

# **Exhibit 7**

1 DANIEL G. BOGDEN  
 United States Attorney  
 2 PAUL L. PUGLIESE  
 Assistant United States Attorney  
 3 100 W. Liberty Street, Suite 600  
 Reno, Nevada 89501  
 4 Tel: (775) 784-5438  
 5 Attorneys for Plaintiff

<input checked="" type="checkbox"/> FILED ENTERED	<input type="checkbox"/> RECEIVED SERVED ON COUNSEL/PARTIES OF RECORD
SLP 1 11 06	
CLERK US DISTRICT COURT DISTRICT OF NEVADA	
BY: _____	DEPUTY

6 UNITED STATES DISTRICT COURT  
 7 DISTRICT OF NEVADA

8 IN THE MATTER OF THE SEARCH OF: )  
 ) No. 3:06-CV-0263-BES-VPC  
 9 The Residence Located at 12720 )  
 Buckthorne Lane, Reno, Nevada, and )  
 10 Storage Units 136, 140, 141, 142, and 143, ) **GOVERNMENT'S COMPLIANCE**  
 Double R. Storage, 888 Maestro Drive, ) **WITH COURT ORDER OF**  
 11 Reno, Nevada ) **AUGUST 17, 2006**  
 )  
 12 )  
 )

13  
 14 COMES NOW, the United States of America, by and through DANIEL G. BOGDEN, United  
 15 States Attorney, and PAUL L. PUGLIESE, Assistant United States Attorney, and complies with the  
 16 Court's order of August 17, 2006.

17 During a hearing on August 17, 2006, the Court directed that the Government provide to the  
 18 Court all reports and information that Special Agent Michael West relied upon in support of the  
 19 information contained in the search warrant affidavits at issue in this matter. Upon receipt, the Court  
 20 would conduct an *in camera* review in order to determine whether any of the information is relevant  
 21 to a determination on issues currently outstanding in this matter.

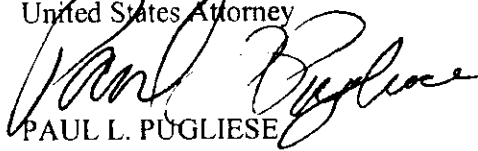
22 \\\  
 23 \\\  
 24 \\\  
 25 \\\  
 26 \\\

69

1 The Government has attached pages numbered 00001 - 00137 and dated September 11, 2006.  
 2 The Government opposes the release of any of the attached documents to counsel for the movants at  
 3 this time. Such release is not appropriate as the investigation of alleged offenses involving Mr.  
 4 Montgomery continues, and the information contained herein is not necessary for a determination on  
 5 the movants' pending motions.

6 Dated: September 11, 2006

7 Respectfully submitted,  
 8 DANIEL G. BOGDEN  
 9 United States Attorney

10   
 11 PAUL L. PUGLIESE  
 12 Assistant United States Attorney  
 13  
 14  
 15  
 16  
 17  
 18  
 19  
 20  
 21  
 22  
 23  
 24  
 25  
 26

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/13/2006

Warren Trepp, Chief Executive Officer, eTreppid Technology, LLC., 755 Trademark Drive, Reno, Nevada, telephone (775) 337-6771, was interviewed at the Reno Resident Agency of the Federal Bureau of Investigation by Special Agents John Piser III and Michael A. West, regarding the theft of trade secrets and classified information from eTreppid Technology, LLC.

Trepp was introduced to Dennis Lee Montgomery by Eldorado Casino Host Steven Sands in 1997. Trepp became aware that Montgomery wanted to start a new business involving the development of pattern recognition and compression of software.

In the end of 1998, Trepp and Montgomery formed Intrepid, a company to develop pattern recognition and compression software. On September 28, 1998, Trepp and Montgomery signed a contribution agreement wherein Montgomery received a fifty percent ownership in Intrepid in return for providing certain computer software technologies to Intrepid. Trepp provided a copy of the contribution agreement signed by Montgomery dated September 28, 1998.

Trepp advised that at a later date, the name Intrepid was changed to eTreppid Technology, LLC to avoid any legal issues relating to the name of Intrepid.

Trepp advised that Montgomery currently owns approximately thirty percent of eTreppid. Montgomery's ownership was reduced due to Montgomery selling a portion of his ownership for 2.25 million dollars and a capitol call in which Montgomery did not participate. The capitol call required equity investors to contribute additional capitol to eTreppid to continue the operation of the business.

Montgomery became the Chief Technical Officer (CTO) for eTreppid and had the responsibility for the day to day activities of eTreppid to include the hiring and firing of employees and preparing the company's products to satisfy customers. Montgomery was also on the Executive Management Committee which controlled the overall activities of the business. This Executive Management Committee consisted of Trepp, Montgomery, and Attorney Doug Frye.

Investigation on 01/31/2006 at Reno, Nevada

File # 295A-LV-39368

Date dictated 02/09/2006

by SA John Piser III  
SA Michael A. West:st

00001

295A-LV-39368

Continuation of FD-302 of Warren Trepp, On 01/31/2006, Page 2

Trepp advised that Montgomery has software programming skills; however, recently Trepp has found out that Montgomery's skills may not be what he has purported them to be. Trepp cited a recent Air Force Office of Special Investigation Inquiry, which determined that Montgomery's programming skills were not what he alleged. Montgomery has hired other employees to do programming and claimed that he did the work.

Trepp recently learned that Montgomery would require eTreppid employees to falsify the results of live demonstrations for it's customers. Jesse Anderson, a programmer for eTreppid, told Trepp that Montgomery would require Anderson and Jim Bauder, another eTreppid employee to go into an office at eTreppid while Montgomery was out in a nearby field with a toy bazooka to demonstrate eTreppid's recognition software capabilities. Montgomery instructed Anderson and Bauder to go into a room and wait to hear a noise on their cell phone and then instructed them to press a button on a computer keyboard that would display an image of a bazooka on the computer screen viewed by the customers, including Department of Defense employees. Trepp advised that the Department of Defense employees were at the demonstration to make a judgment regarding the purchase of this technology.

---

Trepp advised that on December 8, 2005, Montgomery requested a personal loan of two hundred and seventy five thousand dollars through Trepp's financial company known as Friendly Capitol Partner, LP. Trepp further advised that he has loaned Montgomery money since approximately 1999 and estimated that Montgomery has an outstanding balance of approximately 1.375 million dollars and an \$125,000.00 in interest owed.

Trepp advised that Sloan Venables was able to recover approximately five years of Montgomery's e-mails maintained on eTreppid hardware; however, no e-mails were recovered for December 2005 to January 2006. Trepp advised that a review of these e-mails clearly showed that Montgomery is having financial troubles.

Trepp advised that Montgomery goes to the Eldorado Casino/Hotel and the Peppermill Hotel/Casino at night to gamble. Montgomery has told Trepp that he has a system for counting cards in an eight deck shoe in blackjack. Trepp has known Montgomery to use a three hundred thousand dollar line of credit at Nevada casinos.

00002  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Warren Trepp, On 01/31/2006, Page 3

Trepp advised that approximately ten days ago, Montgomery asked Neil Azzinero, an El Dorado Hotel/Casino host, if Azzinero knew of a U.S. citizen who would be interested in funding a new business with him and needed five to ten million dollars.

Trepp advised that Montgomery is married to Brenda Montgomery and has two boys, Brian Montgomery, age 30, Steven Montgomery, age 26, and Kate Montgomery, age 23. Brian Montgomery and Steven Montgomery have been employed at eTreppid in the past, building hardware components.

Trepp advised that on January 9 or January 10, 2006, Montgomery stated "you're an asshole and I will see you again" to Jesse Anderson, which Anderson took as some type of threat. Montgomery has a bad temper and has been verbally abusive to employees and known to throw objects. Montgomery was also known to have had a Temporary Restraining Order issued against him from a former girlfriend who was employed at eTreppid.

Trepp considers Montgomery to be a bright individual, who is a workaholic and has been known to embellish facts to his advantage. Trepp further described Montgomery as being independent and arrogant.

Trepp advised that while Venables was on vacation from December 22, 2006 to January 4, 2006, Montgomery deleted all source code relating to eTreppid's software development efforts and all back up copies related to that software. Trepp further advised that only two employees had access to the company servers, known as the Source Server and the ISA Server. Those two employees were Sloan Venables and Dennis Montgomery. The Source Server contained all source code developed by eTreppid employees and their executable forms. Montgomery had the sole responsibility to back up the Source Server. Venables recently purchased a server known as the ISA server, just prior to his vacation, to act as a data warehouse for all eTreppid data.

Trepp advised that Montgomery routinely backed up the Source Server data onto a stand alone computer in Montgomery's office.

When Sloan returned from vacation, Sloan asked Montgomery where the back up computer for the Source Server was to which Montgomery advised Venables that he took it home. Trepp advised that Montgomery has never been known to take this computer home in

00003  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Warren Trepp, On 01/31/2006, Page 4

the past. Trepp further advised that this back up computer is missing from eTreppid.

Trepp advised that a review of both the Source Server and the ISA server revealed that all pertinent development data was deleted from the Source Server and the ISA server was damaged and is unusable. Trepp further advised that between January 7, 2006 and January 8, 2006, each computer work station at eTreppid was deleted of all software development data. Trepp advised that only two employees at eTreppid would have access to delete this level of data and those two employees are Venables and Montgomery.

Trepp advised that a review of eTreppid's alarm code log revealed that on January 7, 2006 and January 8, 2006, eTreppid alarm was disarmed and re-armed by Montgomery's alarm code.

Trepp further advised that eTreppid maintains a video surveillance system covering the exterior and interior of eTreppid and on January 10, 2006, a review of this equipment revealed that the machines were no longer recording and all data on the computers had been deleted. eTreppid's video surveillance system consists of seventeen video cameras which record on seventeen separate computer systems.

Trepp advised that the Source Server contained all intellectual property developed by eTreppid employees and possibly contained secret information.

Trepp advised that eTreppid has been developing software for use by various U.S. Government agencies and as a part of this development effort, have received authorization to possess and maintain classified information up to the Secret level. eTreppid employees would receive Secret information from U.S. Government agencies on various hard drives and Mini DV tapes which contained still and video images to be used in eTreppid's development efforts. Trepp advised that employees Patty Gray, Sloan Venables, and Dennis Montgomery handled this classified information. eTreppid was required to store this classified information in safes provided by the Air Force.

Trepp advised that after Montgomery left the business on January 10, 2006, an inventory of the classified hard drives and mini DV tapes was conducted and this inventory revealed that nine hard drives containing secret data were missing. As a result of

00004  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Warren Trepp, On 01/31/2006, Page -5-

this inventory, Trepp learned that possibly additional copies of the nine original hard drives were made by Montgomery.

Trepp advised that Montgomery is no longer an employee of eTreppid and alleges that he (Montgomery) has a copyright dating back to 1982 on software used by eTreppid for which he has not been paid.

Trepp advised that Montgomery's behavior is odd, considering that eTreppid would most likely receive government contracts in the near future which would result in million dollar contracts for eTreppid.

Trepp advised that on January 9, 2006, he asked Montgomery, who deleted the data from the Source Server and ISA server, to which Montgomery blamed Patty Gray. Trepp further advised that on January 10, 2006, he requested that Montgomery returned any items including the software that he had taken from eTreppid and Montgomery denied taking anything.

Trepp advised that he required Montgomery to provide him a copy of all data on the Source Server once every year to protect ~~both himself and Montgomery should something ever happen to this~~ data. Trepp advised that when he learned that the Source Server had been deleted and Montgomery refused to return to work, he looked at the copies provided by Montgomery over the years, and found that these disks were blank or contained no data relevant to eTreppid's development efforts.

00005  
Sept. 11' 06



- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/13/2006

Sloan Sterling Venables, white male, [REDACTED]

[REDACTED] cell

[REDACTED] was interviewed at the Reno Resident Agency of the Federal Bureau of Investigation by Special Agents John Piser III and Michael A. West, regarding the theft of trade secrets from eTreppid Technologies, LLC.

Venables has been employed as the Director of Research and Development at eTreppid since approximately December of 1999. Venables duties include being the Facilities Security Officer who is responsible for ensuring compliance with government regulations in the storage of restricted information maintain by eTreppid. Venables is also the Network Administrator who maintains the mail and web servers, maintains the router configurations, purchases hardware for both internal and customer use, and leads half of the programming staff. Venables advised that he or Dennis Montgomery would know all eTreppid's efforts related to software development and the daily operations at ETreppid.

