticket number 2319958 and any other tickets related to or relevant to the matter or the subsequent "forensic investigation," referenced in paragraph

eight (8) above, sent by or received by any state employee or state official, any contract personnel employed by private contractors working for or on behalf of the State of Oklahoma or OMES, including but not limited to NTT Data Services, or any other person or entity whose relevant e-mail traffic is in the possession of any state e-mail system or network or in the possession of any private contractor working for or on behalf of the State of Oklahoma or OMES, including but not limited to NTT Data Services, that may possess or hold e-mails or related data on behalf of the State of Oklahoma or OMES specifically."

OMES Response #9:

Results in folder "question 9."

In compliance with 51 O.S. Section 24A.5(6), OMES has established procedures to protect the integrity and organization of its records and prevent excessive disruption of its essential functions. OMES processed this request by identifying the records that are the records of ODVA and what are records of OMES that were requested pursuant to the Open Records Act.

OMES procedures require a search to locate records, an initial review to ensure only relative records are gathered and then a final legal review to redact any confidential information not subject to the Open Records Act. The total time taken for responding to this request was 39 hours security team and 6.0 hours legal team resulting in a cost of $1,800.00. Because Director Kintsel did not understand that OMES will assist an agency in recovering its records outside the parameters of the Open Records Act and internal OMES policies, inclusive of search fees. OMES waives the aforementioned fee for ODVA. Director Kintsel however, also asked for OMES records. OMES responded to this request for OMES data in #9 with the exception of maintaining one email as confidential as it exposes the OMES Security architecture. If the ODVA chooses to further reveal these records, OMES has no issue with it so doing.

All responsive documents obtained are being provided in a securely encrypted transfer method directly to you. You will receive an additional email with instructions to access the responsive documents. The documents will be identified in the folder designations as identified herein.

If ODVA has additional concerns, I am happy to provide OMES resources to address the same. I am willing to address the Commission or work with you and any member of your team to ensure the security and success of our operations.

Kindest Regards,

Steven Harpe
Chief Operating Officer