EXHIBIT “B”

DECLARATION OF DENNIS L. MONTGOMERY

I, Dennis L. Montgomery, state the following as my declaration pursuant to 28 U.S.C. § 1746:

1. I am a citizen of the United States and resident of the State of Florida.

2. Over the 45 years as a computer scientist, developed software programs, computer hardware, and medical devices.

3. For more than 45 years, I have been engaged in software development and written software focused on developing Data Compression (DC), Anomaly Detection (AD), Pattern Recognition (PR), Object Detection, Identification, and Tracking Technology, and Biometrics in analyzing massive volumes of electronic data.

4. In companies I started, we have developed and then licensed various technologies to the U.S. government intelligence agencies including (CIA), Department of Defense (DOD), SOCOM, Homeland Security (HS), Department of Advanced Naval Research (NAVY), and Air Force (AF).

5. I was issued a TS/SCI security clearance 2004 with case-determined access to SAP programs. I was required to sign a Classified Information Nondisclosure Agreement in connection with my work at eTreppid for the federal government. A true and accurate copy of the nondisclosure agreement that I signed, dated September 16, 2003, is attached

    a. Attached as **Exhibit-01** is a true and correct copy of Dennis Montgomery Security Clearance.

6. I built a myriad of medical technologies. Many are still in use today. I licensed various medical technologies to American Hospital, Baxter Healthcare, Dupont, Corning, Perkin Elmer, the Henley Group, Fisher Scientific, Instrumentation Labs, Kaiser, Siemens, Kodak, among others. I successfully filed multiple medical device registrations with the FDA. I took 3Net Systems Inc. medical company public on Nasdaq August 11, 1992.

7. In addition to these medical technologies, I designed and built programs for GE, Intel, Technicolor, MGM, Hewlett Packard, Novell, IBM, and many others

8. In 1998, I formed eTreppid Technologies, LLC (eTreppid) together with a business partner, Warren Trepp. I was the member of the company who contributed the principal software development capability for the purpose of obtaining contracts with federal government agencies and performing software development services under those contracts.

9. In 2002, eTreppid was approached by representatives of the United States Department of Defense (DOD) and Central Intelligence Agency (CIA), who expressed an interest in various surveillance technologies eTreppid had been developing. These federal government representatives conducted independent tests of eTreppid's technology and then advised us that they had decided to integrate eTreppid's DC, AD, and PR technologies into various programs in the federal government's intelligence community.

    a. Attached as **Exhibit-02** is a true and correct copy of US GOV contract announcement with contract (limited).

10. Following the terrorist attacks of September 11, 2001, eTreppid was awarded contracts with the DoD, U.S. Air Force, CIA, the United State Department of Homeland Security, and other U.S. federal entities to develop and deliver surveillance software technologies. eTreppid fulfilled its obligations under these contracts and delivered intercepted data that enabled the location of foreign terrorists and activities abroad that posed threats to the United States. The work began at our facility in Reno NV. All data collected in our Reno facility was passed on to the intelligence community members in our building and transmitted to the FBI via secure encrypted communication lines at the end of the day. The data was also burned on CDs and couriered weekly by the intelligence officials in our building to their secure facilities in DC.

11. eTreppid Technologies was supplied millions of dollars of hardware by the FBI to begun our surveillance work. Or surveillance work was running on supplied computers by the FBI during my work in Reno NV.

    a. **Attached as Exhibit-03** is a true and correct copy of US GOV supplied surveillance computers.

12. eTreppid Technologies was awarded a surveillance contract by the CIA, DOD, Air Force, and Department of Homeland Security, starting in 2004.

    a. **Attached as Exhibit-04** is a true and correct copy of US GOV contracts (limited pages)

13. Beginning in 2005, I became aware that the CIA and the National Security Agency (NSA) had started using the eTreppid technology that I had developed for locating terrorists abroad to conduct surveillance of citizens of the United States, including members of the Supreme Court of the United States and thousands of other federal and state jurists, members of Congress, state officeholders, numerous public figures and religious leaders in the U.S., and other Americans.

14. On Jan 6, 2006, I separated from Warren Trepp and eTreppid Technologies, which was the very company I started. The separation was related to various business disagreements.

15. In Feb/March 2006, the FBI applied for searched warrants against my home and later storage units. The warrants claimed they were looking for classified documents and various intellectual properties owned by eTreppid. The FBI failed to mention to Magistrate Cooke, who approved the warrants, that I, not eTreppid, owned the intellectual property. It didn't take long for Magistrate Cooke, who issued the search warrant, to figure out how she was duped by the FBI. She realized Agent West took sides in a civil dispute and was there looking for something other than what he listed on the search warrants.

    a. **Attached as Exhibit-05** Copy of FBI Agent West Search warrant affidavit that was handed to me at my house.

16. Eight members of FBI, IRS, and DEA raided Montgomery home and storage units looking for all evidence of FBI/CIA/NSA involvement in operating surveillance programs, foreign and domestic in Nevada that target foreign and domestic individuals, businesses, and elections. The US GOV would only supply the name of SA FBI Agent West. The US GOV refuses to produce the names of the other agents.

17. After three months of testimony, Judge Cooke concluded that Montgomery did nothing wrong and that the FBI filed false affidavits, tampered with evidence they collected, made up false information against Montgomery, and that the FBI violated Dennis Montgomery constitutional rights. When Judge Sandoval (later Governor Sandoval) was confronted with illegal FBI/CIA/NSA domestic surveillance programs operating in NV, he recused himself.

    a. **Attached as Exhibit-06** Judge Cooke probable cause ruling.

18. Judge Cooke issues ruling against the FBI concluding FBI violated Dennis Montgomery constitutional rights. Ordered everything returned to Montgomery family despite objections from DOJ. The FBI shredded the documents that they did not want others to see that reflected US GOV bad actors involved in these illegal surveillance programs, including interfering in foreign elections operating off the grid and away from congressional oversight. After this ruling came out, I was forced to hire 24-hour private security for me and my family given the number of death threats we received. For our safety concerns we were forced to leave our home In Reno, NV and move to Seattle. In WA we continued private 24-hour security for 4 years costing us considerable dollars. The US GOV never appealed the Judge Cooke's ruling.

19. On September 8, 2008, after lengthy legal battles, I settled my differences with my partner, Warren Trepp, and began work at Opspring, later called Blxware. Blxware met with members of the White House and Senate Intel Committee members and eventually went under contract for licensing various technologies to the intelligence community similar to eTreppid products.

20. On Jan 13, 2009, Blxware contracted with the us intelligence community to continue our prior work at eTreppid to be conducted at a new facility Fort Washington, Maryland, which was under the direction of James Clapper.

    a. **Attached as Exhibit-7** is a true and correct copy of US GOV contracts (limited pages)

21. When I learned of CIA and NSA's domestic surveillance using the technology I had developed, I filed whistleblower complaints with the Inspectors General of the CIA, Department of Defense (DOD), Department of Justice (DOJ), Air Force, Director of National Intelligence (DNI), Defense Intelligence Agency (DIA), and others. In those complaints, I objected to the misuse of this surveillance technology to monitor the private communications, bank records, attorney client communications, voting information and other private activities of American citizens.

22. During the eTreppid Litigation, the Director of National Intelligence filed a motion asserting on behalf of the United States a state secrets privilege. In response, on August 29, 2007, the court entered a Protective Order that prohibited certain discovery in the eTreppid Litigation.

    a. Attached as **Exhibit-08** is a true and correct copy of the US Protective Order.

23. On June 6, 2008, I was ordered by a federal district judge in Reno, Nevada to go to the DOJ building in Washington DC and meet separately with two groups in a SCIF. DOJ attorneys Carlotta Wells and Raphael Gomez, who were involved in FBI/CIA/NSA domestic surveillance programs I have worked in since the beginning were not allowed in the meeting. I was not allowed to have any attorney present. I was not allowed to have any mobile devices; nothing could be brought into the room or taken out. In the first meeting, I met with DOD, AF, DIA attorneys and personnel. They claimed all my prior work had been validated and wanted to move forward in contract. In the second meeting, only one woman with the CIA was present and she

wanted to know (a) where all the technology and collected data was kept regarding the CIA surveillance work, foreign and domestic including election monitoring and interference and (b) how I got a copy of 35 CIA enhanced interrogation tapes and where the originals were kept. I made it clear that all work was authorized and supervised by George Tenet, Ed Charbonneau, Donald Kerr, and John Brennan and suggested she talk to them. It was not a pleasant experience and I didn't appreciate the threats she directed at me and my family if their surveillance work ever appeared in the public space. I passed on the CIA threats to the court.

a. Attached as **Exhibit-9 is** an email confirmation I must appear as ordered by the court at the DOJ building in Washington DC.