Venables advised that because of his responsibilities, he knows every piece of hardware at eTreppid as he has either installed it or hired someone to install it.

Venables knew Montgomery prior to coming to work at eTreppid and has worked closely with Montgomery since December of 1999.

Venables advised that in the fall of 2005, Patty Gray suspected Montgomery was doing something other than what he was actually telling people he was doing. Gray was trying to figure out what Montgomery was doing. Venables knew Montgomery promised products to customers that had not been completed or even assigned to programmers. Venables did not have specific details regarding this activity; however, Gray or employee Jesse Anderson may have more information.

Venables advised that Montgomery found out about Gray's and Anderson's efforts to look into his activities. In the beginning of December 2005, Montgomery installed removable hard drives on each of the programmer's workstation so he could remove

Investigation on 02/02/2006 at Reno, Nevada

File # 295A-LV-39368

JPW

Date dictated 02/09/2006

by SA John Piser III

SA Michael A. West:st

00006

Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Sloan Sterling Venables, On 02/02/2006, Page 2

the hard drives and required the programmers, to include Lalith Tenneti and Barjinder Bal, and Krishna Tangirala, to give him the source code that they were working on.

Venables advised that on December 21, 2005, he called Montgomery while driving to work and Montgomery told Venables not to come in to work and to stay home to get ready for his trip. Venables arrived at eTreppid at approximately 11:00 AM on December 21, 2005, to complete work on the Internet Security Accelerator Server or ISA Server. Venables intended this server to act as a proxy server and manage the RAID (Redundant Array of Inexpensive Disks) unit, containing sixteen hard drives, to back up the Source Code Server or SRC Server and all other servers. Venables wanted to put the ISA server in operation and back up all eTreppid data prior to leaving on vacation. Venables mounted the ISA Server and RAID unit in the same cabinet as the SRC Server with the assistance of Jim Bowder.

Venables turned on the ISA Server and started backing up the SRC Server using a program known as XX-Copy which copies files and prepares a log of which files were successfully copied. Venables recalled that the ISA Server finished a few folders on the SRC Server while he was still in the building on December 21, 2005.

The servers at eTreppid contain a large amount of data which would take many hours to back up successfully. The Development Server contains approximately two hundred gigabytes of storage and Venables estimated that the SRC Server contains another two hundred gigabytes of information. Venables advised that because of the file size and structure, it would take a lot of time to successfully delete these files.

Venables advised that on December 21, 2005, he went out into the warehouse where Montgomery had a server and RAID box Montgomery used to periodically back up the SRC Server. Venables noticed that the Central Processing Unit (CPU) and the RAID box were missing and the only thing left at Montgomery's work area were the monitor, mouse, and keyboard. Venables asked Montgomery what happened to the server and the RAID box to which Montgomery stated that he took them home. Venables advised that both the CPU and the RAID box are large and noticeable items with the CPU being a large black Lianli case with a Pentium processor with an ASUS 4C800-E motherboard and a LSI controller to run the RAID box and the RAID box contained eight hard drives and had serial number 6564737. Venables advised that these items are large and noticeable with the

00007  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Sloan Sterling Venables , On 02/02/2006 , Page 3

RAID box weighing approximately one hundred pounds. Venables valued these items at approximately \$5,000.00 for the RAID box, \$5,000.00 for the hard drives, \$600.00 for the controller card, and \$3,000.00 for the CPU.

Venables advised that Montgomery was responsible for backing up the SRC Server onto the RAID box maintained by Montgomery. The server and RAID box used by Montgomery was not accessible by any other computer on the network and was connected directly to the SRC Server. Venables further described the RAID box as being an Ultra Store, model 2081, containing eight IDE 320 gigabyte hard drives with serial number 6564737. eTreppid purchased two like models, one of which is accounted for in the warehouse, and contains serial number 4460005.

Venables questioned Montgomery further as to why he took the server and RAID box home and Montgomery did not respond. Montgomery is known for not responding to people and just walking off.

Venables advised that he is responsible for backing up the data on all other eTreppid servers except for the SRC Server. These other servers included web servers, a SQL database server, and eight other servers for administrative functions at eTreppid.

Venables advised that he was at eTreppid until approximately 11:00 P.M., on December 21, 2005, and left his residence on December 22, 2005, at approximately 7:00 A.M., en route to the Reno Airport to travel to Budapest, Hungary to visit a high school friend for the Holidays. Venables returned to Reno, Nevada at approximately 12:00 A.M., on January 2, 2006.

Venables was unable to sleep after returning from in vacation and decided to go into work early on January 3, 2006, and arrived at the office at around 9:00 A.M. Venables normally arrives at the office around 11:00 A.M. and works into the evening.

Upon arriving at his desk on January 3, 2006, Venables noticed that the server cabinet and keyboard were messed up. Venables went into the Server Room and noticed that the SRC Server had recently been logged into and a process was running. Venables advised that he configured all eTreppid servers to have the screen saver lock out mode activate after one minute of non-use which requires the user to log back into the server after not touching the keyboard for one minute.

00008  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Sloan Sterling Venables, On 02/02/2006, Page 4

Venables noticed the SRC Server had a command prompt on the screen which indicated to him that someone had used the SRC Server console within the last minute and he could see files scrolling by; however, he could not determine what task was running. Shortly thereafter, Montgomery walked into the Server Room and said he was just "cleaning up stuff" on the SRC Server and Venables could cancel the operation. Venables went downstairs to talk to Montgomery more about what he was doing on the SRC Server. Montgomery stated he was "cleaning up stuff" and deleting old files.

Venables advised that he set up the SRC server with a folder named ET Development with sub-folders for each programmer. Each programmer was given permission up to modify which allowed the programmer to add and change but not delete any files. Venables advised that the only eTreppid employees who had the administrative permissions and passwords to delete files from eTreppid's servers were himself and Montgomery. Venables further advised that all eTreppid servers had the same user name and password for administrative functions which were only known to Montgomery and Venables.

Venables advised that after finding the command prompt on the SRC Server, he looked at the server and found that the ET Latest folder was empty; the ET Development folder was empty except for folders named Jesse and Michael; the ET Programmer folder was empty; and the ET Shared folder contained a few files. Venables then went to the ISA Server and noticed the server was locked up or not functioning; however, he could see it was still on the network but all files had been deleted, including the log files created prior to his leaving on December 21, 2005. Venables tested the ISA Server for approximately two months, 24 hours a day, seven days a week prior to putting it use on December 21, 2005, and had no problems.

Based on Venables' experience, Venables believes that the files were intentionally deleted. Venables advised that if the files were deleted due to a hardware malfunction, selected files would not have been deleted, and files or folder would not be accessible. In addition, Venables advised that he would not have been able to undelete the files if they had not been deleted through a normal delete process. Venables has been able to recover some of the deleted files from the SRC Server and from Montgomery's personal computer using Executive Software undelete function.

00009  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Sloan Sterling Venables, On 02/02/2006, Page 5

Venables estimated it would have taken approximately three days to delete the data contained on the SRC Server.

Venables advised that on January 3, 2006, he went to talk to Montgomery about the SRC Server and again asked Montgomery where the RAID box and server were that he used to back up the SRC Server to which Montgomery said "I'll bring it back, I don't need it anymore".

Venables further advised that on January 3, 2006, Montgomery told him that he (Montgomery) was hiding in the building on December 21, 2005, and saw Patty Gray come back into the office after hours and saw her going around the building deleting things. Montgomery said he had set the alarm and hid out in the building and had Gray on video. Venables knew this was a lie because he (Venables) was in the building until approximately 11:00 P.M., on December 21, 2005, and neither Montgomery nor Gray were in the building. Venables further advised if the alarm been set, it would have activated if someone was in the building.

Venables learned that Montgomery had taken each programmer's hard drive and returned it with the current source folder wiped clean.

Tangirala told Venables that Montgomery took his hard drive while Venables was on vacation. Montgomery told Venables that the hard drive crashed; however, Tangirala told Venables that Montgomery just took the hard drive and gave him (Tangirala) back a blank hard drive with only the master image software on it. Tangirala was working primarily on eTreppid's Automatic Target Recognition software and had been working closely with Montgomery the last few months.

Venables asked Lalith Tenneti and Baljinder Bal when Montgomery started deleting the SRC Server, and both stated that the data on the SRC Server gradually started going away while Venables was on vacation. Tenneti and Bal also informed Venables that Montgomery also started deleting the information from their workstation during the time Venables was on vacation.

Venables found out the Gray had copied some information off of one of the programmer's workstations to present to Trepp and he (Venables) knew that Gray did not have the user name and password to delete information. Venables further advised that Gray was also on vacation from December 22, 2005, until January 3, 2006,

00010  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Sloan Sterling Venables, On 02/02/2006, Page 6

along with Jesse Anderson who was on vacation from December 22, 2005 to January 3, 2006.

Venables advised that he last saw Montgomery on January 10, 2006, when Montgomery was in the eTreppid yelling obscenities at Warren Trepp and Joel Safriet.

Venables advised that on January 10, 2006, he found that all sixteen computers used by eTreppid to record video signals from their video surveillance cameras had stopped recording and further inspection revealed that all recorded data on each machine had been deleted from each of the sixteen computers sometime on January 8, 2006 or January 9, 2006 at approximately 8:00 to 8:30 PM.

Venables advised that he is also the Facility Security Officer and first learned that eTreppid had Secret material in the building when he saw Montgomery placing Secret stickers on hard drives. When Venables asked Montgomery about the Secret material, Montgomery told Venables not to worry about it.

Venables advised that after Montgomery left eTreppid on January 10, 2006, he believed that Montgomery had attempted to access eTreppid's computer system through the Internet; however, he has not been successful.

Venables advised that in past conversations with Montgomery, Montgomery has told Venables that he has storage units in Reno, Nevada, possibly at Double R Storage or Mt. Rose Storage.

Venables advised that Steven Montgomery, the son of Dennis Montgomery, worked at eTreppid on projects for Montgomery involving assembly of hardware components.

Venables advised that Montgomery has a daughter, Kathleen "Katie" Montgomery, who lives [REDACTED] in South Reno.

Venables has known Montgomery to use the following telephones: [REDACTED]



295A-LV-39368

Continuation of FD-302 of Sloan Sterling Venables, On 02/02/2006, Page 7

Venables provided an e-mail message dated January 30, 2006, showing the serial number for the Ultra Store RAID storage unit having serial number 6564737.

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/21/2006

Patty Gray, Asian female, [REDACTED]

[REDACTED] was interviewed by Special Agents John Piser III and Michael A. West at the Reno office of the Federal Bureau of Investigation regarding activities at eTreppid Technologies, LLC.

Gray advised that she has a Master's Degree in Computer Engineering and has been employed by eTreppid for approximately three years and four months. Gray holds the title of Vice President of Product Development with responsibilities for business development and marketing for U.S. Government customers. Gray handles all customer relations to include gathering customer requirements and cost estimates for various products. Gray reports to both Chief Technical Officer Dennis Lee Montgomery and Chairman Warren Trepp.

Gray advised that the main project that she had been working on is a long term project with the Special Operations Command (SOCOM) contract to record video feeds from Predator Drones operating overseas and to develop Automatic Target Recognition software.

Gray advised that in March of 2005, she traveled to Nellis Air Force Base in Las Vegas, Nevada to record test video received from a Predator Drone in a demonstration test to record vehicles, people, and weapons. Personnel at Nellis Air Force Base instructed Gray to label these tapes Secret which Gray did in her own handwriting and affix a red Secret level to five mini DV tapes. Gray advised that the same information was received by eTreppid from Fort Bragg, North Carolina; however, these tapes were marked Unclassified and contained more data than the set of tapes she made at Nellis Air Force Base. Gray advised that all five of the tapes marked Secret are accounted for. Gray further advised that Montgomery would take small segments for test data from these tapes; however, Gray did not know if Montgomery took the test data from the tapes labeled Secret or from the Unclassified tapes.

Gray advised that in June of 2005, this process was again repeated by having test data generated from a Predator Drone which

Investigation on 02/06/2006 at Reno, Nevada

File # 295A-LV-39368

Date dictated \_\_\_\_\_

by SA John Piser III JP/IV  
SA Michael A. West:st/4

00013

Sept. 11' 06



295A-LV-39368

Continuation of FD-302 of Patty Gray, On 02/06/2006, Page 2

Gray called a "fabricated scenario", which produced approximately seven tapes which she labeled with handwritten labels and placed a red Secret sticker on each of these seven tapes. Gray advised that these seven tapes are accounted for.

