

AFFIDAVIT

I, David J. Barlow, being duly sworn, depose and say:

Introduction

1. I am a Special Agent with the United States Environmental Protection Agency, Office of Criminal Enforcement, Forensics, and Training, Criminal Investigation Division ("U.S.EPA-CID"). I have been so designated, as a Special Agent, for approximately twenty two years. I am presently assigned to the Cleveland, Ohio, Resident Office, located in Middleburg Heights, Ohio. My immediate responsibilities include violations which occur in the State of Ohio.
2. I was trained in criminal investigations at the Federal Law Enforcement Training Center in Glyncro, Georgia. Training in environmental criminal investigations ensued at the same location. Prior to becoming a Special Agent, I was employed by the United States Environmental Protection Agency ("U.S. EPA"), Environmental Sciences Division, as an Environmental Engineer. As an Environmental Engineer, I conducted compliance inspections, to include those relating to the Clean Water Act. As a Special Agent, I have conducted numerous criminal investigations of Clean Water Act violations.
3. U.S.EPA-CID has been granted primary investigative jurisdiction in matters concerning federal environmental criminal violations. My responsibilities as a Special Agent include the investigation of criminal violations of the federal environmental statutes, including violations of the Clean Water Act ("CWA"), 33 U.S.C. § 1251, et seq.

4. I make this affidavit from knowledge based on my participation in this investigation, including witness interviews by myself and/or other law enforcement officers, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.

5. The information set forth in this affidavit is for the limited purpose of establishing probable cause. This affidavit, therefore, does not necessarily include all of the information collected during this investigation.

6. This affidavit is made in support of applications for search warrants for the following locations and contents of electronic communication:

a. The business office and operating facility of KDA, Inc. ("KDA") at the KDA Kleese family farm facility, located at 5061 Warren Sharon Road, Vienna, Ohio 44473, further described as three buildings and several outbuildings. The first building is a Victorian farmhouse which has been converted into the offices of KDA. The second building is a large barn and is located to the north of the farmhouse. The third building is a large structure associated with the injection wells on the property. Lastly, there are several smaller outbuildings on the property.

b. The business office of KDA, located at 103 West Market Street, Warren, Ohio 44481. The KDA office comprises the entire third floor of the "Atrium Building" at the aforementioned address.

c. Electronic mail communications and other electronic files possessed by AOL, Inc. ("AOL"), 22000 AOL Way, Dulles, Virginia 20166, pertaining to tulsaruffneck5@aol.com.

d. Electronic mail communications and other electronic files possessed by GoDaddy.com, LLC ("GoDaddy") 14455 N. Hayden Rd. Suite 219, Scottsdale, AZ 85260, pertaining to all email addresses ending in @kdadisposal.com.

e. Information stored at premises and controlled by Verizon Wireless, 180 Washington Valley Road, Bedminster, NJ 07921, pertaining to cell phone account 330-360-8055.

Summary of Probable Cause

7. KDA is an Ohio active corporation for profit in Trumbull County, Ohio, that is an operating company for its sole investor, Kleese Development Associates, a family-owned oil and gas service provider. KDA offers injection well services to the oil and gas industry to include, disposal services, fluid hauling services, and oilfield project management services. Based on the investigation, conducted by myself and other investigators, I respectfully submit that there is probable cause to believe the release of oil to waters of the United States, which is a violation of 33 U.S.C. § 1321(b)(3), was the negligent result of inadequately constructed containment at the KDA facility (the "facility") in Vienna, Ohio. Specifically, a light-end petroleum product called "drip-gas" or "condensate" was spilled at the facility and from there it flowed into a tributary of Little Yankee Run, which is a tributary of the Mahoning River, all of which are waters of the United States. In addition,

I respectfully submit that there is probable cause to believe that KDA knowingly failed to report the oil spill, in violation of 33 U.S.C. § 1321(b)(5).

8. Your Affiant further submits that there is probable cause to believe there is now located at the locations described above evidence and instrumentalities of the criminal offenses against the United States as set forth in the preceding paragraph.

Summary of the Law

9. The Federal Water Pollution Control Act, commonly known as the Clean Water Act (“CWA”), 33 U.S.C. § 1251 et seq., was enacted by Congress to restore and maintain the chemical, physical, and biological quality of the Nation’s waters. 33 U.S.C. § 1251(a). In addition, the CWA was enacted to prevent, reduce, and eliminate water pollution in the United States and to conserve the waters of the United States for the protection and propagation of fish and aquatic life and wildlife, recreational purposes, and the use of such waters for public drinking water, agricultural, and industrial purposes. See 33 U.S.C. § 1252(a).