24. On September 9, 2008, the eTreppid Litigation was terminated by dismissal of all claims and counterclaims pursuant to a stipulation of the parties. At the time of settlement, the federal district court in Reno retained control of all matters regarding compliance with the US Protective Order and the State Secrets Privilege. The Department of Justice has continued to claim that I am still prohibited by the Protective Order from disclosing information related to the FBI/CIA/NSA domestic surveillance contracts in which I played a part.

a. Attached as **Exhibit-10** is an email confirmation that the Reno Federal court retains compliance matters over the PO and SSP in place.

b. Attached as **Exhibit-11** is a true and correct copy of October 26, 2020 email correspondence between my attorney and DOJ attorney Greg Addington, in which Mr. Addington states that the Protective Order "**remains in place** to preclude disclosure of the categories of information and related materials described in the order, based on the circumstances giving rise to the protective order."

25. On March 4, 2010, the DOJ and FBI raided the law offices of my attorneys, Liner Law Firm, without a search warrant or any probable cause and seized millions of pages of attorney-client documents, us gov communications, election data collected in FBI/CIA/NSA domestic surveillance programs I worked in, including proof of us gov election surveillance and tampering. Seized documents and electronic media reflected voting machines manufactures vulnerabilities to hacking. Voting machine manufactures communications and intellectual property we hijacked by us gov numerous times over the years I worked in FBI/CIA/NSA surveillance programs, foreign and domestic.

26. The IP that I designed for these surveillance programs was also seized and never been returned to me despite 12 years of requests by me and my attorneys, costing me tens of millions of dollars.

a. Attached as **Exhibit-12** is an email confirmation of the illegal raid on my attorneys I was not allowed to be present at.

27. On November 18, 2010, the US GOV sent Senior DOJ Attorney Carlotta Wells to my deposition in a bankruptcy proceeding. She was accompanied by two armed agents. During the deposition, Ms. Wells asserted the right to bar me from testifying on matters covered by a protective order entered by the Nevada federal district judge enforcing the state secrets privilege.

a. Attached as **Exhibit-13** is a relevant portion of my 2010 deposition.

28. In September 2013 after failed neurosurgery in July 2013, I decided to give FoxNews an interview regarding FBI/CIA/NSA domestic surveillance programs I worked in including election surveillance and interference. Carl Cameron, FOXNEWS reporter interviewed me in my home in Seattle and filmed my computers running domestic surveillance programs I licensed to the us gov involved in domestic surveillance programs I worked which involved domestic election monitoring and interference. Carl Cameron filmed computers hacking into voting machines manufactures and their equipment with ease. I only agreed to the interview under the agreement that I would be provided a copy of the interview; to date I never received my copy of the interview despite my many requests. A second film crew returned to my home October 2013 to film domestic voting interference and voting machines vulnerabilities. The film crew recorded election network vulnerabilities in various Secretary of State election networks, specifically in Florida, Georgia, Arizona, and others. The filming was done by Robert Shaffer, Foxnews field producer, Seattle, WA.

    a. Attached as **Exhibit-14** are email exchanges between me an FOXNEWS reporter Carl Cameron regarding his interview and filming at my home in Seattle Sept/Oct 2013.

29. On November 15, 2013, the Maricopa County Sheriff's Office approached me for identity theft information regarding Maricopa County residents. I provided under Arizona State immunity agreement information collected in FBI/CIA/NSA domestic surveillance programs I worked in, including surveillance of Maricopa residents, businesses, and the state election networks. During a court proceeding related to that matter, Raphael Gomez, a senior DOJ attorney, took possession of approximately 50 hard drives that I had provided to the Maricopa Sheriff under an assertion of a state secrets privilege. Those hard drives have not been returned to me.

    a. Attached **Exhibit-15** Article (limited) detailing actions during the court hearing.

30. On August 3, 2014, I met with Federal Judge Royce Lamberth in his office in the Federal Court House in DC with others present and discussed FBI/CIA/NSA domestic surveillance programs I worked in including election tampering and the abuses of high-ranking US GOV officials who directed and supervised this illegal domestic surveillance programs I worked in, first in Reno NV and then at Ft. Washington, MD. I presented information to him to support the claims I was making in my previous whistleblower complaints. I was seeking immunity to allow me to present my evidence of these super-secret surveillance programs I worked in. He reached out first to Senator Grassley and then to FBI general counsel James Baker. I provided Judge Lamberth proof of election interference both foreign and domestic. FBI General counsel James Baker later denied any knowledge of such FBI/CIA/NSA domestic surveillance programs I worked in, but had to walk back those comments in his testimony before a house committee on us gov surveillance matters.

    a. Attached as **Exhibit-16** FBI general counsel James Baker testimony before congress where he had to acknowledge my us gov surveillance work.

31. On September 8, 2014, I had discussions with Senate Select Committee on Intelligence (SSCI) staffers John Dickas and James Wolfe regarding targeting congressional members in FBI/CIA/NSA domestic surveillance programs I worked in.

    a. Attached as **Exhibit-17** email to John Dickas regarding the use of surveillance technology I built foreign surveillance used to target Americans and their businesses.

32. On February 23, 2015, I notified Judge Holmes in my US Tax Court hearing that the IRS had retaliated against me because they were upset over Judge Cooke's ruling against the agents of the FBI, IRS, and DEA who raided my home on an illegal search warrant in 2006. In my court hearing, Judge Holmes took notice of the IRS retaliation against me. Also took notice many bad actors in us gov surveillance programs I worked in that abused the surveillance technology.

    a. Attached as **Exhibit-18** is a true and correct copy of pages from my tax case a search hearing (limited pages).

33. In July 2015, I was contacted by the Department of Justice and asked to cooperate in their investigation of US GOV officials who directed and supervised FBI/CIA/NSA domestic surveillance programs I worked in. I was granted immunity for my cooperation and document production. The DOJ was interested in the use of the "eTreppid/Blxware" technology that could surveil and interfere in elections, foreign and domestic leaving no trace. I provided the data to the FBI and DOJ from 2003-2015 showing the technology (source code), collected data, previous tampered data in election surveillance programs operated in FBI/CIA/NSA domestic surveillance programs I worked in.

    a. Attached as **Exhibit-19** is a true and correct copy of my immunity agreement with the DOJ.

34. August 19, 2015, I met with the FBI at their Miramar, Florida office to turn over the data the DOJ requested as part of my immunity agreement. I produced 47 hard drives, 90TB of data, and software (source code) that I developed and licensed to the US GOV to show the methods and sources of this vast data collection, developed and intended for foreign surveillance but used by some bad actors in the US GOV for domestic surveillance running on computers owned by me and the US GOV. This data was personal data about millions of Americans and businesses. It related to contracts between 2003-2013. The drives also contained proof of us gov involvement in both foreign and domestic elections.

35. On December 3, 2015, only after the US GOV reviewed the data that I had submitted to the FBI on the 47 hard drives, I was interrogated by a senior DOJ lawyer Deborah Curtis, FBI SA Walter Giardina, and FBI SA William Barnett in the FBI's field office in the District of Columbia did the DOJ decide to move forward. As a result of this interview, DOJ granted me immunity, as shown in **Exhibit-20,** to present information about the illegal domestic surveillance program to appropriate authorities. During the 3.5-hour deposition, under oath and videotaped at FBI headquarters in DC, I discussed matters regarding the contents of the data on the drives including the programs I developed for the us gov that involved election surveillance and interference with data going back to 2004. I answered all questions and never took the fifth. I also produced additional data at the time of this interrogation. This December 3rd 2015 I had with FBI was confirmed later by FBI General Counsel James Baker during his congressional testimony October 18, 2018 regarding FBI/CIA/NSA domestic surveillance programs I worked in.

    a. Attached as **Exhibit-20** is a true and correct copy of the DOJ request for my testimony and additional document production I was required to produce at the interview which I did.

36. I have never received the 48 hard drives back from DOJ or the FBI. I have tried to recover possession of them, but DOJ and the FBI refuse to return them. The drives were to be returned to me after they removed any sensitive data from them.