Gray advised that in November of 2005, eTreppid delivered two servers to SOCOM at Nellis Air Force Base. eTreppid would no longer record the video data on to mini DV tapes and now recorded the video data onto 320 gigabytes hard drives. Gray advised that during this time she would travel to Nellis Air Force Base and start the system recording the data from similar fabricated test scenarios. Gray advised that on one occasion, SOCOM employee Lance Lombardo was supposed to coordinate the activities of the Predator Drone and set up objects to record. On this occasion, Lombardo never showed up and Montgomery instructed Gray to record the data anyway to obtain test data.

Gray advised that when labeling this media, she would prepare a handwritten description on a label which she would place on the hard drive which included the date of the information and which server, Server A or Server B, and then affix a red Secret label to the hard drive. Gray would apply the label and Secret sticker to the outer case of the removable Imclose case but not directly to the hard drive. Gray was instructed by SAIC Contractor Personnel at Nellis Air Force Base to double wrap the hard drives for shipment. Gray identified a red Secret label described as an SF-707 label as being identical to the red Secret label she applied to these hard drives.

Gray advised that the video data she recorded contains dates and times in Zulu time and GPS coordinates in each video frame. Gray kept personal notes regarding what videos were made and would make those available to the FBI.

Gray would send these Secret hard drives via Federal Express to Montgomery in Reno, Nevada. Gray recalled that she made three FedEx shipments, two of which were received and signed for by Montgomery and one was received by another eTreppid employee; however, Gray recalls delivering this package directly to Montgomery upon arriving in Reno, Nevada.

Gray advised that she recorded the information at Nellis Air Force Base onto nine hard drives which she labeled Secret and were all eventually mailed to eTreppid in Reno, Nevada via Federal Express. These nine Secret hard drives along with the Secret Mini

00014  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Patty Gray, On 02/06/2006, Page 3

DV tapes, were stored in a GSA approved container or safe when they were not in use. Gray advised that only she, Montgomery, and Trepp had access to the combination for the safe containing the Secret information with her and Montgomery having the primary access.

Gray advised that on several occasions, she found the entire contents of the safe were gone and would go to Trepp to complain about Montgomery's non-compliance with the security procedures. Trepp would immediately get up from his desk and tell Montgomery to put the Secret material back in the safe and Montgomery would return the Secret items. Gray further advised that Montgomery was the only other employee at eTreppid besides herself that would use the Secret data. Gray advised that she did see other eTreppid employees using tapes with similar content but was unsure if the content was classified. These employees would have received the data from Montgomery.

Gray advised that Montgomery instructed the software engineers or programmers not to talk to her and Montgomery had the engineers afraid that they would be fired and removed from the U.S. if they spoke to Gray. eTreppid employees hires a number of foreign individuals as software engineers.

In December of 2005, Montgomery took the nine Secret hard drives out of the safe and said he was going to condense the nine original hard drives onto six hard drives due to their being unused space on the original nine Secret hard drives. Gray recalled that Montgomery returned six hard drives labeled Secret into the safe along with the original nine Secret hard drives.

Around that same time, Trepp asked Gray to place test data on Mini DV tapes containing segments of day and night operations. Gray advised that Trepp wanted two sets of tapes, one set for Montgomery and one set for Trepp to be used to validate Montgomery's work and to ensure that the results of Montgomery's work was not staged. Gray informed Trepp that because the video segments were only five to seven minutes in length, anyone could train the software to work in a certain way to achieve a specific result for that short time frame. Trepp suggested that Gray made additional tapes for him and place those tapes in a separate drawer in the safe with the combination only being known to Trepp and Gray. Gray prepared four tapes containing Secret data, two of which she placed in the safe only known to her and Trepp and gave the two remaining tapes to Montgomery. Gray advised that the two

00015  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Patty Gray, On 02/06/2006, Page 4

tapes provided to Montgomery are missing, however, the two tapes placed in the safe are accounted for.

Gray advised that Montgomery would store Secret tapes and hard drives in a file cabinet located behind his desk in the warehouse. Gray advised that when she would find the Secret information missing from the GSA approved safe, she would find the tapes or hard drives with Montgomery in the warehouse. Gray recalled that the second to the last time she found these tapes missing, she told Montgomery that he may lose his security clearance if he did not store the Secret material properly. Montgomery told Gray "I will never lose my clearance because they will always want me to do the work". Gray told Trepp of Montgomery's statement and Trepp told her to collect the Secret material and change the combination and not to give the combination to Montgomery. Gray advised that she did as instructed by Trepp and placed the nine Secret original hard drives and the six copies and all Secret mini DV tapes in the safe. Gray recalled that she did this prior to December 18, 2005 and believed that she had placed all classified material in the safe and only she had the combination.

On December 18, 2005, Gray returned home to Arizona and received a number of telephone calls from Trepp and Montgomery. Gray received a number of text messages from Montgomery requesting access to the Secret material in the safe so he could work. Gray received a telephone call from Trepp in which Trepp instructed Gray to give the combination to the safe to Montgomery to let him work and that they would re-secure the data on Monday. Gray advised that she told Trepp that she felt that Montgomery only wanted access to the Secret data to make copies of it so he would not seem to be in non-compliance with security procedures. Upon Gray's return to Reno, she put all the classified material that she had back in the safe that both Trepp and Montgomery had access to and went on vacation from December 21, 2005 to January 3, 2006 in Phoenix, Arizona. Gray felt that she lost control of the classified material and left it up to Trepp and Montgomery to secure the data.

Software Engineer Lalith Tenneti told Gray that before New Years, Montgomery sat down at Tenneti's computer and deleted his source code while Tenneti watched. Montgomery told Tenneti that he didn't need the source code on his work station and Montgomery had a new back up system in place. Gray later found out that Montgomery did this on every engineer's work station.

00016  
Sept. 11' 06

295A-LV-39368

Continuation of FD-302 of Patty Gray, On 02/06/2006, Page 5

Gray advised that Montgomery created an environment that if anyone challenged him they felt they would be fired or deported as the majority of eTreppid's software engineers are foreigners.

Gray felt that Montgomery had extremely poor program management and assigned work to the software engineers that had been promised to customers which had not been complete or yet been assigned. Gray also found out that Montgomery was taking credit for writing code done by others.

Gray informed Trepp that Montgomery claimed to have written 95% of the source code for various eTreppid products and she learned that he had not. In December of 2005, Gray started collecting information about Montgomery's activities and provided this information to Trepp on December 21, 2005, and somehow Montgomery became aware of Gray's efforts. Gray advised that she received a telephone call thirty minutes after having a close door meeting with Trepp from Jesse Anderson. Montgomery told Anderson that Trepp and Gray were ganging up on Anderson and wanted to know if he had any source code on his computer. Gray further advised that Sloan Venables called her on December 21, 2005, and said that Montgomery was leaving the building with a case of hard drives and believed that Montgomery was talked to by Trepp.

Gray further advised that engineers Young Mian and Zehang Sun, who are both from China, may have had access to classified data on their computers. Gray advised that she saw some video content on both their computers which was similar to the classified video content. Gray asked Young Mian where he got the data and Young Mian told her from Montgomery.

Gray advised that after Montgomery left the business on or about January 10, 2006, she and other employees conducted a search of the entire eTreppid office space to locate the nine original Secret hard drives and or their removable enclosures. During the search, an additional copy of the six Secret hard drives were located labeled Secret and were put in the safe; however, the nine original Secret tapes were not located.

Gray provided a chronological list of events occurring at eTreppid related to the Secret hard drives which is attached to and considered a part of this FD-302.

00017  
Sept. 11' 06

Date	Description
11/3/05 – 11/4/05	Traveled from Reno to Nellis AFB to test latest ATR software and gather test data. Generated data on 3 HDDs, marked them all Secret, double-wrapped them and sent them via Fedex to Dennis using Priority Overnight with Saturday delivery. Dennis did receive them on Saturday.
11/7/05	Arrived in Reno and confirmed with Dennis that he had received the data.
11/9/05 – 11/11/05	Traveled from Reno to Nellis AFB to test the latest ATR software and gather additional test data. Generated 5 HDDs, marked them all Secret, double-wrapped them and sent them via Fedex to Dennis using Priority Overnight with Saturday delivery. Dennis did receive them on Saturday.
11/14/05	Arrived in Reno and confirmed with Dennis that he had received the data.
11/17/05 – 11/18/05	Traveled from Reno to Nellis AFB to test latest ATR software and gather test data. Dennis was on vacation 11/18/05 – 11/20/05. The software that I was to test had a bug and no update was sent so 3 HDDs were sent back. Two with the OS and ATR application, one with classified data. The classified material was marked Secret, double-wrapped. All 3 HDDs were sent via Fedex to myself using Overnight for Monday delivery.
11/21/05	Arrived in Reno. Altan Bora signed for the Fedex delivery close to noon. I arrived in the office shortly after noon, and gave the unopened Fedex package to Dennis in the warehouse.
12/5/05	Arrived in Reno shortly after noon. I requested from Zehang Sun and/or Dennis that I get a copy of the latest version of the motion detection software so that I could do some testing. Dennis told Zehang that he would get it to me right away. Zehang told me the latest version was on Yongmian's computer.
12/6/05	Reminded Dennis that I was still waiting for the motion detection software for testing. He continued to promise but I did not receive it. At 3pm, I went to Yongmian's computer (Yongmian was away at a conference) and copied it from his computer onto mine. When I started the application in my office, noticed that it appeared that the test content on Yongmian's computer was classified video. I then checked the safes to find out if the rest of the data was being correctly stored and saw that all of the original hard drives from Nellis were not in the safe. I notified Warren who told Dennis to correct this.
12/7/05	I checked the safes and noticed that the classified content was still not in the safe. I approached Dennis and he said that it was all in the file cabinets in the warehouse. I verbally told him that this was not the correct place to store classified content. I notified Warren that the content was still not being correctly stored.



12/8/05	I sent an email to Dennis and copied Warren to remind him that all classified content should be stored in the safe and asked that he use a particular safe so that we could both have access to it since we both had the combination. As a result, all original classified HDDs and tapes were moved to the safe.
12/12/05	Warren asked me to generate some test tapes from the classified HDDs for internal testing. I sent an email to confirm this since previously Dennis had told me he wanted to use the HDDs, not tapes. Warren requested that I make 4 DV tapes, two for Dennis (one night video, one day) and two for him that he could conduct a blind test with (one night video, one day). I retrieved one of the HDDs (content from 11/5/05) to start looking for which scenes to extract to a tape.
12/13/05	<p>I went to get another HDD to generate more of the test tapes and found that all of the HDDs were missing from the safe again. I alerted Warren and he had Dennis return the content to the safe immediately. I completed the 4 test tapes in the late afternoon using content from the Nellis classified content from 11/5/05 and 11/13/05. I handed two tapes to Dennis. During the time that I was generating the second tape, Dennis came in to put a new label on the HDD that I was using. He said that he was condensing the hard drives I had used at Nellis because some were only partially full.</p> <p>I changed the combination to the top drawer of the safe and secured Warren's two test tapes in that drawer. The rest of the original hard drives were stored in the bottom drawer that Dennis and I both had the combination to.</p>
12/15/05	I went to get a HDD so that I could resume testing the motion detection software. Once again, all of the HDDs were missing from the safe. I went to ask Dennis about this and he said that he wanted to store them in the file cabinet in the warehouse because it was more convenient for him. I told him that this was not the appropriate way to secure the classified content and he was risking losing his clearance. He said "I don't care about my clearance. They'll always give me my clearance because they want me to do the work." I reported this to Warren and he agreed that access to the classified material needed to be restricted. He had Dennis immediately return all of the classified HDDs and tapes to the safe and then instructed me to move all of the classified material in the top drawer of the safe and not give the combination to Dennis.