CWA Violation – Discharge of Oil

10. Under the CWA, as amended by the Oil Pollution Act in 1990, the discharge of oil into or upon the navigable waters of the United States in such quantities that may be harmful is prohibited. See 33 U.S.C. § 1321(b)(3).

11. “Discharge” includes, but is not limited to, spilling, leaking, pumping, pouring, emitting, emptying or dumping. See 33 U.S.C. § 2701(7). See also 33 U.S.C. §1321(a)(2).

12. “Oil” means oil of any kind or in any form, including petroleum, fuel oil, sludge, oil refuse, and oil mixed with wastes other than dredged spoil. See 33 U.S.C. § 2701(23). See also 33 U.S.C. § 1321(a)(1).

13. Discharge of oil in such quantities “that may be harmful” is defined as any amount of oil that causes a film or sheen on the surface of the water, or causes sludge or emulsion to be deposited beneath the surface of the water. See 40 C.F.R. § 110.3. See also 33 U.S.C. § 1321 (b)(4).

14. “Navigable Water” is defined as the waters of the United States. See 33 U.S.C. § 1362(7). See also 33 U.S.C. § 2701(21). This term includes all waters that could affect interstate commerce, including rivers, streams, and their tributaries. See 40 C.F.R. § 110.1.

CWA Violation – Failure to Notify of Oil Discharge

15. The Oil Pollution Act also amended the CWA to provide notification requirements concerning oil spills. Specifically, any person in charge of a vessel or an onshore or offshore facility shall, as soon as he has knowledge of any discharge of oil or a hazardous substance from such facility in violation of 33 U.S.C. § 1321(b)(3), immediately notify the appropriate agency of the United States Government of such discharge.

16. The term “in charge” is not defined by statute or regulation. However, courts have held that a corporation can be a “person in charge.” See Apex Oil Co. v. United States, 530 F.2d 1291, 1293 (8th Cir.), cert. den., 429 U.S. 827 (1976); United States v. Mobil Oil Corp., 464 F.2d 1124, 1127 (5th Cir. 1972).

17. An onshore facility is defined as “any facility (including, but not limited to, motor vehicles and rolling stock) of any kind located in, on, or under, any land within the United States, other than submerged land.” See 33 U.S.C. § 1321(a)(10).

18. The “appropriate agency” is the United States Coast Guard, which operates the National Response Center (“NRC”), reachable around the clock through a toll-free 800 telephone number. See 40 C.F.R. § 110.6.

19. A spill is supposed to be reported immediately upon receipt of knowledge of it by the person in charge. What constitutes immediate notice, though, may depend upon circumstances unique to the case. See United States v. Messer Oil Corp., 391 F. Supp. 557, 562 (W.D. Pa. 1975).

20. A negligent violation of the oil discharge prohibition at 33 U.S.C. § 1321(b)(3), is criminally enforceable pursuant to 33 U.S.C. § 1319(c)(1)(A). Failure to notify the NRC in the event of an oil spill is criminally enforceable pursuant to 33 U.S.C. § 1321(b)(5).

Summary of Investigation

21. KDA, per its website, operates seven underground injection wells at two facilities in Trumbull County, Ohio. Five of the current injection wells are on the 200-acre KDA Kleese family farm in Vienna, Ohio, and are referred to as the “Kleese Wells.” This disposal facility can handle up to 8,000 barrels of oil/gas well-related fluid injection daily, with two quintiplex pumps.

22. The address for the KDA Kleese family farm facility is 5061 Warren Sharon Road, Vienna, Ohio 44473. This property occupies the northwest quadrant of the intersection of

Warren-Sharon Road and Sodom-Hutchings Road. At the corner of the property, at the intersection of Warren-Sharon Road and Sodom-Hutchings Road, is an old two-story farmhouse. The Kleese #1 injection well and tank batteries are located north of the farmhouse.

23. The tank batteries consist of two individual tank batteries located next to each other. The tank batteries were built at different times, the most recent battery, the northern most battery, was constructed approximately one year ago.

24. Across the street (Sodom-Hutchings Road) from the KDA Kleese family farm facility, is a wetland that drains to a creek, which is a tributary to Little Yankee Run, which is a tributary to the Mahoning River; which are waters of the United States.

The Spill

25. On April 10, 2015, Kurt Kollar, On-Scene Coordinator, Ohio Environmental Protection Agency ("OEPA"), Division of Environmental Response and Revitalization, related to your affiant that on Thursday, April 02, 2015, he was made aware of a release of an oily substance from the KDA Kleese family farm facility property in Vienna, Ohio.