37. From 2006-2022, the us gov has seized or failed to return 1,213 electronic media devices (disk drives, flash drives, DVD, CD, etc. containing proof of FBI/CIA/NSA domestic surveillance I worked in and built technology for. These drives contain personal information on over 25 million Americans and their businesses collected in these illegal surveillance programs I worked in.

38. The 47 hard drives, 90TB, hundreds and millions of pages of documents I provided the FBI and the us gov is holding outlined in this declaration will prove US voting machine manufactures and their employees were hacked several times; collecting documents, electronic communications, and intellectual property in illegal FBI/NSA/CIA surveillance programs I worked in. I provided proof to us law enforcement 2005, 2008, 2010, 2012, and 2015. The data was also provided to the FBI Director James Comey's general counsel James Bakers office on 08/19/2015 and 12/03/2015. The voting machine companies included Election Systems & Software, Inc (ES&S), Clear Ballot Group, Inc., Dominion Voting Systems Corp, Hart InterCivic, Inc., MicroVote General Corp., Smartmatic USA Corporation, VotingWorks, and Unisys Voting Solutions.

39. In 2021, I agreed to convey certain assets that I acquired and developed for eTreppid and Blxware to Mike Lindell Management.

40. In the recent 2020 elections, terabytes of data ("Election Data") comprising internet transmissions sent during 2020 election were collected by the same technology I developed and previously licensed by the us gov. US GOV or their agents continued to use the "election technology" I licensed to them previously. The US GOV has refused to pay license fees associated with technology as they continue to use the technology and have paid for in the past.

41. Because DOJ has asserted that the eTreppid Litigation Protective Order "remains in place" to "preclude disclosure of the categories of information and related materials described in the order," I believed when I owned eTreppid and Blxware, and continue to believe today, that DOJ asserts that the Protective Order applies to the FBI/CIA/NSA domestic surveillance data including Election Data, and that public disclosure of the Election Data would violate the Protective Order and the state secrets privilege.

I certify under penalty of perjury that the foregoing is true and correct.

Executed this 19 day of August, 2022 in NAPLES, Florida.

Dennis L. Montgomery

EXHIBIT “1”

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, all 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	SOCIAL SECURITY NUMBER (See Notice below)
[signature]	9/16/03	[redacted]

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

ETREPID TECHNOLOGIES, LLC 3C5X0
755 TRADEMARK DR.
RENO, NV 89521

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: [signature] DATE: 16 Sept 03	SIGNATURE: [signature] DATE: 16 Sept 03
NAME AND ADDRESS (Type or print): Defense Security Svc. (S41PY) 4349 Duffer Drive North Las Vegas NV 89191	NAME AND ADDRESS (Type or print): SAME

SIGN HERE

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.

Person Summary

MONTGOMERY, DENNIS LEE

SSN: [redacted]
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

Date of Birth: [redacted]
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

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	

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

eTreppid Technologies, LLC www.eTreppid.com
755 Trademark Drive
Reno, NV 89521
Tel: (775) 337-6771
Fax: (775) 337-1877

To Whom It May Concern:

Name: Dennis Lee Montgomery
SSN: [redacted]
Date of Birth: [redacted]
Place of Birth: Mena, Arkansas
Citizenship: US

The above listed person, **Dennis Lee Montgomery**, has been granted **Top Secret** by DISCO effective February 14, 2004 and is therefore authorized to be a courier for material that is classified up to the level of clearance eligibility that he has been granted.

Clearance data and other information furnished is certified to be true and correct and this request is made in the national interest.

Verified and Approved by: _____ **Date: 1 June 2005**
Facility Security Officer: Sloan S. Venables

eTreppid Technologies, LLC www.eTreppid.com
755 Trademark Drive
Reno, NV 89521
Tel: (775) 337-6771
Fax: (775) 337-1877

To Whom It May Concern:

Name: Dennis Lee Montgomery
SSN: [redacted]
Date of Birth: [redacted]
Place of Birth: Mena, Arkansas
Citizenship: US

The above listed person, **Dennis Lee Montgomery**, has been granted **SCI - DCID 6/4** by **AFCAF** effective **06 October 2005**, and is therefore authorized to be a courier for material that is classified up to the level of clearance eligibility that he has been granted.

Clearance data and other information furnished is certified to be true and correct and this request is made in the national interest.

Verified and Approved by: _____ **Date: 10 October 2005**
Facility Security Officer: Sloan S. Venables

eTreppid Technologies, LLC www.eTreppid.com
755 Trademark Drive
Reno, NV 89521
Tel: (775) 337-6771
Fax: (775) 337-1877

January 12, 2004

To whom it may concern,

For about four months eTreppid Technologies, LLC (the "Company") has been providing assistance and information (including that related to the Company's technology, know-how, business and processes) pursuant to an agreement with the CIA (the "Government"). As part of the consideration for providing such assistance and information, the Government agreed that eTreppid Technologies' identity as a contractor and source of the assistance and information as well as the information supplied by the Company would be kept confidential, would only be disclosed to individuals within the government on a need to know basis only, and would not be revealed to the public under the Freedom of Information Act or otherwise. The purpose of this letter agreement is to confirm in writing the understanding between the parties.

It is our current intent to continue to work with the Government with regard to this matter. This will confirm that the U.S. Government agrees not to make any attempt to unilaterally use or otherwise take technology, intellectual property or other property or assets owned by eTreppid Technologies. In addition, the Government agrees that it will negotiate in good faith an agreement that sets forth future services (including technology and intellectual property) to be provided by the Company and the compensation to be paid for such future services as well as services already rendered.

eTreppid Technologies, LLC

By: Warren Trepp, CEO

US Government

By:

Edward B. Charbonneau
Associate DDS&T for Technical Operations

Central Intelligence Agency
Washington, DC 20505
(703) 482-4848
Fax: (703) 482-6350

EXHIBIT “2”

eTreppid Awarded IDIQ Contract for Compression, ATR, and Biometric Technology

Reno, Nevada—(BUSINESS WIRE)—Feb. 18, 2004—

eTreppid Technologies, LLC has been awarded a five-year indefinite delivery, indefinite quantity (IDIQ) contract with the United States Government to supply software compression, Automatic Target Recognition (ATR), and biometric products. With a contract ceiling of $30 million, this contract provides a vehicle for the procurement of eTreppid's breakthrough technology by all services and agencies in the U. S. Government.

eTreppid Technologies provides a family of compression products based on its proprietary lossless and "lossy" data compression technology. These products include data, audio, still imagery, and video compression systems that enable transmission of time-critical information over limited bandwidth equipment. Because of the unique qualities of eTreppid's compression approach, the identification of objects within the data while the data is in its compressed state is possible.

"eTreppid compression is, in a word, impressive," stated Mr. Pete Wiedemann, an expert in real-time motion imagery and communications who provides applied solutions to the United States Air Force (USAF) as a consultant. "Just the single-pass, lossy compression by itself yields high quality at very tight ratios, making it a valuable tool for communications and storage of a wide variety of data. Its ability to add lossless iterative re-compression magnifies that capability, achieving even tighter compression. Additional compression factors of 2 to 3 are thus easily achievable in near real time for live transmission and even higher re-compression factors are obtainable for media storage, where the additional processing time on the order of a minute or two is easily tolerated. Remarkably, such re-compression does not increase decompression time. Lastly, valuable additional capabilities such as Automatic Target Cueing/Recognition, directly from the compressed data without first needing to decompress, are like icing on the cake. The combination of these capabilities makes using this technology all but irresistible. Not only can these capabilities make significant contributions to expand use and lower the cost in traditional compression environments, but should open many new communications and storage areas and markets heretofore inaccessible to the delivery of bandwidth/storage consumptive products." Mr. Wiedemann rendered these

observations upon completion of an independent "hands-on" evaluation of the compression system, using a variety of actual and purposely selected aerial video clips.

"eTreppid's compression technology enables video to be transmitted over satellite radios using the same bandwidth that audio or still images had required in the past," stated Warren Trepp, eTreppid's Chief Executive Officer. "Whether it is satellite imagery or email, our compression technology can reduce the storage and transmission needs for the Government."

"eTreppid's ATR technology can be used in many ways in markets such as surveillance and security," stated Patty Gray, eTreppid's VP of Product Development. "Whether for the protection of our interests at home or elsewhere in the world, ATR can provide the additional information needed to address today's tough security problems."

eTreppid Technologies, LLC is a privately held innovative company specializing in compression and data processing technology.