12/18/05	Dennis tried to contact me by text message. Warren eventually made contact with me by cell phone and told me to provide the combination to Dennis so that he could access the classified material. I told Warren that I suspected that Dennis would make copies of the content and that he would also have access to the two tapes that Warren wanted for the blind testing. He still wanted me to provide Dennis with the combination and we would talk to him and re-secure everything when I got back into the office on Monday.
12/20/05	I sent a note to Warren that indicating that I was not comfortable being responsible for securing the content because I was suspicious that Dennis had made copies of all of the content.
12/21/05	I met with Warren to discuss several issues including that I had seen what appeared to be classified content on Zehang's shared folder on his computer. As I was trying to copy it over to my system, it got deleted. I left for my vacation at 6:35a on 12/22/05.
1/8/06	Lalith told me that Dennis had deleted all of the source code from his and the other engineers's systems between Christmas and New Year's. I arranged to have him talk to Warren about this.
1/9/06	We began looking for source code on any hard drive in the building. I found seven HDDs in his file cabinet that were copies of the original 9 Nellis HDDs. When I checked the safe, another copy of the original 9 Nellis HDDs were there (condensed to seven HDDs) but the originals were missing. In addition, two of the four tapes generated per Warren's request on 12/12/05 were also missing.
1/10/06 -- 1/13/06	A search of the work and storage areas in the building did not result in locating the missing classified material.
1/23/06	I checked one of the HDDs that Dennis had generated to see what was on it. It was labeled "Nellis Images WIP 12/8/05". On it was a recent version of the target detection/motion detection software and test imagery. I asked Yongmian to describe the test sequences that he had been using. His description matches the test sequences in the two directories on this HDD that contain the detection software. At least one of the test sequences is from classified material. However, without showing Yongmian the sequence, I cannot be positive that the test sequence he had access to and the imagery on this HDD are the same.

FD-302 (Rev. 10-6-95)

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/13/2006

Neil Azzinaro

[REDACTED]

was interviewed by Special Agents John Piser III and Michael A. West regarding Dennis Lee Montgomery.

Azzinaro is an independent casino host who periodically works in Reno, Nevada, where he met Warren Trapp and Dennis Montgomery in approximately 1999 or 2000.

Azzinaro advised that in the first of January 2006, he called Montgomery to discuss a home computer problem with Montgomery. Azzinaro knows Montgomery to have extensive knowledge of computer and Montgomery has helped Azzinaro resolve problems in the past.

During this telephone call, Azzinaro asked how Montgomery was doing. Montgomery advised that things were not going well for him, that he made Warren Trepp eleven million dollars last year, recently asked Trepp for a raise, and Trepp would not give him one. Montgomery commented that he was aware that Azzinaro knew a lot of people through the casino business and wanted to find someone with ten to eleven million dollars. Montgomery advised this individual could only be from this country, not from a corporation, and has to be a private party. Montgomery told Azzinaro he wanted to start his own business.

Azzinaro told Montgomery that he would look around.

Azzinaro commented that during this telephone conversation, Montgomery sounded very revengeful and reiterated that he made a lot of money for Trepp and Trepp owes him. Montgomery stated on more than one occasion during this conversation that he made Trepp eleven million dollars and he got nothing.

Azzinaro is aware that Montgomery gambles large sums of money and on occasions has borrowed ninety thousand dollars from a casino and lost the ninety thousand dollars. Montgomery paid the money back the next day which Azzinaro found to be odd as most high stakes gamblers don't repay their debts immediately. Azzinaro was

Investigation on 02/06/2006 at Reno, Nevada

File # 295A-LV-39368

Date dictated 02/09/2006

by SA John Piser III  
SA Michael A. West:st

00021

Sept. 11' 06



FD-302a (Rev. 10-6-95)

295A-LV-NEW

Continuation of FD-302 of Neil Azzinero, On 02/06/2006, Page -2-

also aware of an occasion when Montgomery had a three hundred thousand dollar outstanding credit bill with Nevada casino on which he immediately paid two hundred thousand dollars.

00022  
Sept. 11' 06

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/21/2006

Sloan Venables, Director of Research and Development, eTreppid Technologies, LLC, 755 Trademark Drive, Reno, Nevada, telephone number (775) 337-6771, voluntarily provided Special Agent Michael A. West with one Supermicro Central Processing Unit, no serial number, containing dual Xeon processors, a X5DAE motherboard, and two internal hard drives removed from eTreppid's video surveillance system.

Venables was provided a copy of a FD-597, "Receipt for Property" which was placed in the 1A section of the case file.

Investigation on 02/8/2006 at Reno, Nevada

File # 295A-IV-39368

Date dictated 02/21/2006

by SA Michael A. West:maw

00023

Sept. 11' 06

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/23/2006

Patty Gray, Vice President of Product Development, eTreppid Technology, LLC, 755 Trademark Drive, Reno, Nevada, telephone number (775) 337-6771, provided the attached inventory of classified material maintained at eTreppid Technology, LLC.

Investigation on 02/14/2006 at Reno, Nevada

File # 295A-LV-39368

Date dictated 02/23/2006

by SA Michael A. West:maw

00024

Sept. 11' 06

#	Date of material	Dispatch/ Receipt	Date of D/R	Classification	Unclassified description of material	ID of activity (contract #/recipient)
1	3/15/05	R	3/15/05	Secret	Mini-DV Tape labeled Tape 1 EO 10K, 7.5K 5K altitude 3/15/05	SOCOM USZA26-03-P-3294
2	3/15/05	R	3/15/05	Secret	Mini-DV Tape labeled Tape 1 0330 IR&EO, No targets 3/15/05	SOCOM USZA26-03-P-3294
3	3/15/05	R	3/15/05	Secret	Mini-DV Tape labeled Tape 2 IR 3-15-05 10K, 7.5K, 5K	SOCOM USZA26-03-P-3294
4	3/15/05	R	3/15/05	Secret	Mini-DV Tape labeled Short Test Clip	SOCOM USZA26-03-P-3294
5	6/3/05	R	6/3/05	Secret	Mini-DV Tape labeled Gold #97 White #88 Purple #80 POCN 03JUN05	SOCOM USZA26-03-P-3294
6	6/3/05	R	6/3/05	Secret	Mini-DV Tape labeled Orange #76 GCS 7 Night 03JUN05	SOCOM USZA26-03-P-3294
7	6/3/05	R	6/3/05	Secret	Mini-DV Tape labeled Red-75 ORA-81 6/3/05	SOCOM USZA26-03-P-3294
8	6/3/05	R	6/3/05	Secret	Mini-DV Tape labeled 12.5K Orange #76 Night 03JUN05	SOCOM USZA26-03-P-3294
9	6/3/05	R	6/3/05	Secret	Mini-DV Tape labeled Orange GCS 7 #78 Day Nellis IR/EO 03JUN05 2330PM	SOCOM USZA26-03-P-3294
10	6/3/05	R	6/3/05	Secret	Mini-DV Tape labeled Orange #76 03JUN05 Day	SOCOM USZA26-03-P-3294
11	6/3/05	R	6/3/05	Secret	Mini-DV Tape labeled Orange #76 03JUN05 Day	SOCOM USZA26-03-P-3294
12	11/4/05	MISSING	12/12/05	Secret	Mini-DV Tape labeled Tape 1 11/4/05 IR	SOCOM USZA26-03-P-3294
12	11/4/05	R	12/12/05	Secret	Mini-DV Tape labeled Tape 2 11/4/05 IR	SOCOM USZA26-03-P-3294
13	11/10/05	R	11/10/05	Secret	Mini-DV Tape labeled GCS 11 #125 IR 11/10/05	SOCOM USZA26-03-P-3294
14	11/10/05	R	11/10/05	Secret	Mini-DV Tape labeled GCS 6 #61 11/10/05 IR	SOCOM USZA26-03-P-3294
15	11/10/05	R	11/10/05	Secret	Mini-DV Tape labeled GCS 10 #119 11/10/05 IR Tape 1(A)	SOCOM USZA26-03-P-3294
16	11/10/05	R	11/10/05	Secret	Mini-DV Tape labeled GCS 6, #61 to GCS 11 #125 IR 11/10/05	SOCOM USZA26-03-P-3294

17	11/13/05	MISSING	12/13/05	Secret	Mini-DV Tape labeled Tape 3 11/13/05 Day	SOCOM USZA26-03-P-3294
17	11/13/05	R	12/13/05	Secret	Mini-DV Tape labeled Tape 4 11/13/05 Day	SOCOM USZA26-03-P-3294
18	11/4/05	MISSING	11/4/05	Secret	HDD labeled 11/4/05 Nellis	SOCOM USZA26-03-P-3294
19	11/4/05	MISSING	11/4/05	Secret	HDD labeled 11/4/05 Nellis	SOCOM USZA26-03-P-3294
20	11/4/05	MISSING	11/4/05	Secret	HDD labeled 11/4/05 Nellis	SOCOM USZA26-03-P-3294
21	11/10/05	MISSING	11/10/05	Secret	HDD labeled 11/10/05 Nellis	SOCOM USZA26-03-P-3294
22	11/10/05	MISSING	11/10/05	Secret	HDD labeled 11/10/05 Nellis	SOCOM USZA26-03-P-3294
23	11/10/05	MISSING	11/10/05	Secret	HDD labeled 11/10/05 Nellis	SOCOM USZA26-03-P-3294
24	11/11/05	MISSING	11/11/05	Secret	HDD labeled 11/11/05 Nellis	SOCOM USZA26-03-P-3294
25	11/11/05	MISSING	11/11/05	Secret	HDD labeled 11/11/05 Nellis	SOCOM USZA26-03-P-3294
26	11/12/05	MISSING	11/12/05	Secret	HDD labeled 11/12/05 Nellis	SOCOM USZA26-03-P-3294
27	11/4/05	R	12/7/05	Secret	Hard Disk Drive labeled Nellis 11/04/05 MPG RAW	SOCOM USZA26-03-P-3294
28	11/11/05	R	12/7/05	Secret	Hard Disk Drive labeled Nellis 11/11/05 MPG RAW	SOCOM USZA26-03-P-3294
29	11/11/05	R	12/7/05	Secret	Hard Disk Drive labeled Nellis 11/4/05 - 11/11/05 MPG RAW	SOCOM USZA26-03-P-3294
30	11/4/05 - 11/12/05	R	12/7/05	Secret	Hard Disk Drive labeled Nellis 11/04/05 - 11/12/05 MPG RAW A	SOCOM USZA26-03-P-3294
31	12/04 - 04/05	R	12/7/05	Secret	Hard Disk Drive labeled SOCOM 12/04 - 04/05 B	SOCOM USZA26-03-P-3294
32	12/04 - 04/05	R	12/7/05	Secret	Hard Disk Drive labeled SOCOM 12/04 - 04/05 A	SOCOM USZA26-03-P-3294
33	12/8/05	R	12/8/05	Secret	Nellis Images WIP 12/8/05	SOCOM USZA26-03-P-3294
34	11/4/05 - 11/12/05	R	12/19/05	Secret	Hard Disk Drive labeled Nellis 11/4/05 - 11/12/05 MPG RAW B	SOCOM USZA26-03-P-3294
35	12/8/05	Destroyed	1/11/06	Secret	Hard Disk Drive labeled Nellis Images WIP 12/8/05 B	DoD 7-pass delete and wipe
36	11/4/05 - 11/11/05	R	12/19/05	Secret	Hard Disk Drive labeled Nellis 11/4/05 - 11/11/05 MPG RAW B	SOCOM USZA26-03-P-3294
37	11/11/05	R	12/19/05	Secret	Hard Disk Drive labeled Nellis 11/11/05 MPG RAW B	SOCOM USZA26-03-P-3294
38	03/05-06/05	Destroyed	1/19/06	Secret	Hard Disk Drive labeled Lance Prod 03/05-06/05 B	DoD 7-pass delete and wipe

39	7/7/05-7/10/05	R	12/19/05	Secret	Hard Disk Drive labeled Lance Data	SOCOM USZA26-03-P-3294
40	06/05-07/05	R	12/19/05	Secret	Hard Disk Drive labeled Lance Prod	SOCOM USZA26-03-P-3294

41 03/05-04/05 R  
 42 04/05-07/05 R

Secret Hard Disk labeled Certificate 03/05 - 04/05 A  
 Secret Hard Disk labeled Certificate 04/05 - 07/05 A

43 R  
 44 R  
 45 R  
 46 R  
 47 R  
 48 R  
 49 R  
 50 R  
 51 R

Secret Mini DV Webcam 6/26 - 6/27 Beacon Track Download  
 Mini DV 1850 N 04 ORS Big Red Tape 2  
 Mini DV 04 Mary Patterson Hostate loc  
 Mini DV 12 Mary Patterson ORS Garrison/Later  
 Mini DV Redington  
 Mini DV Redington  
 Mini DV 31 Dec 03  
 Mini DV Camp I  
 Mini DV Camp II

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/23/2006

Sloan Sterling Venables, Director of Research and Development and Facility Security Officer, eTreppid Technology, LLC, 755 Trademark Drive, Reno, Nevada, telephone number (775) 337-6771, provided the attached documents relating to Security Clearances of Chief Technical Officer Dennis Lee Montgomery:

Standard Form 312, "Classified Information Nondisclosure Agreement", signed and dated September 16, 2003, by Dennis Lee Montgomery, [REDACTED]

Department of the Army, U.S. Army Security Operations Training Facility, Post Office Box 70660, Fort Bragg, North Carolina, "Security Briefing" Form, briefed and signed on August 25, 2003, by Dennis Montgomery, [REDACTED]

Department of Security Services, Investigation Summary, for Dennis Lee Montgomery.