26. Kollar stated that the released oil-related product was evident throughout the watercourse, which makes up the tributary to Little Yankee Run, and includes the stream/creek portions, the wetlands areas and private ponds. Kollar acknowledged that the oil-related product was in the stream/creek portion and that he has photographs. Kollar stated that the oil derived product had an oily sheen and film associated with it.

27. Kollar's subsequent involvement and investigation revealed that between 2,000 and 8,000 gallons of a light-end petroleum derivative called "drip gas" was released to the wetland and creek referred to above, from the tank batteries associated with the Kleese Wells. The release occurred sometime prior to March 30, 2015, when citizen complaints began to be received by regulatory agencies.

28. Kollar stated that he learned from KDA employees that a company, IWC, was contracted by KDA to perform some tank-related maintenance/cleaning activities at the facility, during which time an incident occurred that released a significant amount of petroleum, approximately 10,000 gallons, within the north tank battery. The incident occurred approximately two to three weeks prior to Kollar speaking to the employees.

Inadequate Containment

29. Based on observations by your affiant and review of Ohio Department of Natural Resources ("ODNR") file documents, the KDA tank batteries consist of numerous storage tanks constructed within a "containment," an impermeably lined concrete pad with cement and earthen dikes around it designed to inhibit the release of any liquids resulting from a tank failure, leaks or spillage within the confines of the diking perimeter. There are two almost-identical tank batteries associated with the KDA property in Vienna; both approved by the ODNR, based on drawings and representations submitted by KDA.

30. Steve Ochs, ODNR, stated that an impermeable liner should have been installed under the concrete base (floor), and dike berms, of the containment, to inhibit the release of anything spilled within it. KDA has been ordered to dismantle the entire tank battery.

Ochs stated that, to date, there is no evidence that a liner was installed under the concrete base of the containment.

31. Andrew Adgate, Geologist, ODNR, advised that ODNR requires containments of surface facilities, like the tank batteries at the Kleese family farm facility, to be impermeable. This would require a one piece liner under the floor and berms of the containment, or if multiple liners are used, with welded seems. Adgate acknowledged that liners that merely overlap and do not have welded seems are not impermeable. In the event that a concrete pad is used, the construction of the containment would require that the joint between the walls or berms and the floor of the containment be impermeable. The fact that product migrated from the containment at the KDA facility reveals that the containment was not impermeable. Adgate produced a drawing from his file and hand written notes that Adgate identified to have been written by Matt Kleese, which describes a 30 mil liner to be installed under the concrete pad of the south battery. The north battery was supposed to be identical to the south battery.

Failure to Report Spill

32. Ochs stated that he has been present at the site, as a representative of the ODNR, during the remediation efforts, to date. When Ochs first arrived at the KDA Kleese family farm property on April 02, 2015, in response to a citizen complaint of a release of an unknown substance, he observed an oil absorbent material called "Peatsorb" that had been deployed, and standing pools of what appeared to be an oily product, in a swale on the property. The evidence of the flow of the oil-related product in the swale ended at a

depression in the front lawn of the facility. Subsequent excavation of the depression revealed a drain pipe that conveyed the oil to the wetlands across Sodom-Hutchings Road. KDA representatives denied knowledge of a release of product or even how the Peatsorb came to be deployed in the swale.

33. Ochs stated that investigative efforts, that include dye testing from within the tank battery containment and excavation outside it, show that product spilled within the north tank battery, easily migrated under the dike wall to an underground gravel layer on top of a clay layer, where it flowed to agricultural field drainage tiles. The field drainage tiles empty to a culvert which, in turn, discharges to the swale, where the Peatsorb and pools of product were observed.

34. Ochs stated there is a drain system around the perimeter of the diking surrounding the tank batteries. The drain system drains to a sump, equipped with a pump, which pumps the sump's contents back inside the containment. KDA related that the sump is checked daily. When OEPA and ODNR representatives checked the contents of the sump, it was full of a light-end oily product, like gas. Ochs stated this, and the presence of the Peatsorb material and standing pools of product in the swale suggest to him that KDA knew of a release of product.

35. On or about April 2, 2015, KDA reported the spill to OEPA, after OEPA arrived at the facility.

KDA Business Offices

36. Kollar stated that there are offices on the Kleese family farm facility in which Krissy Burrows, Field Office Manager, and other KDA office personnel conduct work. Kollar has been in the office area and has observed office work stations that include computers. Kollar stated that a closed circuit video camera system records any events that occur in proximity to or in association with the injection well/tank battery. KDA personnel can access live video footage via their cell phone.

