UNITED STATES DISTRICT COURT

for the

Southern District of Indiana

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	
The property and premises known as the Terre Haute Administration Building, located at 3200 South State Road 63, Terre Haute, Indiana (more particularly described in Attachment A, incorporated herein by reference)	)	Case No. 2:17-mj-00011

Sealed

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Indiana *(identify the person or describe the property to be searched and give its location)*:

The property and premises known as the Terre Haute Administration Building, located at 3200 South State Road 63, Terre Haute, Indiana (more particularly described in Attachment A, incorporated herein by reference)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before August 1, 2017 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Tim A. Baker *(United States Magistrate Judge)*.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: 07/18/2017 11:30 am

Judge's signature

City and state: Indianapolis, Indiana

Hon. Tim A. Baker

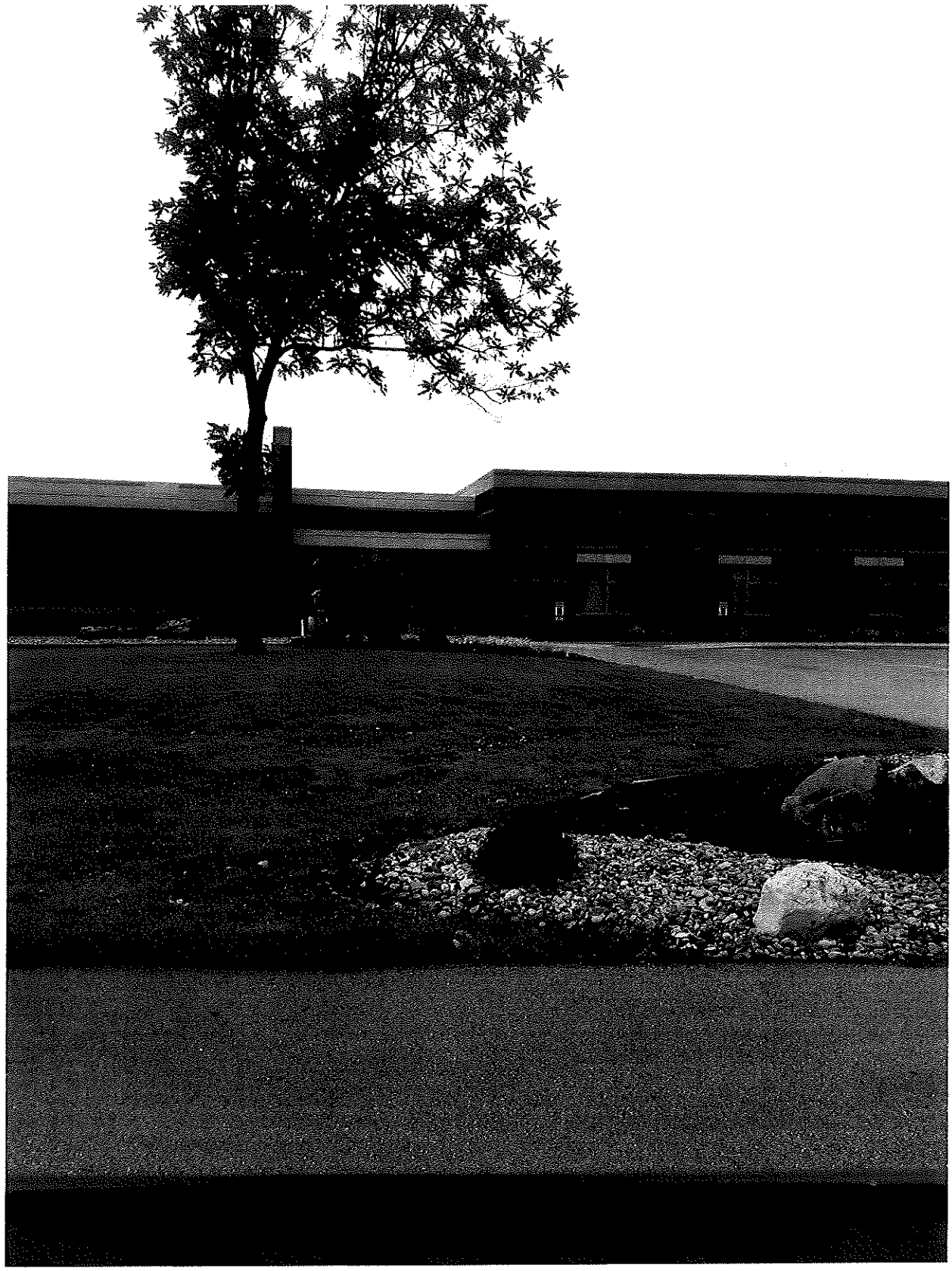
Printed name and title

ATTACHMENT A

The Terre Haute Administration Building is located at 3200 South State Road 63, Terre Haute, Indiana. Photographs of the building are affixed to this Attachment.