Department of Defense, Letter of Consent, National Industrial Security Program, Clr Date, May 7, 2003, to Dennis Lee Montgomery, [REDACTED]

Investigation on 02/14/2006 at Reno, Nevada

File # 295A-LV-39368

Date dictated 02/23/2006

by SA Michael A. West:maw

00028

Sept. 11' 06

---

**CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT**


---

 AN AGREEMENT BETWEEN DENNIS MONTGOMERY AND THE UNITED STATES
 

---

 (Name of Individual — Printed or typed)
 

---

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, \*952 and 1924, Title 18, United States Code, \*the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)



10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE 	DATE 9/16/03	SOCIAL SECURITY NUMBER (See Notice below) [REDACTED]
---------------	-----------------	--

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)  
(Type or print)

ETREPAD TECHNOLOGIES, LLC  
755 TRADEMARK DR  
RENO, NV 89521

305Xφ

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE 	DATE 16 Sept 03	SIGNATURE 	DATE 16 Sept 03
NAME AND ADDRESS (Type or print) Defense Security Inc. (S41194) 4349 Duffer Drive Nellis AFB, NV 89151		NAME AND ADDRESS (Type or print) SAME	

**SECURITY DEBRIEFING ACKNOWLEDGEMENT**

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

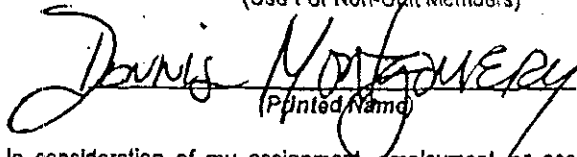
\*NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

00030

DEPARTMENT OF THE ARMY  
U. S. MY SECURITY OPERATIONS TRAINING FACILITY  
POST OFFICE BOX 70660  
FORT BRAGG, NORTH CAROLINA 28307-5000

### SECURITY BRIEFING

(Use For Non-Unit Members)

  
(Printed Name)

I understand that in consideration of my assignment, employment, or association with the Security Operations Training Facility (SOTF), I may be granted access, if properly authorized or security cleared, to information, material, and plans which concern the security of the United States of America and which are either sensitive or classified by the order of the President or as authorized by statute.

1. I agree that I will never divulge, publish, or reveal by writing, word, conduct, or otherwise, to any unauthorized person, any classified or sensitive information relating to the SOTF Facility / Project, its personnel, fiscal data or security measures without prior consent of the Director, SOTF or his designated security representative.

2. I agree that the burden is upon me to ascertain whether or not information is sensitive or classified, and, if so, who is authorized to receive it. I will, therefore, obtain the decision of the authorizing officials of the SOTF Security Office on these matters before disclosing such information.

3. I agree to submit information for review by the SOTF Security Office, prior to discussing with or showing to any publisher, literary agent, architectural firm, or other unauthorized persons, all manuscripts, articles, speeches, resumes, and all architectural design drawings and papers, written or drawn by me or in conjunction with others, which contain or are derived from information or material obtained by virtue of my assignment, employment or association with this facility or project. I agree that the purpose of such review is to ensure that no sensitive or classified information or material obtained by virtue of my assignment, employment or association with this facility/project is contained therein. I further understand that such review shall not constitute nor shall be represented as a verification of factual accuracy or an endorsement of the opinions contained in any such manuscripts, articles, speeches, resumes, advertisements or papers.

4. I agree that all classified or sensitive information acquired by me in connection with my assignment, employment or association with this facility/project remains the property of the Government of the United States of America, and I must surrender, upon demand by the Director, SOTF or his Security Representatives, any material in my possession relating to such information.

5. I agree to report, without delay, to my superiors or the Security Manager, the details or circumstances of any case which comes within my knowledge wherein an unauthorized person has obtained or is attempting to obtain classified or sensitive information or material, or wherein such information or material may be or is being disclosed or removed in an unauthorized manner.

6. I agree that my compliance with all the obligations required to protect classified and/or sensitive information may be a consideration of my continuing assignment, employment or association with this facility/project. I understand that any failure to so comply may subject me to administrative action including termination of my assignment, employment or association with this facility/project.

( Continued on Reverse )

**SECURITY BRIEFING**  
(Use For Non-Unit Members)

(Continued from front page)

7. I understand that the provisions of the Espionage Act apply during my assignment, employment or association with the SOTF. I have been made aware and understand that the provisions of the Espionage Act, Sections 793, 794, and 798, of Title 18, United States Code provide penalties for any violation of the Espionage Act.

8. I have read and understand the contents of this briefing. I have been made aware and understand that Section 1001 of Title 18, United States Code provides information on the penalties involved in the making of false, fictitious, or fraudulent statements or representations.

Person Conducting the Briefing:

Date: 8/26/03

MICHAEL S ALLEN  
Printed Name

N/A  
Social Security Number

CDI (910) 907-5120  
Section Phone Number

[Signature]  
Signature

Person being briefed:

Date: 8/25/03

Donnis Montgomery  
Printed Name

[Redacted]  
Social Security Number

STRASIT  
Organization

[Signature]  
Signature

NOTICE: The PRIVACY ACT, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that the authority for soliciting your Social Security Account Number (SSAN) is Executive Order 8397. Your SSAN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above. While the disclosure of your SSAN is not mandatory, your failure to do so may delay the processing of such certification.

**Person Summary**

**MONTGOMERY, DENNIS LEE**

Person Category Industry (KMP) 3C5X0-I

Open Investigation: N/A  
 PSQ Sent Date: N/A  
 Attestation Date: N/A  
 Incident Report: 2006 01 20  
 SF 713 Fin Consent Date: N/A  
 SF 714 Fin Disclosure Date: N/A  
 Polygraph: N/A  
 Foreign Relation: N/A

Marital Status: N/A  
 Place of Birth: Arkansas  
 Citizenship: U.S. Citizen  
 NdA Signed: No  
 NdS Signed: No

PSQ Sent  
 Non-SCI Access History

Request to Research/Upgrade Eligibility

**Accesses**

Category	PSP	Suitability and Trustworthiness
Industry (KMP) 3C5X0-I Access Suspended	No	IT: N/A Public Trust: N/A Child Care: N/A

**Person Category Information**

Category Classification: KMP

Organization: 3C5X0-I, ETREPPID TECHNOLOGIES, LLC, 755 Trademark Drive, Reno, NV, 89521

Organization Status: Top Secret, ACTIVE, 2005 06 01

Occupation Code: N/A

Separation Date: N/A

SCI SMO: W4VYAA - INSCOM MISSION SPT CMD, Level 2, 703-706-1352, Alt phone for SSO INSCOM: (703) 706-1768/2520 or (703) 428-4376. FOR CONTRACTOR CLEARANCE ISSUES CONTACT THE CONTRACTOR SUPPORT ELEMENT (CSE) AT: (301) 677-6982; (301) 677-4628 OR (301) 677-4622

Non-SCI SMO: ETREPPID TECHNOLOGIES, LLC, Level 4, 775-337-6771 X 14,

Servicing SMO: No

Office Symbol: N/A

Grade: N/A

Position Code: N/A

PS: N/A

Arrival Date: N/A

RNLTD: N/A

Office Phone Comm: N/A

Office Phone DSN: N/A

Separation Status: N/A

TAFMSD: N/A

Interim: N/A

Proj. Departure Date: N/A

Proj. UIC/RUC/PASCODE: N/A

Report Incident

In/Out Process

Remarks

Suspense Data

**Investigation Summary**

Investigation History

SSBI from DSS, Opened: 2003 04 04 Closed 2004 02 13

NAC from DSS, Opened: Closed 2003 04 29

00033

Sept. 11 '06

# Incident Report Update Notification

Records 1 - 1 of 1, Page 1 of 1

SSN	Name	Person Category	Incident Date	Incident Status	Incident Criteria	Expand Incident	Remove From Display
[REDACTED]	MONTGOMERY, DENNIS LEE	Industry	2006 01 20	Initial	Personal Conduct, Emotional, Mental and Personality Disorders, Criminal Conduct, Security Violations, Misuse of Information Technology Systems	<input type="checkbox"/>	<input type="checkbox"/>

Records 1 - 1 of 1, Page 1 of 1

**Notice:** Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.

**Person Summary**

**MONTGOMERY, DENNIS LEE**

Eligibility: SCI - DCID 6/4, 2005 10 06, AFCAF  
 Investigation: SSBI, 2004 02 13, DSS  
 Open Investigation: N/A  
 Date PSQ Sent: N/A  
 Incident Report: N/A  
 Polygraph: N/A  
 Foreign Relation: N/A

Place of Birth: Arkansas  
 Citizenship: U.S. Citizen  
 Marital Status: N/A  
 NdA Signed: No  
 NdS Signed: No  
 Attestation Date: N/A

PSQ Sent  
Non-SCI Access History

Request to Research/Upgrade Eligibility

**Person Category** Industry (KMP) 3C5X0-I

**Category Classification:** KMP

**Organization:** 3C5X0-I, ETREPPID TECHNOLOGIES, LLC, 755 Trademark Drive, Reno, NV, 89521

**Organization Status:** Top Secret, ACTIVE, 2005 06 01

**Occupation Code:** N/A

**Office Symbol:** N/A

**Position Code:** N/A

**Grade:** N/A

**Arrival Date:** N/A

**PS:** N/A

**Office Phone Comrn:** N/A

**Office Phone DSN:** N/A

**Separation Date:** N/A

**RNLTD:** N/A

**Separation Status:** N/A

**TAFMSD:** N/A

**Interim:** N/A

**Proj. Departure Date:** N/A

**PSP:** No

**Proj. UIC/RUC/PASCODE:** N/A

**SCI SMO:** N/A

**Non-SCI SMO:** ETREPPID TECHNOLOGIES, LLC, Level 4, 775-337-6771 X 14,

**Servicing SMO:** No

Report Incident

In/Out Process

Remarks

Suspense Data

Non-SCI Access		SCI Access
US: N/A	NATO: N/A	SPA: N/A
CNWDI: N/A	SIOP: N/A	Access: No
PRP: N/A	Restricted Data: N/A	
SIGMA 16: N/A		
IT: N/A	Public Trust: N/A	Child Care: N/A
	Indoctrinate	

**Investigation Summary**

SSBI from DSS, Opened: 2003 04 04 Closed 2004 02 13  
 NAC from DSS, Opened: Closed 2003 04 29

Investigation History 00035

Sept. 11' 06

### Person Summary

MONTGOMERY, DENNIS LEE

Eligibility: Top Secret, 2004 02 21, DISCO  
Investigation: SSBI, 2004 02 13, DSS  
Open Investigation: NLC, 2003 04 04, DSS  
Date EPSQ Sent: N/A  
Incident Report: N/A  
Polygraph: N/A  
Foreign Relation: N/A

Place of Birth: Arkansas  
Citizenship: U.S. Citizen  
NdA Signed: No  
NdS Signed: No  
Attestation Date: N/A

#### Person Category

Industry (KMP) 3C5X0-I

Category Classification: KMP

Organization: 3C5X0-I, ETREPPID TECHNOLOGIES LLC, 755 Trade Mark Drive, Reno, NV, 89521

Occupation Code: N/A  
SA: N/A  
Arrival Date: N/A  
Office Phone Comm: N/A  
Separation Date: N/A  
Separation Status: N/A  
Interim: N/A  
PSP: No  
SCI SMO: N/A  
Non-SCI SMO: N/A  
Servicing SMO: No

Office Symbol: N/A  
Grade: N/A  
PS: N/A  
Office Phone DSN: N/A  
RNLTD: N/A  
TAFMSD: N/A  
Proj. Departure Date: N/A  
Proj. UIC/RUC/PASCODE: N/A

Report Incident

In/Out Process



US: N/A  
CNWDI: N/A  
PRP: N/A  
SIGMA 16: N/A

NATO: N/A  
SIOP: N/A  
Restricted Data: N/A

SPA: N/A  
Access: No

IT: N/A      Public Trust: N/A      Child Care: N/A

#### Investigation Summary

SSBI from DSS, Opened: 2003 04 04 Closed 2004 02 13  
NAC from DSS, Opened: Closed 2003 04 29

#### Adjudication Summary

PSI Adjudication of SSBI DSS, Opened 2003 04 04, Closed 2004 02 13, determined Eligibility of Top Secret on 2004 02 21 DISCO

PSI Adjudication of NAC DSS, Opened , Closed 2003 04 29, determined Eligibility of Interim Top Secret on 2003 12 29 DISCO

---

**External Interfaces**

Perform SII Search

DCII

---

**Notice:** Under the Privacy Act of 1974, you must safeguard personnel information retrieved through this system. Disclosure of information is governed by Title 5, United States Code, Section 552a Public Law 93-579, DoDD 5400.11, DoDR 5400.11-R and the applicable service directives.