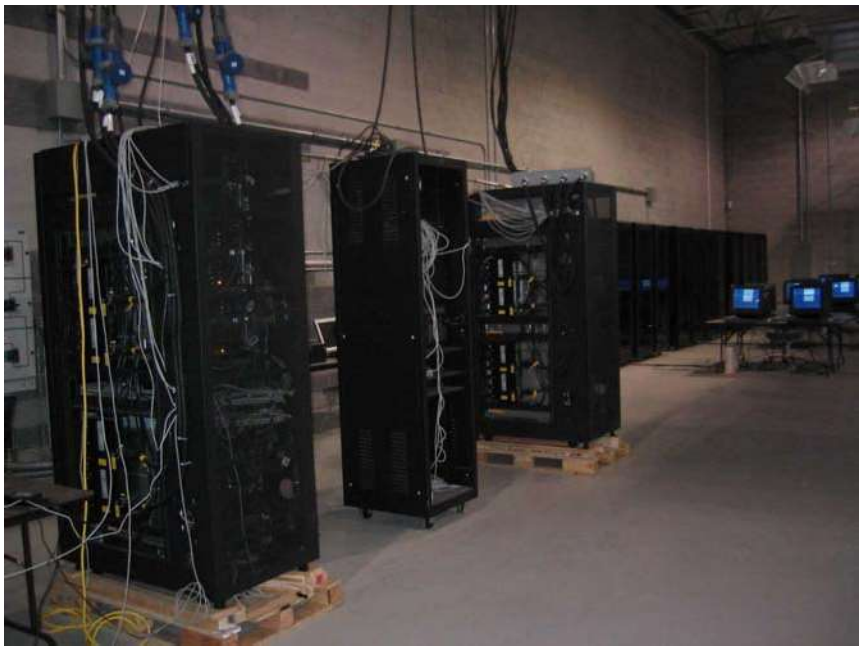
CONTACT INFORMATION:
Patricia Gray
eTreppid Technologies
http://www.etreppid.com

EXHIBIT “3”

eTreppid Technologies Computer Facility

05/12/2004

FBI/CIA Supplied Surveillance Computers



DOD Supplied Surveillance Computers

EXHIBIT “4”

ORDER FOR SUPPLIES OR SERVICES

(Contractor must submit four copies of invoice.)

Form Approved OMB No. 0704-0187 Expires June 30, 1997

PAGE 1 OF 2

PLEASE DO NOT RETURN YOUR FORM TO EITHER OF THESE ADDRESSES.
SEND YOUR COMPLETED FORM TO THE PROCUREMENT OFFICIAL IDENTIFIED IN ITEM 6.

1. CONTRACT/PURCH ORDER NO.	2. DELIVERY ORDER NO.	3. DATE OF ORDER	4. REQUISITION/PURCH REQUEST NO.	5. PRIORITY
H92222-04-D-0006	0001	16-FEB-2004	1SP50040420100	DO-C9

6. ISSUED BY CODE H92222
HQ US Special Operations Command
ATTN: SOAL-KB (Holland)
7701 Tampa Point Blvd
Macdill AFB, FL 33621

7. ADMINISTERED BY *(if other than 6)* S0507A
DCMA San Francisco Lathrop Office
700 E. Roth Rd
French Camp, CA 95231

8. DELIVERY FOB
X DEST
☐ OTHER
(See Schedule if other)

9. CONTRACTOR CODE 3CSX0 FACILITY CODE
NAME AND ADDRESS
eTreppid Technologies, LLC
755 Trademark Dr
Reno, NV 89521
TEL:
FAX:

10. DELIVER TO FOB POINT BY (Date) (YYMMDD)
SEE SCHEDULE

11. MARK IF BUSINESS IS
☐ SMALL
☐ SMALL DISADVANTAGED
☐ WOMEN OWNED

12. DISCOUNT TERMS

13. MAIL INVOICES TO See Section G

14. SHIP TO CODE H92222
UQ USSOCOM/SOAL-SP (Mohr)
7701 Tampa Point Blvd
MacDill AFB, FL 33621
ATTENTION: SOAL-SP (Brad Mohr)

15. PAYMENT WILL BE MADE BY HQ0339
DFAS-Columbus - West Entitlement Operations
PO Box 182381
Columbus, OH 43218

MARK ALL PACKAGES AND PAPERS WITH CONTRACT OR ORDER NUMBER

16. TYPE OF ORDER
DELIVERY ☐ This delivery order is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
Reference your ____ furnish the following on terms specified herein.
PURCHASE X

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

ETREPPID TECHNOLOGIES, LLC		WARREN TREPP, CEO	040216
NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYMMDD)

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies: ____

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE
ACRN AA: 974/60300 56SF SD4 52SP 54X000 SP10 525700 F25700 $325,125.00

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE CONTINUATION SHEET				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity Ordered and encircle.

24. UNITED STATES OF AMERICA
BY SUSAN M GRIFFIN
CONTRACTING/ORDERING OFFICER

25. TOTAL $325,125.00
29. DIFFERENCES

26. QUANTITY IN COLUMN 20 HAS BEEN
☐ INSPECTED ☐ RECEIVED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED
DATE ____ SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE ____

27. SHIP NO. ☐ PARTIAL ☐ FINAL
28. D.O. VOUCHER NO.
30. INITIALS
31. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL
32. PAID BY
33. AMOUNT VERIFIED CORRECT FOR
34. CHECK NUMBER
35. BILL OF LADING NO.

36. I certify this account is correct and proper for payment
DATE ____ SIGNATURE AND TITLE OF CERTIFYING OFFICER ____

37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED (YYMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

DD FORM 1155, JUN 94 PREVIOUS EDITION MAY BE USED

Continuation Sheet

1. **CONTRACT LINE ITEMS**:

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0001AA		1	Each	$25,000.00	$25,000.00
	Falconview (PFPS) Maps - Compression FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				
0001AB		1	Each	$40.00	$40.00
	Falconview (PFPS) Maps - Plug-in Decoder FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				
0001AC		1	Each	$25,000.00	$25,000.00
	Still Image Compression FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				
0001AD		1	Each	$10.00	$10.00
	Still Image Decoder FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				
0001AE		1	Each	$50,000.00	$50,000.00
	Video Imagery w/ Audio - Compression FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				
0001AF		1	Each	$25.00	$25.00
	Video Imagery w/ Audio - Decoder FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				
0001AN		1	Each	$125,000.00	$125,000.00
	Generic Data Compression FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				

0001AP		1	Each	$50.00	$50.00
	Generic Data Decompressor FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				
0001AQ		1	Each	$100,000.00	$100,000.00
	Detection of Human and Non-Human Objects FFP 1 Each = 1 CPU that this software is installed on. FOB: Destination				

2. **GOVERNMENT FURNISHED PROPERTY.**

a) The Government will furnish one laptop computer to:
eTreppid Technologies
755 Trademark Dr
Reno NV 89521.

b) Upon receipt of the Government-furnished laptop, the Contractor shall load the software ordered on the task order and return the laptop to:
HQ USSOCOM
ATTN: SOAL-SP (Brad Mohr)
7701 Tampa Point Blvd
MacDill AFB, FL 33621.

3. **DELIVERY TIMEFRAME.** The contract shall have 14 days from the receipt of the Government-furnished laptop to load the software and return the laptop to the Government. If the 14th day falls on a weekend or federal holiday, the due date shall automatically extend to the next business day.

//nothing follows//

ORDER FOR SUPPLIES OR SERVICES

(Contractor must submit four copies of invoice.)

Form Approved OMB No. 0704-0187 Expires June 30, 1997

PAGE 1 OF 3

PLEASE DO NOT RETURN YOUR FORM TO EITHER OF THESE ADDRESSES.
SEND YOUR COMPLETED FORM TO THE PROCUREMENT OFFICIAL IDENTIFIED IN ITEM 6.