CITY OF
TERRE HAUTE


Terre Haute Wastewater
Utility
3200 S. STATE RD 63



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence, instrumentalities and fruits concerning violation of Title 18, United States Code, Sections 666 (federal program bribery), 1341 (mail fraud), 1343 (wire fraud), and 371 (conspiracy to defraud the United States), as follows:

1. Financial records, including receipts, checks, bank and savings and loan records of deposit, withdrawal and wire transfer, statements and other bank records, letters of credit, credit card statements, money orders, cashier's checks, passbooks, cancelled checks, certificates of deposit, loan records, customer account information, income and expense summaries, cash disbursement journals, financial statements, and state and federal income tax returns.

2. Documents related to vendors used by the Terre Haute Wastewater Utility to perform services at its facilities including, business or financial records which show compensation, deposits, withdrawals, disbursements, or reimbursement to the Terre Haute Wastewater Utility.

3. Documents related to the Terre Haute Wastewater Utility including:

- Records of income or expenses including invoices and receipts;
- records of vendors or suppliers;
- records of receipts or disbursements;
- accounting information, including trial balances or work sheets adjusting, reclassifying, closing, or reversing entries;
- bank statements, check registers, or canceled checks;
- duplicate deposit tickets;
- bank account reconciliations;
- passbooks, certificates of deposit, money orders, or cashier's or official checks;
- records of payroll or employee earnings;

- records of bartering activity such as exchanges of property or services;
- financial statements or copies of tax returns;
- memos or other records of communications including documents of E-mails, fax transmissions or receipts;
- Employee organizational charts;

4. Documents and items relating to the Terre Haute Wastewater Utility, Christopher Mark Thompson, and or vendors of the Terre Haute Wastewater Utility, including correspondence, financial records, contracts or written agreements, invoices, deposits, withdrawals, contributions, donations, donors, gifts, notes, ledgers, appointment calendars, address books, diaries, photographs, and videos.

5. Any and all communication between employees of the Terre Haute Wastewater Utility and its vendors from January 1, 2013, to the present.

6. Any and all correspondence, including invoices, records of phone calls, E-mails, and letters between Christopher Mark Thompson, other Terre Haute Wastewater Utility employees, and any past, present or potential vendors of the Terre Haute Wastewater Utility.

7. Safe deposit box keys, other items evidencing the obtaining, secreting, transfer, concealment or expenditure of funds.

8. Any and all electronic devices that are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data. These devices include computers, personal digital assistants ("PDA"s),

computer components, external hard drives, servers, and other computer related electronic devices.

9. Documents in any format or medium that describe or refer to any accounts with an Internet Service Provider.

10. Documents in any format or medium that describe or refer to online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

11. With respect to any computer equipment or other electronic devices:

a. Passwords, encryption keys, and other access devices that may be necessary to access the computer equipment.

b. Documents or other items demonstrating the presence or absence of computer software that would allow others to control the items, and presence or absence of security software designed to detect such malicious software.

c. Documents or other items demonstrating the attachment of other computer hardware or storage media.

d. Counter forensic programs and associated data that are designed to eliminate data.

12. Items in the paragraphs above that are stored in computer media, including media capable of being read by a computer (such as external and internal

computer hard drives, memory sticks, and thumb drives), and electronic devices that are capable of analyzing, creating, displaying, converting, or transmitting electronic or magnetic computer impulses or data (such as cellular telephones, and personal digital assistants (PDAs)), shall be searched in accordance with the attached Addendum.

13. Documents concerning occupancy or ownership of the Subject Premises (described in Attachment A), such as utility and telephone bills, mail envelopes, or addressed correspondence.

14. Documents that demonstrate the use, ownership, or control of the computers or other electronic devices located at the Subject Premises (described in Attachment A), including the times the computer was accessed, such as sales receipts, bills for Internet access, and handwritten notes.

13. Documents and items, in any form, which are evidence, instrumentalities and fruits concerning violation of Title 18, United States Code, Sections 666 (federal program bribery), 1341 (mail fraud), 1343 (wire fraud), and 371 (conspiracy to defraud the United States).

ADDENDUM TO ATTACHMENT B

This warrant does not authorize the "seizure" of computers and related media within the meaning of Rule 41(c) of the Federal Rules of Criminal Procedure. Rather this warrant authorizes the removal of computers and related media so that they may be searched in a secure environment. The search shall be conducted pursuant to the following protocol:

With respect to the search of any computers or electronic storage devices removed from the premises described in Attachment A hereto, the search procedure of electronic data contained in any such computer may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein;

d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized as set forth herein;

e. scanning storage areas to discover data falling within the list of items to be seized as set forth herein, to possibly recover any such recently deleted data, and to search for and recover deliberately hidden files falling within the list of items to be seized; and/or

f. performing key word searches through all electronic storage media to determine whether occurrences of language contained in such storage media exist that are likely to appear in the evidence described in Attachment B.

The government will return any computers or electronic storage devices removed from the premises described in Attachment A hereto within 30 days of the removal thereof, unless contraband is found on the removed computer and/or electronic storage device, or unless otherwise ordered by the Court.