VENABLES confirmed he and SUBJECT were the only employees with the administrator password necessary to access the SRCSERVER and ISASERVER, therefore they were the only two employees who could have deleted the Source Code. VENABLES denied deleting the Source Code.

VENABLES said that only the individual programmers and SUBJECT had the passwords necessary to delete the Source Code from the individual workstations. VENABLES further said the passwords on the workstations were established and set by SUBJECT. VENABLES said he established his own password on his workstation; therefore his information was not deleted. Additionally, SUBJECT had the building alarm codes for all of the company employees. VENABLES said SUBJECT possessed the necessary accesses and passwords to access the surveillance cameras within the facility and could have deleted the last four months worth of video recordings.

VENABLES said he would attempt to obtain the workstation motherboard and RAID controller serial numbers for the equipment SUBJECT took home.

VENABLES was aware SUBJECT had several storage units around the Reno, NV area. He believed that SUBJECT often used different storage unit locations. He was unaware of the specific locations of these storage units.

VENABLES provided a copy of SUBJECT's signed CLASSIFIED INFORMATION DNONDISCLOSURE AGREEEMNET (Attachment 20), Standard Form 312, and signed by SUBJECT on 16 Sep 2003.

I. (U) Interview of: GRAY  
Date/Place: eTreppid/24 JAN 2006  
Asst Interviewer: SA Smith  
Associated Exhibit Numbers:

---

GRAY stated that she has been employed by eTreppid for approximately three years and four months. She indicated that she has known SUBJECT for a little more than six years; three of those years were prior to employment with ETREPPID, as she had done some work with eTreppid when she was employed by INTEL CORPORATION. GRAY stated that she came to work for eTreppid because she believed that she could help bring its products to the marketplace.

GRAY stated eTreppid was awarded a contract from US Special Operations Command, Fort Bragg, NC, to develop Automatic Target Recognition. The contract was awarded on 12 March 2003 and required the company to have access to SECRET material at other contractor and government locations.

On 1 August 2005, US SOCOM amended the Department of Defense Contract Security Classification Specification, DD Form 254, permitting eTreppid to have storage and Automated Information System processing at the facility.

00119  
Sept. 11' 06

During the period of 9-18 Nov 2005, GRAY recorded SECRET predator video images onto nine eTrepid hard drives. The video images were recorded at the predator operations center, Nellis AFB, NV. Upon completion of the recordings, GRAY was instructed by contractor personnel (NFI) to mark the hard drives with a SECRET sticker, which she did. GRAY subsequently mailed the hard drives to eTrepid. The hard drives were stored at eTrepid in a GSA approved safe in a room secured by a cipher lock.

GRAY related that on 06 Dec 2005 she discovered that the nine SECRET hard drives were not in the GSA approved safe at eTrepid's office. GRAY said she and SUBJECT were the only two employees with the safe combination; therefore she suspected SUBJECT had the SECRET hard drives. She notified TREPP who, in turn, informed SUBJECT to return the hard drives to the safe. GRAY again checked the safe on 7 Dec 2005 and found that the hard drives were once again missing. GRAY asked SUBJECT about the location of the SECRET hard drives and SUBJECT told her that they were all in the file cabinet in the warehouse. GRAY informed SUBJECT that this was not the correct location to store the hard drives and informed TREPP of the incident. GRAY was uncertain if SUBJECT returned the SECRET hard drives to the safe.

On 8 Dec 2005, GRAY e-mailed SUBJECT, copying TREPP on the e-mail to remind SUBJECT that all classified material should be stored in one safe. GRAY said that as a result of this e-mail all original nine original SECRET hard drives were returned to the safe.

GRAY said that on 12 Dec 2005, TREPP asked her to generate some test tapes for internal testing from the nine SECRET hard drives. TREPP requested that four DV tapes be made, two for SUBJECT and two for TREPP. TREPP wanted the two tapes so he could perform a "blind test." GRAY retrieved one of the nine SECRET hard drives used for classified recording and started making copies for TREPP.

GRAY related that on 13 Dec 2005, when she went to retrieve another hard drive she discovered that once again the nine SECRET hard drives were missing. GRAY informed TREPP that the nine SECRET hard drives were not properly stored. TREPP had SUBJECT return the hard drives to the safe. GRAY also related that while generating test tapes, SUBJECT came into her work area and placed a new label on one of the hard drives that she was using to generate test tapes. GRAY said that SUBJECT told her he was condensing the original nine SECRET hard drives that were used at Nellis AFB because some were only partially full. As per TREPP, GRAY also gave SUBJECT two SECRET test tapes.

GRAY changed the safe's upper drawer combination and placed TREPP's two copies of test tapes into this drawer. The original nine SECRET hard drives were secured in the safe's bottom drawer, to which both GRAY and SUBJECT had the combination.

GRAY related that on 15 Dec 2005, she discovered that all of the SECRET hard drives were once again missing from the safe. When GRAY approached SUBJECT about the SECRET hard drives he told her he wanted to store the hard drives in the file cabinet in the warehouse for his convenience. GRAY told SUBJECT he could not store the SECRET hard drives in the warehouse and was risking losing his clearance. GRAY said SUBJECT replied, "I don't care about my clearance. They'll always give me my clearance because they want me to do the work." GRAY informed TREPP about the incident and he determined that the classified material needed to be restricted. TREPP had SUBJECT return the SECRET hard drives and tapes to the safe. GRAY said TREPP then asked her to move all of the classified material to the top drawer of the safe and not give SUBJECT the combination. GRAY complied.

GRAY said that on 18 Dec 2005, SUBJECT tried to contact her via text message, but she did not respond. Eventually she was contacted by TREPP who instructed her to give the top drawer safe combination to SUBJECT. GRAY related to TREPP that she had concerns that SUBJECT would make copies of the classified material he would have access to the two SECRET tapes that GRAY had segregated for the blind test. GRAY said that TREPP instructed her to give SUBJECT the combination so SUBJECT could perform work. TREPP told her to change the combination when she returned from the weekend. GRAY said that TREPP said he would speak with SUBJECT and have him re-secure the SECRET hard drives and tapes when she returned on 19 Dec 2005.

GRAY said that on 21 Dec 2005, at approximately 1030 hours, she had a closed door meeting with TREPP where she told TREPP that she had reason to believe SUBJECT had not written significant software for the company. She also speculated that she observed what may have been classified imagery on a computer used by Zehang SUN, programmer, eTreppid, who is a Chinese National. GRAY said the images appeared to be predator aerial images taken in Iraq from the predator and displayed the geo-coordinates. She said that she was told Mr. Lance Lombardo, Program Manager, US SOCOM, that any images reflecting the geo-coordinates were classified SECRET. GRAY said she tried to copy what appeared to be the classified content from SUN's shared folder. But, as she was trying to copy it to her computer the file was deleted. GRAY believed that SUBJECT deleted it because SUBJECT learned of her conversation with TREPP and because SUBJECT was allowed access to all of the engineer's folders. GRAY also informed TREPP that she had fairly complete information that led her to believe SUN had worked on a classified project involving ocean images.

These ocean images were later determined by the U.S Government to be unclassified.

GRAY stated that soon after her meeting with TREPP she received a call from JESSE ANDERSON, programmer, eTreppid asking her what was going on in the building. ANDERSON told GRAY that he had just received a call from SUBJECT who told him that TREPP and GRAY were "ganging up on him." ANDERSON also told GRAY that SUBJECT asked if any Source Code was resident on ANDERSON's computer. GRAY told him that she didn't know what he was talking about and her conversations with TREPP were private. GRAY said that almost immediately after her conversation with ANDERSON, VENABLES called her on the office intercom and said he just received call from SUBJECT who told him that TREPP and GRAY were "ganging up on him" and accusing VENABLES of "stuff" (NFI).

GRAY believed that her conversation with TREPP earlier in the day was either overheard or somehow monitored. GRAY informed TREPP of her conversations with ANDERSON and VENABLES and of her belief that their conversation had been monitored. GRAY said VENABLES called at approximately 1530 hours on the office intercom and inquired as to why SUBJECT was leaving the building with hard drives. GRAY told TREPP about VENABLES call. She and TREPP went to the company's warehouse and GRAY observed TREPP and SUBJECT engage in a conversation. She was not privy to the conversation.

GRAY said that on 8 Jan 2006, LALITH TENNETI, software engineer, eTreppid told GRAY that eTreppid's Source Code was deleted from all of the engineer's systems between Christmas 2005 and New Year's 2006.

GRAY said that on 9 January 2006 she found 7 hard drives, which were copies of the original nine SECRET hard drives, in SUBJECT's file cabinet in the warehouse. GRAY stated an inspection of the safe revealed another 7 hard drives, also copies of the original nine SECRET hard drives. GRAY said a search of eTreppid's facility failed to locate the original nine SECRET hard drives. GRAY said that she knows the original 9 SECRET hard drive disks were missing because the hard drives at ETREPPID offices are not the original ones which she "personally placed descriptive labels on" in Nov 2005. Furthermore, GRAY related that the nine missing SECRET hard drives had actual Predator missions on them. In addition to the nine missing SECRET hard drives, GRAY related that 2 of the 4 SECRET test tapes made for the blind test were missing from the safe. GRAY stated that between 9 Jan and 13 Jan 2006 she and the rest of the company's employees searched the company for the nine original SECRET hard drives and two SECRET test tapes but were unable to locate them. GRAY was unable to explain the disappearance of the hard drives but knows she does not have them and the only other person with access to the missing original nine SECRET hard drives was SUBJECT.

GRAY also added that she believes SUBJECT processed classified information on an unclassified stand-alone system that was not part of eTreppid's computer network/domain. She suspected this, because SUBJECT had to use a computer system to make copies of the nine original SECRET hard drives and the company did not have approval to process classified information on any system.

J. (U) Interview of: ANDERSON  
Date/Place: eTreppid  
Asst Interviewer: SA Smith  
Associated Exhibit Numbers:

ANDERSON said he was an employee of eTreppid for approximately five years and had both a personal and professional relationship with SUBJECT. ANDERSON stated that he, SUBJECT and other employees met each other socially on numerous occasions. ANDERSON characterized SUBJECT's recent demeanor as "unstable, needs to be hospitalized and needs psychological help."

ANDERSON stated that on 22 or 23 Dec 2005 SUBJECT called him and asked if he had any Source Code resident on his computer. ANDERSON told him he did not. ANDERSON said that this call took place when he was on vacation 21-28 Dec 2005. ANDERSON said that he called GRAY and said, "Dennis (SUBJECT) just called me and asked if I had any Source Code on my computer, what's going on?" ANDERSON said that he could not recall GRAY's response.

*Handwritten:* SA Smith  
DELETED

ANDERSON said that on 28 or 29 Dec 2005, TENNETI informed him that eTreppid Source Code was missing from his eTreppid computer workstation.

ANDERSON said that on 7 JAN 2006, JALE TREPP (JTREPP), TREPP's wife, told him that GRAY had called her and said that he might have some information about SUBJECT's activities at eTreppid. ANDERSON agreed to meet JTREPP at a Barnes & Noble store located at 5555 South Virginia Street, Reno NV 89502. ANDERSON related to JTREPP that SUBJECT was using open Source Code to develop eTreppid's Source Code, not writing software, does not possess adequate technical abilities, and was dishonest. ANDERSON also informed JTREPP that SUBJECT said that he owned 51% of the company, TREPP was just an investor and that GRAY was going away for some time. JTREPP told ANDERSON to discuss these issues with TREPP.