1. CONTRACT/PURCH ORDER NO.	2. DELIVERY ORDER NO.	3. DATE OF ORDER	4. REQUISITION/PURCH REQUEST NO.	5. PRIORITY
H92222-04-D-0006	0004	29 Mar 05 ~~01 MAR 2004~~	ISP50050070100	DO-C9

6. ISSUED BY CODE H92222
HQ US Special Operations Command
ATTN: SOAL-KB (Lopez)
7701 Tampa Point Blvd
Macdill AFB, FL 33621

7. ADMINISTERED BY *(If other than 6)* S0507A
DCMA San Francisco Lathrop Office
700 E. Roth Rd
French Camp, CA 95231

8. DELIVERY FOB
X DEST
☐ OTHER
(See Schedule if other)

9. CONTRACTOR CODE 3C5X0 FACILITY CODE
NAME AND ADDRESS
eTreppid Technologies, LLC
755 Trademark Dr
Reno, NV 89521
TEL:
FAX:

10. DELIVER TO FOB POINT BY (Date) (YYMMDD)
SEE SCHEDULE

11. MARK IF BUSINESS IS
☐ SMALL
☐ SMALL DISAD-VANTAGED
☐ WOMEN OWNED

12. DISCOUNT TERMS

13. MAIL INVOICES TO See Section G

14. SHIP TO CODE
SEE SCHEDULE
ATTENTION:

15. PAYMENT WILL BE MADE BY HQ0339
DFAS COLUMBUS WEST ENTITLEMENT OPERATIONS
PO BOX 182381
COLUMBUS OH 43218-2381

MARK ALL PACKAGES AND PAPERS WITH CONTRACT OR ORDER NUMBER

16. TYPE OF ORDER
DELIVERY X
PURCHASE

This delivery order is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
Reference your ____ furnish the following on terms specified herein
ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

ETreppid Technologies, LLC		Warren Trepp, CEO & President	18 Mar 05
NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYMMDD)

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies. ____

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE
ACRN AA: 9740100.12SF SG4 52SP SPCP00 01 592 012140 525700 F25700

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE CONTINUATION SHEET				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity Ordered and encircle.

24. UNITED STATES OF AMERICA
BY SUSAN M. GRIFFIN 29 Mar 05
CONTRACTING/ORDERING OFFICER

25. TOTAL $184,147.98
29. DIFFERENCES

26. QUANTITY IN COLUMN 20 HAS BEEN
☐ INSPECTED ☐ RECEIVED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED
DATE ____ SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

27. SHIP NO. ☐ PARTIAL ☐ FINAL
28. D.O. VOUCHER NO.
30. INITIALS
31. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL
32. PAID BY
33. AMOUNT VERIFIED CORRECT FOR
34. CHECK NUMBER
35. BILL OF LADING NO.

36. I certify this account is correct and proper for payment
DATE ____ SIGNATURE AND TITLE OF CERTIFYING OFFICER

37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED (YYMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

DD FORM 1155, JUN 94 PREVIOUS EDITION MAY BE USED

Continuation Sheet

Line Items

ITEM NO	SUPPLIES/SERVICES	QTY	UNIT	UNIT PRICE	TOTAL AMOUNT
0001	SOFTWARE APPLICATIONS – CONTRACTOR FUNDED (FFP) The Contractor shall furnish the COTS software (license and media) FOB: Destination USSOCOM Form 9 Number: ISP50050070100	1	LOT	NSP	NSP
0001AE	VIDEO IMAGERY w/AUDIO – COMPRESSION (FFP) 1 Each = to be install on 1 CPU furnished as GFP	4	EACH	$30,000	$120,000.00
0001AF	VIDEO IMAGERY w/Audio - Decoder(FFP) 50 Each = to be installed on 1 CPU furnished as GFP	50	EACH	$15.00	$750.00
0004	FFP - Fixed Price Task Order The contractor shall furnish all materials, equipment, personnel and travel required to perform the requirements of the Statement of Work entitled " Evaluation and Integration of Digital Compression " FOB: Destination USSOCOM Form 9 Number: ISP50050070100	1	LOT		$63,397.98
0007	Data FFP The contractor shall furnish data as required in individual task orders. FOB: Destination USSOCOM Form 9 Number: ISP50050070100	1	LOT	$0.00 NSP	$0.00 NSP
				TOTAL AMOUNT TASK ORDER 0004	**$184,147.98**

development, Mr. Montgomery approached Warren Trepp, eTreppid's Chief Executive Officer, and they formed eTreppid Technologies, LLC.

During the first few years, eTreppid remained largely in a Research and Development stage, continuing to refine the technology. The algorithm achieves its remarkable compression ratios by applying multiple passes at the data until a gain in compression is too small to warrant an additional pass. The decompression process, however, is always just one pass. In addition, a compression pass does not have to be completed on the entire data set before a user can have access to that file. It has also been used to compress previously compressed files where its compression strength is apparent.

Due to a large demand for compression of multimedia data, eTreppid worked on developing an initial compression pass that would alter a user-defined amount of the data in an effort to increase compression. The resulting "lossy" compression pass is then followed by multiple "lossless" passes to achieve a typical compression ratio of 400-600 : 1 on video data.

Another benefit of compressing data with eTreppid's technology is that objects within the data can be located and operated on while the data is compressed. This greatly increases the speed of database searches and operations on the objects. For example, objects within a video stream can be accurately identified at rates up to 1000 objects per second at greater than 98% accuracy with virtually no false-positive reports. If desired, the detected object can then have an effect applied such as blurring or color changes without the need to decompress the video frame first. This ability is not restricted to video objects. 3D models, text, audio, numerical data, are all examples of objects that can be operated on.

Today, eTreppid's compression technology has been evaluated or applied in many different industries including real time video surveillance, seismic data analysis, medical imaging, broadcast audio and video, facial and fingerprint identification, mapping applications, and still imaging.

Deliverables

Government Furnished Equipment

USSOCOM will provide eTreppid with the following equipment, information, or access in order for eTreppid to complete its tasks:

- Access to the PSYOP media production center and equipment
  - to gather information required to correctly integrate eTreppid's compression technology into the existing system
  - to gather information required to provide architecture recommendations for integrating eTreppid's compression technology "in-line" or in replacement of existing equipment
- A listing of software formats that are of interest to the US Government
  - to enable eTreppid to enable support for the formats
  - to enable eTreppid to provide estimates on the development of software support for currently unsupported formats
- Technical information on the network interface
  - to enable eTreppid to understand network certification and configuration management requirements for transmission through network firewalls and Microsoft operating system networks
- Computing hardware per eTreppid's specifications
  - to be used inline with existing equipment during Phase 2

Other Government Furnished Resources

USSOCOM shall provide the following resources to support this effort:

- Program manager (PM) who shall act as a single point of contact

eTreppid Deliverables

eTreppid shall deliver the following items in support of this contract:

- An estimate for the development of software support for any currently unsupported formats
- An architecture diagram providing eTreppid's recommendations on integrating its compression software either "in-line" or in replacement of existing equipment
- Software and/or systems for any procured licenses along with installation assistance, training, technical support and maintenance as described in this document.

Other eTreppid Resources

eTreppid shall provide the following resources in support of this contract:

- eTreppid shall provide a Program Manager (PM) who shall act as the single point of contact that is provided at a rate of 10% of the total resource hours for each phase.
  - Program Manager: Patty Gray, eTreppid Technologies, LLC, 755 Trademark Drive, Reno, Nevada 89521, 775-337-6771 (office), 602-421-1453 (mobile), patty@etreppid.com

The eTreppid compression and object identification technology will at all times remain the sole property of eTreppid Technologies, LLC and all licenses will be granted pursuant to Contract No. H92222-04-D-0006, CLIN 0001, Attachment 2. No data or other rights of any nature in eTreppid's technology will accrue to USSOCOM by virtue of eTreppid performing under this ROM.

eTreppid Technologies, LLC
www.eTreppid.com
755 Trademark Drive
Reno, NV 89521
Tel: (775) 337-6771
Fax: (775) 337-1877

January 12, 2004

To whom it may concern,

For about four months eTreppid Technologies, LLC (the "Company") has been providing assistance and information (including that related to the Company's technology, know-how, business and processes) pursuant to an agreement with the CIA (the "Government"). As part of the consideration for providing such assistance and information, the Government agreed that eTreppid Technologies' identity as a contractor and source of the assistance and information as well as the information supplied by the Company would be kept confidential, would only be disclosed to individuals within the government on a need to know basis only, and would not be revealed to the public under the Freedom of Information Act or otherwise. The purpose of this letter agreement is to confirm in writing the understanding between the parties.

It is our current intent to continue to work with the Government with regard to this matter. This will confirm that the U.S. Government agrees not to make any attempt to unilaterally use or otherwise take technology, intellectual property or other property or assets owned by eTreppid Technologies. In addition, the Government agrees that it will negotiate in good faith an agreement that sets forth future services (including technology and intellectual property) to be provided by the Company and the compensation to be paid for such future services as well as services already rendered.

eTreppid Technologies, LLC

By: Warren Trepp, CEO

US Government

By:

Edward B. Charbonneau
Associate DDS&T for Technical Operations

Central Intelligence Agency
Washington, DC 20505
(703) 482-4848
Fax: (703) 482-6350

OMB Approval 2700-0042

AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350) ▶	RATING	PAGE 1	OF PAGES 26
2. CONTRACT (Proc. Inst. Ident.) NO. 2004*I111530*000	3. EFFECTIVE DATE 1 April 2004	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.		