37. On April 10, 2015, Steve Ochs, ODNR, related to your affiant that the old farmhouse on the KDA Kleese family farm property, serves as the offices for the Vienna, Ohio facility. Ochs has been in the farmhouse and has observed work spaces, with computers, that facilitate the day to day work of KDA office personnel, to include, Krissy Burrows, who is identified on a "KDA Spill Cleanup 04/2015" contact information sheet, as the Chief Operations Officer.

38. On April 15, 2015, Adgate related to your affiant that he communicates, at times with Matt Kleese, who is the Vice President of Field Operations for KDA, via e-mail. Adgate advised that Kleese's e-mail address is tulsaruffneck5@aol.com. Adgate receives e-mails sent from Kleese's telephone, a 4G LTE Droid, which has a telephone number associated with it as 330-360-8055. Subsequent to the interview with Adgate, Adgate forwarded an example e-mail to your affiant that he received from "MJ Kleese [mailto:tulsaruffneck5@aol.com]" on March 20, 2015. At the end of the e-mail from Kleese, it is written: "Sent from my Verizon Wireless 4G LTE DROID"

39. Written correspondence between ODNR and KDA, relative to its injection wells, is typically to or from the business address of Kleese Development Associates, 103 W. Market Street, Warren, Ohio 44481. Adgate recalled that the ODNR “Chief’s Order” to discontinue activity at the site, as a result of the recent release, was hand delivered to the Kleese family farm facility by Steve Ochs.

40. On April 16, 2015, your affiant visited the publically accessible business offices of KDA, Inc., 103 West Market Street, Warren, Ohio, which occupies the third floor of the “Atrium Building.” Your affiant observed a number of work stations equipped with desktop computer units.

Affiant’s Request for a Search Warrant

41. Your Affiant respectfully submits that the foregoing facts establish probable cause that by virtue of constructing a non-impermeable containment around a tank battery comprised of tanks containing oily wastewater, as required, KDA negligently caused the discharge of oil into navigable waters of the United States, in violation of 33 U.S.C. § 1321(b)(3).

42. Your Affiant also respectfully submits that the foregoing facts establish probable cause that the release of an oil derived pollutant occurred from the KDA Kleese family farm facility into a water of the United States, in violation of 33 U.S.C. § 1321(b)(3) and was not reported by KDA, in violation of 33 U.S.C. § 1321(b)(5).

43. Therefore, your Affiant respectfully requests a search warrant be issued for the locations identified in Attachment A, and to seize the items identified in Attachment B.

44. The agents will utilize best efforts to minimize disruptions at the KDA facility.

45. Pursuant to 18 U.S.C. § 3105, your Affiant requests assistance from the Ohio Attorney General's Office, Bureau of Criminal Investigation; the Ohio Environmental Protection Agency and local police and fire service, and others deemed necessary to assist in conducting the search.

Technical Terms

46. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Computers, Electronic Storage, And Forensic Analysis

47. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or

other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

48. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

e. Based on the investigation, including the review of e-mails and correspondence, there is reason to believe that there is a computer system currently located on the PREMISES.

49. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection

programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an

incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

50. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be

unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

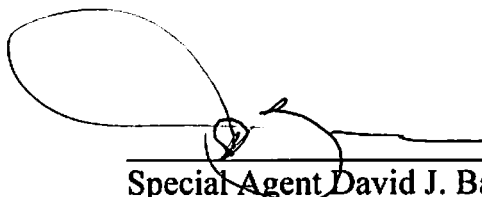
c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

51. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence

described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

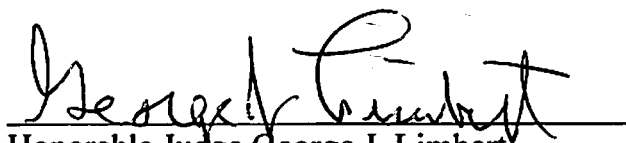
52. KDA (“the Company”) is a functioning company that conducts legitimate business. The seizure of the Company’s computers may limit the Company’s ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent

practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

A handwritten signature in black ink, appearing to read 'David J. Barlow', written over a horizontal line.

Special Agent David J. Barlow
U.S. Environmental Protection Agency
Criminal Investigation Division

Sworn and Subscribed to before me and subscribed in my presence this 27 day of April 2015

A handwritten signature in black ink, appearing to read 'George J. Limbert', written over a horizontal line.

Honorable Judge George J. Limbert
United States Magistrate Judge
Northern District of Ohio