ANDERSON stated that on 8 Jan 2006, he met TREPP at the Tamarack Junction Restaurant Casino located at 13101 South Virginia Street, Reno, NV 89511. ANDERSON said that he voiced his concerns about SUBJECT's continued claims that he was the majority shareholder in the company, had "lots of cash" invested in the company and that TREPP was only an investor. ANDERSON also informed TREPP that SUBJECT was using open source to develop eTreppid Source Code, SUBJECT was dishonest, SUBJECT said GRAY would be going away for some time. He also told TREPP that as long as five years ago he had suspicions that SUBJECT was less technically competent than he led people to believe.



ANDERSON said that he had suspicions that SUBJECT was using open Source Code to develop eTreppid Source Code for almost two years. ANDERSON said that he confronted SUBJECT about eTreppid's use of open Source Code to develop its Source Code when he was at Fort Bragg, NC conducting some training. SUBJECT told him that the "government knew about it" and that TREPP knew about it and TREPP was "O.K with it".

ANDERSON recommended to TREPP that he speak with VENABLES and TENNETI so TREPP could be further informed of SUBJECT's activities.

ANDERSON said that on 10 Jan 2006, while he was at ETREPPID's office SUBJECT said to him that, "You're an asshole" and, "We'll meet again". ANDERSON asked SUBJECT, "Is that a threat?" and SUBJECT replied, "No". ANDERSON stated that he had suspicions that his phone conversations and his conversations at work may have been monitored. He felt this was the only way in which SUBJECT could have learned about the conversation he and TREPP had about SUBJECT. ANDERSON feared that SUBJECT may harm him in some way and believes that SUBJECT has the capacity to do so.

ANDERSON related that on 11 and 12 Jan 2006, he was asked by TREPP to look at all of ETREPPID's computers and talk with employees to ascertain if there was any Source Code resident on eTreppid's computers. ANDERSON stated that eTreppid Source Code had been deleted from all of the computers. ANDERSON stated that a program known as "Wipe N Clean" was resident on all of ETREPPID's programmer's computers and that program had been resident on the computers prior to the deletion of eTreppid Source Code. "Wipe N Clean" is a program used to permanently delete data from computers. ANDERSON stated that a portion of eTreppid Source Code was resident on his computer and had not been deleted. ANDERSON stated that approximately three years ago SUBJECT instructed all eTreppid personnel to save the Source Code in a file named "Current\_Source" located on their individual workstations. ANDERSON said this easily permitted SUBJECT access to the Source Code and would have facilitated the ease in which the Source Code was located and subsequently deleted.

ANDERSON said that on 15 Jan 2006, he saw SUBJECT at the Peppermill Hotel Casino located at 2707 South Virginia Street, Reno, NV 89502. ANDERSON was at the casino to have lunch with his girlfriend's family. ANDERSON said that while he was waiting on line for lunch service he observed SUBJECT-playing blackjack at one of the casino's blackjack tables. ANDERSON said that SUBJECT looked like he had been playing cards all night as SUBJECT look tired, intoxicated, although he did not have a drink glass in front of him and his hair was a mess. ANDERSON said that SUBJECT looked up and said to him, "Get the fuck out of here!" and asked a casino security guard to make ANDERSON move. The security guard asked ANDERSON to move and ANDERSON refused informing the security guard that he was just watching the game on TV and waiting in line for lunch. SUBJECT again asked the security guard to move ANDERSON and this time ANDERSON complied so SUBJECT would "not cause a scene."



ANDERSON stated he did not have access to the nine missing SECRET hard drives or two missing SECRET mini DV tapes. ANDERSON said he did not possess the combinations to the company's safes. ANDERSON stated that he had nothing to with the deletion of Source Code from eTreppid's computers.

ANDERSON also provided that approximately four months ago SUBJECT gave him electronic TIF files (images), of what ANDERSON said he believed to be the ocean, and directed him to divide the TIF images into 1k x 1k pixels. ANDERSON said that he compiled the images and they remained resident on his computer.

ANDERSON subsequently provided these images to SA HARALDSEN and deleted them from his workstation.

ANDERSON said that during an Automatic Target Recognition demonstration in 2003 (NFI), and upon the direction of SUBJECT, ANDERSON was told to monitor a display on ANDERSON's computer. SUBJECT instructed ANDERSON to strike the "A" key on his computer's keyboard each time a bazooka held by SUBJECT came into view on the video screen. ANDERSON said that he did this for approximately forty separate demonstrations. ANDERSON stated that sometime in October or November of 2005, he learned from GRAY that representatives from the Department of Homeland Security (DHS) were coming to see the ATR product and that this visit was in relation to a potential contract award. ANDERSON said that to his knowledge his prior participation in the ATR product was limited to bazooka demonstrations. ANDERSON did not want to participate "if eTreppid was going to be paid by the DHS." ANDERSON told SUBJECT that he did not want to participate when DHS arrived and he did not. ANDERSON said that subsequent to that date SUBJECT no longer spoke with him and ceased all social contact.

---

K. (U) Interview of: BAUDER  
Date/Place: 25 JAN/eTreppid LLC  
Asst Interviewer: SA Smith  
Associated Exhibit Numbers: 21

BAUDER said he worked for eTreppid since April 2000 and was hired by SUBJECT. His relationship with SUBJECT was strictly professional. He characterized SUBJECT as eccentric with minimal personal skills. Because of BAUDER's size, "a large man," SUBJECT would often ask him to move heavy "stuff."

On Friday, 23 Dec 2005, SUBJECT asked BAUDER to move approximately six boxes from SUBJECT's office and office closet to the warehouse's back door. BAUDER accomplished this task. He said the box flaps were closed therefore he was unable to determine the boxes' contents. BAUDER observed SUBJECT load at least two of the boxes into his (SUBJECT's) truck. BAUDER thought this was a little peculiar since he never witnessed SUBJECT remove anything from the facility.

BAUDER said about one year ago, SUBJECT requested he purchase some open Source Code called MICATOGE XPLAYER. This purchase was an online purchase using BAUDER's PayPal account. The cost of the Source Code was about \$100. BAUDER said that SUBJECT claimed he did not have a PayPal account and required the open Source Code for work.

BAUDER subsequently provided a copy of the PayPal receipt (Attachment 21) to SA HARALDSEN. A review of the receipt is reflected in paragraph 3-1 L.

BAUDER said he assisted SUBJECT with some work regarding "images of the ocean." He said SUBJECT instructed him to place symbols on the images. BAUDER was unaware of why he was accomplishing this task, but surmised it had to do with "terrorist boats." SUBJECT never explained why this work was being performed or for whom.

Sometime in JAN 2006, BAUDER assisted the eTrepid employees with a search of the facility to determine if they could locate any media containing the company's Source Code. While conducting this search BAUDER, observed GRAY, holding two hard drives with red stickers on them. He said these hard drives were found in a warehouse filing cabinet used by SUBJECT. He said he looked in the cabinet drawer and saw additional hard drives in the drawer. He was uncertain how many hard drives were in the cabinet drawer. When he tried to assist GRAY, she explained that BAUDER did not have the appropriate clearance level to take possession of the hard drives.

BAUDER further said that during the summer of 2003 SUBJECT made a peculiar request of BAUDER. SUBJECT invited BAUDER to his office and when BAUDER arrived SUBJECT shut the office door and closed the blinds. SUBJECT instructed BAUDER to "hit the space bar on his (meaning SUBJECT's) keyboard" whenever BAUDER heard an audible tone on his phone. BAUDER explained that SUBJECT was demonstrating a "bazooka" test to some unidentified customers. SUBJECT would hold a simulated bazooka and walk into the field behind the company. While SUBJECT held the bazooka, a camera was trained on SUBJECT. This camera was connected to a laptop computer in the company warehouse and the customers were observing the laptop display. As the camera was trained on the bazooka, SUBJECT would send BAUDER an audible tone to BAUDER's phone. When BAUDER heard the tone he hit the space bar. He was uncertain what "hitting the space bar did" but suspected it highlighted the bazooka on the laptop display. The demonstration lasted about 5-10 minutes. SUBJECT explained that this was for demonstration purposes only and not to worry about it. BAUDER knew better than to pursue this line of questioning because if you questioned SUBJECT you were "eventually fired." BAUDER believed SUBJECT was using "trickery" during this demonstration.

L. (U) Review of PayPal Receipt  
Date/Place: 25JAN 2006/eTreppid  
Associated Exhibit Number: 21

On 25 JAN 2006, SA HARALDSEN reviewed the copy of the PayPal receipt provided BAUDER. The review disclosed that the receipt was identified by the following data:

"Web Accept Payment Sent ID number OXM90015NS3987849  
Original transaction date 30 Nov 2004,  
Payment to XIAO CAN YANG, for the amount of 99.00  
Item Title: Micatoge XPlayer  
Item Number: Source Code License  
Time: 0719:07 PST  
Shipping Address:  
JIM BAUDER  
[REDACTED]  
United States

M. (U) Interview of: VENABLES  
Date/Place: 26 JAN 2006/eTeppid LLC  
Asst Interviewer: SA Smith  
Associated Exhibit Numbers: 22

VENABLES provided a copy of the VISTA 100, ADT Alarm Setup Codes (Attachment 22) for eTreppid, LLC. VENABLES indicated that user #13 was assigned to SUBJECT. A review of the attachment confirmed the information originally provided by TREPP in paragraph 3-1 A. Additionally, VENABLES said that SUBJECT was also aware of all the user alarm codes.

N. (U) Interview of: TREPP  
Date/Place: 27 Jan 2006/Telephonic  
Associated Exhibit Number: 23

TREPP forwarded an email (Attachment 23) referencing AZZINARO's conversation with SUBJECT. A review of the email determined SUBJECT asked AZZINARO if he knew someone who he (SUBJECT) could borrow \$5-\$10 million. Additionally, the email reflected that SUBJECT was looking for a potential investor "from the United States & not from a foreign country."

TREPP's opinion is that SUBJECT is looking for an investor to sell eTreppid's Source Code.

00127  
Sept. 11' 06

O. (U) Interview of: TREPP  
Date/Place: 31 Jan 2006/Telephonic/Email  
Associated Exhibit Number: 24

TREPP forwarded an email (Attachment 24) from VENABLES reflecting that the nomenclature and serial number for the missing RAID stand-alone workstation. The nomenclature and serial was identified as: 1-8-drive IDE RAID with a serial number of: 6564737.

P.(U) Interview of TREPP  
Date/Place: 9 Feb 2006/Telephonic  
Associated Exhibit Number 25

TREPP said that District Court Judge ROBERT H. PERRY, 2<sup>nd</sup> Judicial District Court of the State of Nevada in and for the County of Washoe, Reno, NV, concluded that a preliminary injunction was warranted in the present context. TREPP read the court order, which reflected the following:

SUBJECT was ordered to restrain from destroying, hypothecating, transferring, modifying, and/or assigning the eTreppid Source Code, from discussing any eTreppid technology, including anomaly detection and pattern recognition software, with any third party, except experts or other persons and witnesses necessary to Defendant's case. TREPP said the court issued this injunction to maintain the status quo and to avert any irreparable harm that eTreppid may suffer and based on the risk that SUBJECT could delete and or transfer the last version of the eTreppid Source Code that remains in tact.

TREPP said his attorneys were filing motions to have the judge to order SUBJECT to return the Source Code by a specific date.

---

TREPP provided a copy of the court order (Attachment 25), dated 8 February 2006.

#### 4-1. SUBJECT INTERVIEW:

Interview of: SUBJECT  
Date/Place: 7 February 2006/Telephonic

SUBJECT telephoned SA HARALDSEN and requested a point of contact at the XXX who would "be able to give me permission to testify about working for them and the types of products I developed." SUBJECT said he was going to testify at the civil hearing regarding the TRO, which TREPP had filed against him. He said he needed to be able to defend himself and felt he would not be able to if he were not permitted to tell the judge about whom he worked for. He said "I am afraid of being held in contempt of court when I have to explain to the judge that I can't give this information out."

SUBJECT further said "I signed a letter of treason saying that I will go to jail if I divulge that I worked for them (inferring the XXX)" He further said "I need something so I can divulge everything. Obviously Paul (referring to SA HARALDSEN) you have only heard one side of the story." SUBJECT did not provide any additional information.