5. ISSUED BY	CODE	6. ADMINISTERED BY (If other than Item 6)	CODE
Calvin A. Boone P.O. Box 40931 Arlington, VA 22204		Susan B. (703) 790-9442	

7. NAME AND ADDRESS OF CONTRACTOR (No. street, county, state and ZIP Code)	8. DELIVERY ☐ FOB ORIGIN ☐ OTHER (See below)
eTreppid Technologies, LLC 755 Trademark Drive Reno, NV 89521	9. DISCOUNT FOR PROMPT PAYMENT N/A
	10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN: ▶ ITEM G-2.

CODE	FACILITY CODE

11. SHIP TO/MARK FOR	CODE	12. PAYMENT WILL BE MADE BY G-2.	CODE

13. AUTHORITY FOR USING OTHER FULL AND OPEN COMPETITION:
☐ 10 U.S.C. 2304(c)( ) ☐ 41 U.S.C. 253(c)( )

14. ACCOUNTING AND APPROPRIATION DATA

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	See Page 2 CL BY: 2025200 CL RSN: 1.5(c) DECL ON: X1 DRV FRM: CON 1-82				
	15G. TOTAL AMOUNT OF CONTRACT ▶				$ 0

16. TABLE OF CONTENTS

(✓)	SEC.	DESCRIPTION	PAGE(S)	(✓)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	20
X	B	SUPPLIES OR SERVICES AND PRICE/COST	3			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	C	DESCRIPTION/SPECS./WORK STATEMENT	4	X	J	LIST OF ATTACHMENTS	26
X	D	PACKAGING AND MARKING	5			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
X	E	INSPECTION AND ACCEPTANCE	7		K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
X	F	DELIVERIES OR PERFORMANCE	8				
X	G	CONTRACT ADMINISTRATION DATA	9		L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	12		M	EVALUATION FACTORS FOR AWARD	

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. ☒ CONTRACTOR'S NEGOTIATED AGREEMENT *(Contractor is required to sign this document and return __1___ copies to issuing office.)* Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. *(Attachments are listed herein.)*

18. ☐ AWARD *(Contractor is not required to sign this document.)* Your offer on Solicitation Number _____, including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.

19A. NAME AND TITLE OF SIGNER *(Type or print)*	20A. NAME OF CONTRACTING OFFICER
WARREN TREPP	John S. Tarah

19B. NAME OF CONTRACTOR	19C. DATE SIGNED	20B. UNITED STATES OF AMERICA	20C. DATE SIGNED
(Signature of person authorized to sign)	4/21/04	BY *(Signature of Contracting Officer)*	20 Apr 2004

NSN 7540-01-152-8069
PREVIOUS EDITION UNUSABLE

26-107
Computer Generated

STANDARD FORM 26 (REV. 4-85)
Prescribed by GSA

EXHIBIT “5”

AO106 (Rev. 12/03) Affidavit for Search Warrant

FILED

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

FEB 28 2006

MAGISTRATE JUDGE
DISTRICT OF NEVADA

BY _____ DEPU

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

12720 Buckthorn Lane, Reno, Nevada

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

Case Number: 3:06-MJ-0023-VPC

I, MICHAEL WEST being duly sworn depose and say:

I am a(n) SPECIAL AGENT, FEDERAL BUREAU OF INVESTIGATION and have reason to believe
Official Title

that ☐ on the person of or ☑ on the property or premises known as (name, description and/or location)

12720 Buckthorn Lane, Reno, Nevada, further described in Attachment A, fully incorporated by reference and attached hereto

in the _____ District of NEVADA

there is now concealed a certain person or property, namely (describe the person or property to be seized)

SEE ATTACHMENT B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

property that constitutes evidence of the commission of a criminal offense; the fruits of a crime, and/or property designed or intended for use which is or has been used as a means of committing a criminal offense

concerning a violation of Title 18 United States code, Section(s) 793(e)

The facts to support a finding of probable cause are as follows:

SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT MICHAEL WEST

Continued on the attached sheet and made a part hereof: ☑ Yes ☐ No

Signature of Affiant

Sworn to before me and subscribed in my presence,

February 28, 2006 at RENO NEVADA
Date City State

VALERIE P. COOKE US MAGISTRATE
Name of Judge Title of Judge

Signature of Judge

AFFIDAVIT

I, Michael A. West, Special Agent (SA), United States Federal Bureau of Investigation, being duly sworn, state the following:

I have been employed as a Special Agent with the Federal Bureau of Investigation for approximately ten years. As part of my regularly assigned duties, I investigate violations of federal statutes to include theft of trade secrets and the unlawful retention of information relating to the national defense which occur in Northern Nevada.

Your affiant makes this affidavit in support of the accompanying application for a search warrant for the premises located at 12720 Buckthorn Lane, Reno, Nevada (further described in "Attachment A").

Your affiant has investigated or been advised by other Special Agents of the U.S. Government and confirmed the following:

Your affiant became involved in investigating DENNIS LEE MONTGOMERY based on a complaint made by Management Committee Chairman Warren Trepp of eTreppid Technologies, LLC, a Nevada Limited Liability Corporation, located at 755 Trademark Drive, Reno, Nevada. Trepp alleged that Chief Technical Officer (CTO) DENNIS LEE MONTGOMERY removed eTreppid computer equipment and storage media containing Source Code files derived from eTreppid's development efforts relating to data compression and pattern recognition software, removed hard disk drives containing Secret information provided by the Department of Defense (DOD), and systematically deleted all Source Code files from the remaining eTreppid data servers, all in violation of Title 18, United States Code, Section 1832, Theft of Trade Secrets, and Title 18, United States Code, Section 793(e), Unlawful Retention of National Defense Information.

eTreppid Technologies, LLC, (eTreppid), a Nevada Limited Liability Company, was originally formed in 1998 as "Intrepid" by founders Warren Trepp (Trepp) and DENNIS LEE MONTGOMERY (MONTGOMERY) to develop software that relates to data compression and pattern recognition, among other products. Since that time and to the present, Trepp has held the

position of Management Committee Chairman and MONTGOMERY held the title of Chief Technical Officer (CTO).

MONTGOMERY signed a Contribution Agreement, dated September 28, 1998, in which MONTGOMERY effectively assigned all rights to his "Contributed Assets" to eTreppid in exchange for a fifty percent (50%) interest Management Interest in eTreppid. The "Contributed Assets" meant all of MONTGOMERY's know-how; trade secrets; patent rights, copyrights, trademarks, licenses and permits, registered or unregistered, pending or approved; software programs and all programming and Source Codes used in connection therewith or otherwise required to operate any component thereof; and all programming documentation, designs, materials and other information, all in whatever form and wherever located, relating to or used in connection with, or otherwise describing or consisting of any part of, the software compression technology.

MONTGOMERY also signed the "Amended And Restated Operating Agreement of eTreppid Technologies, LLC, A Nevada Limited Liability Company, Dated and Adopted Effective As Of November 1, 2002", which in paragraph 6.5, "Time Devoted to Management", MONTGOMERY agreed to "devote substantially all of his full time and attention and efforts to the Business and affairs of the LLC"; in paragraph 6.6, "Restriction on Independent Activities; Agreement Not to Compete", MONTGOMERY agreed that he "and his Affiliates, during the term of this Agreement, none of them shall compete with the LLC, whether for their own account and/or for the account of others, individually, jointly with others, or as a part of any other limited liability company, limited partnership, general partnership, joint venture, corporation or other entity, by: (i) developing, licensing, or exploiting in any manner any software programs or other technology which is competitive with the Technology or the Business of the LLC, or providing any services or supplies which are encompassed within the definition of the "Business" of the LLC set forth in this Agreement."

MONTGOMERY, as the Chief Technical Officer, was responsible for leading the software development efforts of eTreppid, including those related to data compression, pattern recognition, change and anomaly detection, and other inventions, from 1998 until he was terminated on January 18, 2006.