**5-1. (U) FBI REFERALL:**

A. On 26 Jan 2006, SA Mike McKinley, Resident Agent in Charge and SA John Piser, FBI Field Office, Reno Nevada was briefed regarding the deletion and removal of company Source Code. SA McKinley said they would review the information provided, but based upon the briefing he believed they would initiate an investigation.

B. 30 Jan 2006, SA PISER said the FBI was assuming investigative jurisdiction regarding the alleged deletion and theft of eTreppid Source Code by SUBJECT.

C. On 2 Feb 2006, SA PISER said the FBI opened an economic espionage and theft of intellectual property investigation.

**5-2 Local Agency Check:**

A. On 13 Feb 2006, SA DERMOT O'REILLY conducted a review of the AFOSI Investigative Information Management System and determined that SUBJECT was not reflected in this database.

B. On \_\_\_\_\_ SA \_\_\_\_\_ conducted a review of the Reno Police Department criminal records which revealed.

---

**6-1 National Agency Check**

A. On 23 January 2006, SA HARALDSEN conducted a review of the Joint Personnel Adjudication System, which reflected SUBJECT's Sensitive Compartmented Intelligence eligibility was listed as: DCID 6/4, 2005 10 06 AFCAF.

B. On 23 January 2006, SA HARALDSEN conducted a review of the Joint Clearance Access Verification System, which revealed the following information regarding SUBJECT: SUBJECT possessed a Top Secret security clearance with SCI access based upon a single scope background investigation (SSBI) conducted by Defense Security Service. The SSBI was opened on 04 April 2004 and closed on 13 Feb 2004 without any derogatory information being identified. The Defense Information Security Office, DSS, adjudicated the Personal Security Investigation favorably on 21 Feb 2004.

C. (U) On 13 Feb 2006, SA ORIELLY conducted a review of the Defense Central Index of Investigations \_\_\_\_\_

**7-1EXHIBITS**

**West, Michael**

---

**From:** West, Michael A.  
**To:** warren@etreppid.com  
**Cc:**  
**Subject:** Additional Questions  
**Attachments:**

**Sent:** Fri 2/10/2006 7:58 PM

Warren,

Here are a few additional questions I would like to talk to you in person about the first of next week.

- Describe Etreppid's trade secrets.
- What security procedures are in place to protect the trade secrets.
- Is there a non-disclosure agreement signed by Montgomery.
- What is the value of Etreppid's trade secrets.

Thank you

**Michael West**  
**Special Agent**  
**Federal Bureau of Investigation**  
**Reno, Nevada**  
**(775) 825-6600**

00130  
Sept. 11' 06

**West, Michael**

---

**From:** West, Michael A. **Sent:** Fri 2/17/2006 12:28 AM  
**To:** paul.haraldsen@pentagon.af.mil  
**Cc:**  
**Subject:** Concurrence for Telephone Recording  
**Attachments:**

Paul,

Thanks again for coming out to Reno, Nv on short notice. Your trip was very successful.

On 2/15/2006, Chief Assistant U.S. Attorney Ronald C. Rachow, Reno, Nv, and Acting/SAC W. Woerner, Las Vegas, Nv, authorized you to make consensually monitored telephone calls in this matter.

I will document the approval to my case file and prepare a report.

Let me know if you would like a copy.

Thanks

**Michael West**  
**Special Agent**  
**Federal Bureau of Investigation**  
**Reno, Nevada**  
**(775) 825-6600**

00131  
Sept. 11' 06



Attachments can contain viruses that may harm your computer. Attachments may not display correctly.  
Access to the following potentially unsafe attachments has been blocked: fbplayer.exe

**West, Michael**

**From:** West, Michael A. **Sent:** Tue 2/21/2006 7:31 PM  
**To:** Haraldsen Paul Civ SAF/AAZ  
**Cc:**  
**Subject:** RE: Program Update  
**Attachments:** comct132.dll(438KB) fbplayer.dll(156KB) vcl40.bpl(1MB) vclx40.bpl(246KB) vdcomponents.bpl(24KB)

**Michael West**  
**Special Agent**  
**Federal Bureau of Investigation**  
**Reno, Nevada**  
**(775) 825-6600**

---

**From:** Haraldsen Paul Civ SAF/AAZ [mailto:Paul.Haraldsen@pentagon.af.mil]  
**Sent:** Sat 2/18/2006 12:51 PM  
**To:** West, Michael A.  
**Subject:** RE: Program Update

Mike,

I still am unable to get this working. Would you please send me another copy or due me in how to get this working.  
Thanks Paul

-----Original Message-----

**From:** West, Michael A. [mailto:Michael.West2@ic.fbi.gov]  
**Sent:** Fri 2/17/2006 2:18 PM  
**To:** Haraldsen Paul Civ SAF/AAZ  
**Cc:**  
**Subject:** Program Update

Paul,

I tried the CD this morning & the FBPlayer file which plays the record did not work.

Attached is a good copy of this program. Copy it into a directory with all the other file and it showed run.

If not, I will send you a working copy.

Mike

**Michael West**  
**Special Agent**  
**Federal Bureau of Investigation**  
**Reno, Nevada**  
**(775) 825-6600**

**West, Michael**

---

**From:** Haraldsen Paul Civ SAF/AZ [Paul.Haraldsen@pentagon.af.mil] **Sent:** Sat 2/18/2006 10:43 AM  
**To:** West, Michael A.  
**Cc:**  
**Subject:** RE: Concurrence for Telephone Recording  
**Attachments:**

Mike,

A report would be good to assuage the concerns of my General Counsel. I am working to make it out there next week. It may have to be later in the week, depending on my wife's doctor's appointments. I will keep you up to speed on my projected arrival times and dates. Call me when you get a chance - cell phone 703-980-9441. By the way the file still did not work. I still am unable to run the audio. Please send me all the files again or if you can convert it to windows media player that would be great. Thanks.

//signed//

PAUL L. HARALDSEN

Special Agent, AFOSI Region 7

Pentagon, Washington, DC

-----Original Message-----

**From:** West, Michael A. [mailto:Michael.West2@ic.fbi.gov]  
**Sent:** Fri 2/17/2006 12:28 AM  
**To:** Haraldsen Paul Civ SAF/AZ  
**Cc:**  
**Subject:** Concurrence for Telephone Recording

Paul,

Thanks again for coming out to Reno, Nv on short notice. Your trip was very successful.

On 2/15/2006, Chief Assistant U.S. Attorney Ronald C. Rachow, Reno, Nv, and Acting/SAC W. Woerner, Las Vegas, Nv, authorized you to make consensually monitored telephone calls in this matter.

I will document the approval to my case file and prepare a report.

Let me know if you would like a copy.

Thanks

Michael West  
Special Agent  
Federal Bureau of Investigation  
Reno, Nevada  
(775) 825-6600

00133  
Sept. 11' 06

The sender of this message has requested a read receipt. [Click here to send a receipt.](#)

**West, Michael**

**From:** Haraldsen Paul Civ SAF/AZ [Paul.Haraldsen@pentagon.af.mil] **Sent:** Mon 2/27/2006 7:19 AM  
**To:** West, Michael A.  
**Cc:**  
**Subject:** RE: Program Update  
**Attachments:**

Mike,

At about 8pm on Sunday, I received a phone call from SUBJECT. He said he was concerned about violating the TRO if he provided copies of the anomaly detection and pattern recognition technical capabilities to the government. He said the government needed "to remove the TRO" if they were truly interested in these capabilities." He is looking for the government to take action to nullify the TRO. He implied that his attorney either met with or phoned the other government agency counsel to discuss the TRO too.

It appears that SUBJECT's attorney is warning him not to violate the TRO. This will hamper our concept of ops for recovering the source code and we will most likely have to revise our approach. SUBJECT said he was still willing to meet with me and discuss any issues, but would not be able to provide examples of the capabilities until the TRO is lifted.

Call me when you get in.

Paul

//SIGNED//  
PAUL L. HARALDSEN, DAFC, USAF  
Director of Policy (SAF/AZ)  
Email (SAF/AZ): Paul.Haraldsen@pentagon.af.mil  
Email (AFOSI - HQ Region 7): Paul.Haraldsen@ogn.af.mil  
Office: (703) 693-2013 (SAF/AZ)  
U/Fax: (703) 693-2059 (SAF/AZ)  
S/Fax: (703) 521-4279 (SAF/AZ)

-----Original Message-----

**From:** West, Michael A. [mailto:Michael.West2@ic.fbi.gov]  
**Sent:** Tuesday, February 21, 2006 11:06 PM  
**To:** Haraldsen Paul Civ SAF/AZ  
**Subject:** RE: Program Update

Excellent!!!

Michael West  
Special Agent  
Federal Bureau of Investigation  
Reno, Nevada  
(775) 825-6600

00134  
Sept. 11' 06

---

From: Haraldsen Paul Civ SAF/AAZ [mailto:Paul.Haraldsen@pentagon.af.mil]  
Sent: Tue 2/21/2006 8:49 PM  
To: West, Michael A.  
Subject: RE: Program Update

Mike,

All files work properly. Thanks for you help. Talk with you soon.

Paul

PAUL L. HARALDSEN, SA  
AFOSI Region 7  
Pentagon, Wash, DC,

-----Original Message-----

From: West, Michael A. [mailto:Michael.West2@ic.fbi.gov]  
Sent: Tue 2/21/2006 7:31 PM  
To: Haraldsen Paul Civ SAF/AAZ  
Cc:  
Subject: RE: Program Update

Michael West  
Special Agent  
Federal Bureau of Investigation  
Reno, Nevada  
(775) 825-6600

---

From: Haraldsen Paul Civ SAF/AAZ [mailto:Paul.Haraldsen@pentagon.af.mil]  
Sent: Sat 2/18/2006 12:51 PM  
To: West, Michael A.  
Subject: RE: Program Update

Mike,

I still am unable to get this working. Would you please send me another copy or clue me in how to get this working. Thanks Paul

-----Original Message-----

From: West, Michael A. [mailto:Michael.West2@ic.fbi.gov]  
Sent: Fri 2/17/2006 2:18 PM  
To: Haraldsen Paul Civ SAF/AAZ  
Cc:  
Subject: Program Update

00135  
Sept. 11' 06

Paul,

I tried the CD this morning & the FBPlayer file which plays the record did not work.

Attached is a good copy of this program. Copy it into a directory with all the other file and it showed run.

If not, I will send you a working copy.

Mike

Michael West  
Special Agent  
Federal Bureau of Investigation  
Reno, Nevada  
(775) 825-6600

00136  
Sept. 11' 06

**West, Michael**

---

**From:** Sloan S. Venables [sloan@eTrepid.com] **Sent:** Thu 3/2/2006 8:34 PM  
**To:** 'Dixon, James, CIV, DSS'  
**Cc:** West, Michael  
**Subject:** classified materials findings  
**Attachments:**

Jay,

As you instructed me to do, starting on Tuesday of this week I went to every computer machine in the building and searched for the classified (secret) files that Patty Gray said she saw on Yongmian's computer. Patty explained to me that the file(s) she saw were a video sequence totaling several hundred megabytes with the first file in the video sequence named 000000.bmp She also said that the files could be identified as originating from the classified video footage by the date 11/11/05 time-stamped on the video and the particular scenario in the video. Having previously reviewed with Paul Haraldsen the original MiniDV tapes that these files originated from, I knew what to look for when searching the computers in our building.

I found 2 instances of these files still in existence on computers in the building. The 2 computers were named "Yongmian" belonging to Yongmian Zhang and "Xilinx1" belonging to Zehang Sun as his secondary testing machine. Both of these people said that they did not know that these files existed on their machines. This was backed up by the fact that these files were located in folders that Dennis Montgomery had created on their hard drives and only he had network sharing access to them. These two employees further said that Dennis routinely copied "sample files" to their machines for them to experiment with and that he did this so often that they could never keep track of what files Dennis had copied to their machines.

As instructed by the person you had on the conference call with us on Tuesday, to remove the files from these machines I ran a wipe and delete on the folders containing these files on both of these computers. After our phone call today I went and removed the hard drives from these 2 machines and placed them in our classified material container.

I also checked the emails of everyone in the building and found no evidence of anyone sending or receiving this video sequence or any other large number of files or video sequences.

Sloan S. Venables  
Facility Security Officer  
Director of Research & Development  
eTrepid Technologies, LLC  
755 Trademark Drive  
Reno, NV 89521  
sloan@eTrepid.com  
Tel: (775) 337-6795  
Fax: (775) 337-1877