MONTGOMERY filed ten Patent Assignment applications with the United States Patent and Trademark Office during the period of November 2000 to November 2001 for patents pertaining to various technologies developed by MONTGOMERY while an employee at eTreppid and on each patent MONTGOMERY assigned full and exclusive rights, title, and interest of these technologies to eTreppid.

Trepp considers eTreppid's trade secrets to be various software programs relating to data compression, pattern recognition, change and anomaly detection, among other things, which derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public. eTreppid has earned in excess of ten million dollars in revenues since 1998 from various government and commercial contracts. Trepp anticipates that eTreppid's development efforts will result in other multi-million dollar contracts.

eTreppid has taken reasonable steps to keep its information and development efforts secret by requiring Programmers or Software Developers to use unique user names and passwords to log onto eTreppid computers with limited access to prevent unauthorized duplication, modification, or deletion of Source Codes. Software Developers store their work or Source Code on a hard drive installed in their workstation and on a Source Code Server, a high capacity data storage device, which uses Redundant Array of Inexpensive Disks (RAID) storage to maintain and ensure reliable accessibility to the Source Code files produced by all Software Developers. The Source Code Server is backed up by the Internet Security Accelerator (ISA) Server which also uses RAID storage to maintain and ensure reliable accessibility to the Source Code files. Only two eTreppid employees, MONTGOMERY and Director of Research and

Development Sloan Venables, had the access rights to duplicate, modify, or delete Source Code files maintained on the Source Code and ISA Servers.

MONTGOMERY was responsible for and regularly maintained a separate backup copy of the Source Code Server data on an eTreppid black Lianli Central Processing Unit (CPU) connected to an Ultra Storage eight hard drive RAID storage unit, Model 2081, serial number 6564737, located in a work area occupied by MONTGOMERY in the eTreppid warehouse.

As an additional security measure, Trepp required MONTGOMERY to provide him with periodic copies of eTreppid's current Source Code files on compact disks or hard drives over the past seven years which Trepp stored in a secure off-site location.

eTreppid's facility is physically secured by door locks, access control devices, and a monitored alarm system. eTreppid also maintains a video surveillance system that records sixteen surveillance cameras covering internal and external views of eTreppid's facility.

On March 12, 2003, eTreppid was awarded a contract from the U.S. Special Operations Command (SOCOM), Fort Bragg, North Carolina, to develop Automatic Target Recognition software which required eTreppid to have access to [redacted] material at other contractor and government locations. On August 1, 2005, SOCOM amended the Department of Defense (DOD) contract Security Classification Specification, DD Form 254, permitting eTreppid to store Secret material at the facility.

On or about August 25, 2003, MONTGOMERY received and signed a Security Briefing from Michael S. Allen, Department of the Army, U.S. Army Security Operations Training Facility (SOTF), Fort Bragg, North Carolina, regarding MONTGOMERY's obligation to protect either sensitive or classified material which concern the security of the United States of America due to MONTGOMERY's assignment, employment, or association with SOTF.

On or about September 16, 2003, MONTGOMERY received another Security Briefing from the Defense Security Service, Nellis Air Force Base (AFB), Las Vegas, Nevada, and signed a Standard Form 312, "Classified Information Nondisclosure Agreement", in which

MONTGOMERY was made aware of his obligation to protect from unauthorized disclosure, unauthorized retention, or negligent handling of classified information, marked or unmarked, which could cause damage or irreparable injury the United States or could be used to advantage by a foreign nation.

During the period of November 9, 2005 to November 18, 2005, [redacted], traveled to [redacted] located on the Nellis AFB, and recorded [redacted] video images onto nine eTreppid hard drives for use in the development of the Automatic Target Recognition software. [redacted] marked the nine hard drives with red standard U.S. Government [redacted] labels as instructed by contractor personnel at Nellis AFB and placed a hand written descriptor label on each of the nine hard drives. [redacted] subsequently mailed the nine [redacted] hard drives to eTreppid in Reno, Nevada, and these [redacted] hard drives were stored in a GSA approved safe as required by the DOD. [redacted] Trepp, and MONTGOMERY were the only eTreppid employees with the combination to the safe.

On or about December 6, 2005, [redacted] discovered that the nine [redacted] hard drives were not in the GSA approved safe and notified Trepp who told MONTGOMERY to store the [redacted] hard drives correctly in the GSA approved safe. On or about December 7, 2005, MONTGOMERY told [redacted] all the [redacted] hard drives were stored in a file cabinet in the warehouse. [redacted] informed MONTGOMERY that this was not the correct location to store the [redacted] hard drives and notified Trepp. On December 8, 2005, all nine [redacted] hard drives were returned to a GSA approved safe which was accessible by [redacted], Trepp, and MONTGOMERY.

On or about December 13, 2005, [redacted] was completing work on copying selected data from the [redacted] hard drives to four Mini DV cassette tapes at the request of Trepp. [redacted] found the nine [redacted] hard drives missing from the GSA approved safe and notified Trepp. MONTGOMERY returned all nine [redacted] hard drives to the GSA approved safe. Later on December 13, 2005, [redacted] handed MONTGOMERY two Mini DV cassette tapes labeled [redacted] placed the two other [redacted] Mini DV cassette tapes in the top drawer of the GSA approved

safe and changed the combination so she was the only one with the combination. MONTGOMERY told [redacted] he was condensing the nine original [redacted] hard drives as some were only partially full. MONTGOMERY eventually provided [redacted] with the nine original [redacted] hard drives and six additional hard drives labeled [redacted] by MONTGOMERY. Gray secured the nine original [redacted] hard drives and the six [redacted] hard drives containing copies of the nine original [redacted] hard drives in the bottom drawer of the GSA approved safe. The bottom drawer of the GSA approved safe was only accessible by [redacted] Trepp, and MONTGOMERY.

On or about December 15, 2005, [redacted] again found all nine original [redacted] hard drives missing from the GSA approved safe. MONTGOMERY told [redacted] that he wanted to store the hard drives in the file cabinet in the warehouse. [redacted] informed MONTGOMERY this was not the appropriate way to secure classified content and he was risking losing his security clearance. MONTGOMERY stated "I don't care about my clearance. They'll always give me my clearance because they want me to do the work". [redacted] notified Trepp and Trepp agreed that access to the classified material needed to be restricted and instructed [redacted] to place all classified material in the top drawer of the GSA approved safe. [redacted] changed the combination to the top drawer and was the only eTreppid employee with the combination. [redacted] secured all classified material in the top drawer of the GSA approved safe, to include the nine original [redacted] hard drives.

On or about Sunday, December 18, 2005, MONTGOMERY attempted to contact [redacted] by text message to get access to the classified material. Eventually, Trepp contacted [redacted] by telephone and instructed [redacted] to give MONTGOMERY the combination to the top drawer of the GSA approved safe so MONTGOMERY could work and all classified material would be re-secured on Monday.

On or about December 19, 2005 or December 20, 2005, [redacted], a Software Developer at eTreppid, observed MONTGOMERY delete eTreppid Source Code files from the hard drive installed in [redacted] computer workstation which [redacted] had not recently used. MONTGOMERY stated he deleted the files for security reasons and copies of these files were

accessible on the Source Code Server. At that time, [redacted] observed that more recent Source Code files [redacted] used in [redacted] development efforts remained on [redacted] hard drive installed in [redacted] computer workstation.

On or about December 21, 2005, [redacted] and [redacted] discovered that the Central Processing Unit and RAID storage unit used by MONTGOMERY to backup the Source Code Server was missing. [redacted] asked MONTGOMERY what happened to the Central Processing Unit and RAID storage unit and MONTGOMERY stated he took them home. [redacted] described the missing equipment as a black Lianli Central Processing Unit (CPU) connected to an Ultra Storage eight hard drive RAID storage unit, Model 2081, serial number 6564737. [redacted] stated this equipment is large and heavy. [redacted] has never known MONTGOMERY to remove this equipment from the eTreppid facility as MONTGOMERY used the equipment on a daily basis.

Also on December 21, 2005, [redacted] installed and activated the Internet Security Accelerator (ISA) Server designed to back up all of eTreppid's server's data, including the Source Code Server. Prior to leaving eTreppid on December 21, 2005, [redacted] verified that the ISA Server was operating properly and noted data was being successfully completed from eTreppid servers.

On or about December 22, 2005 [redacted] departed Reno, Nevada, for the Christmas holiday and did not return to Reno, Nevada, until January 3, 2006.

In December 2005, right before the Christmas holiday, [redacted] a Software Developer at eTreppid, noticed the collection of eTreppid Source Code files that [redacted] had stored on the hard drive installed in [redacted] computer workstation had been deleted. [redacted] asked MONTGOMERY about these files and MONTGOMERY explained that he was backing up eTreppid Source Code and would provide [redacted] the portion eTreppid Source Code necessary for [redacted] to work. Between December 25, 2005, and January 1, 2006, [redacted] would request eTreppid Source Code file from MONTGOMERY and MONTGOMERY would place the request Source

Code file on a shared drive where [redacted] retrieved the Source Code file. Upon completing his work on that Source Code file, [redacted] would copy the file back to the shared drive and inform MONTGOMERY who was responsible for copying that file to the Source Code Server.

On or about December 23, 2005, [redacted], an employee at eTreppid, moved six closed boxes from MONTGOMERY's office to the back door of the warehouse at MONTGOMERY's request. [redacted] was not aware of the contents of these boxes. [redacted] observed MONTGOMERY load at least two of these boxes into MONTGOMERY's truck. [redacted] has never known MONTGOMERY to remove anything from the facility in the past.

On or about January 3, 2006, [redacted] returned from vacation and noticed the Source Code Server cabinet and keyboard were in disarray. [redacted] entered the Server Room and found the Source Code Server screen active and could see a process running on the screen. Shortly thereafter, MONTGOMERY entered the Server Room and [redacted] asked MONTGOMERY what he was doing. MONTGOMERY stated he was "cleaning stuff up." [redacted] went to the warehouse to further discuss what MONTGOMERY was doing on the Source Code Server and MONTGOMERY stated he was just "cleaning stuff up" and deleting old files. While in the warehouse, [redacted] noticed the Central Processing Unit and RAID storage unit used by MONTGOMERY to backup the Source Code Server was still missing. On or about January 3, 2006, [redacted] asked MONTGOMERY where was the equipment and MONTGOMERY stated "I'll bring it back, I don't need it anymore."

[redacted] looked at the Source Code Server and found that the majority of the Source Code files contained in specific folders used by the Software Developers had been systematically deleted. [redacted] attempted to access the ISA Server which [redacted] found inoperable and unable to access.

On or about January 9, 2005, Trepp became aware that the Source Code was missing when his employees complained that they were unable to operate their computer systems. Trepp asked [redacted] about the problem and was told by [redacted] that all eTreppid's Source

Code had been deleted from the Source Code Server, the ISA Server, and all of eTreppid's Software Developer's workstations. Trepp confronted MONTGOMERY who said that the Source Code could be located on the 753 removable hard drives located at the company. Trepp instructed eTreppid employees to conduct an analysis of each of the company's 753 hard drives in an effort to locate the Source Code. The two day analysis failed to locate the Source Code.

While looking for the Source Code on eTreppid hard drives, [redacted] located seven hard drives containing copies of the nine original [redacted] hard drives recorded at Nellis AFB in MONTGOMERY's file cabinet. [redacted] checked the drawer in the GSA approved safe where all [redacted] material was to be maintained and found seven more hard drives containing copies of the nine original [redacted] hard drives recorded at Nellis AFB. A complete search of the eTreppid facility failed to locate the nine original [redacted] hard drives recorded or two [redacted] Mini DV cassette tapes containing copied segments of the original [redacted] hard drives. [redacted] stated that [redacted] and MONTGOMERY were the only eTreppid employees with access to the top drawer of the GSA approved safe.

On or about January 10, 2006, Trepp instructed [redacted] to review eTreppid's video surveillance system. [redacted] found that each of the sixteen computer systems were no longer recording video from eTreppid's sixteen cameras. [redacted] also found that all video footage stored on the sixteen computer systems had been deleted.

MONTGOMERY returned to eTreppid on morning of January 10, 2006, when [redacted] asked MONTGOMERY where was eTreppid's Source Code. MONTGOMERY stated it was on 320 gigabyte hard drives in the building. No such hard drives were located. MONTGOMERY again returned to eTreppid later on January 10, 2006, and [redacted] again asked MONTGOMERY where a certain part of the Source Code to which MONTGOMERY stated "he (Trepp) needs to give me big money if he wants it."

Trepp retrieved the annual or periodic copies provided to him by MONTGOMERY over the last seven years from the secure off-site location. [redacted] conducted

a review of the compact disks and hard drives provided by MONTGOMERY and found that these compact disks and hard drives contained no data relevant to eTreppid's development efforts or Source Code except for one program developed in 2002 which is currently not being used.

Trepp advised the MONTGOMERY devoted eight years of his life to developing various software products at eTreppid, including to data compression, pattern recognition, change and anomaly detection. MONTGOMERY worked on these products every day during normal business hours and would often return at night and on weekends to continue his efforts. MONTGOMERY considered some of these capabilities to be of paramount importance to him (MONTGOMERY) that he (MONTGOMERY) would never delegate the project to someone else. Trepp further advised if MONTGOMERY intended to continue work on eTreppid's Source Code, MONTGOMERY would need substantial computing power, similar to the workstation and RAID unit removed from the warehouse, and access to video images contained on the nine Secret hard drives.

MONTGOMERY did not return to eTreppid after January 10, 2006, and has not returned any eTreppid property. MONTGOMERY was terminated as an employee of eTreppid on January 18, 2006.

[redacted]

Based on the conversation MONTGOMERY had with [redacted] and possibly other unknown individuals, it appears that MONTGOMERY may have provided information relating to the Source Code to others and is looking for investors for the Source Code.

[redacted]

[redacted]

Instrumentalities and Evidence of the Crime

As set forth above, there is probable cause to believe that the premises located at 12720 Buckthorn Lane, Reno, Nevada, contains evidence of the offense of Theft of Trade Secrets and Unlawful Retention of National Defense Information. Therefore, the computer hardware, software, computer documentation, passwords, and data security devices further described in Attachment B constitute means of committing criminal offenses. Additionally, there is probable cause to believe that MONTGOMERY has used his computers and related electronic storage devices to collect, store, maintain, retrieve, conceal, transmit, and use electronic data relating to these offenses in the form of electronic records, documents, and materials, including those used to facilitate communications, each of which constitutes evidence of the offense.

Seizure of Equipment and Data

Based on my knowledge, training, and experience, and my conversations with other FBI Special Agents and computer trained personnel, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate

such a computer, be seized and subsequently processed by a certified Computer Forensic Examiner in a laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (such as hard disks, DVDs, compact disks, diskettes, tapes, laser disks, and other storage devices.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data analysis on-site.

b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus it is difficult to know prior to the search which expert possesses sufficient specialized skill to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above reference equipment, software, data, and related instruction be seized and subsequently processed by a certified Computer Forensic Examiner in a laboratory setting. Under appropriate circumstance, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal

from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such--or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readily, quickly, and thus less intrusively, analyzed off site, with due considerations given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number if discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

Analysis of Electronic Data

The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer capable of containing pertinent files, in order to locate the evidence and instrumentalities authorized for seizure by the warrant); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

Based on the investigation [redacted] made to MONTGOMERY, MONTGOMERY appears to have removed the necessary computer equipment and data from eTreppid to continue his development efforts and more likely than not maintains

this computer equipment and data at his residence located at 12720 Buckthorn Lane, Reno, Nevada.

Based on the forgoing, your affiant believes there is reasonable grounds and probable cause to believe that DENNIS LEE MONTGOMERY did steal trade secrets, a violation of Title 18, United States Code, Section 1832, Theft of Trade Secrets, and unlawful retained National Defense Information, a violation of Title 18, United States Code, Section 793(e), Unlawful Retention of National Defense Information.

Wherefore, your affiant requests a search warrant for the premises located at 12720 Buckthorn Lane, Reno, Nevada (further described in "Attachment A") for the purpose of locating and seizing items listed in Attachment B.

MICHAEL A. WEST, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence this 20th day of February 2006.

VALERIE P. COOKE
United States Magistrate Judge

ATTACHMENT A

12720 Buckthorn Lane, Reno, Nevada, is a single family residence located on the westside of Buckthorn Lane. The residence is a single level home having an off-white stucco exterior and an attached three car garage with white garage doors facing Buckthorn Lane. The numbers "12720" are affixed to the southern corner of the garage structure and two planters with small green trees are located on either side of the entryway arch.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Any Black Lianli Central Processing Unit (CPU)

2. Any Ultra Storage eight hard drive RAID storage unit, Model 2081, serial number 6564737.

3 Any address and/or telephone books and papers reflecting names, addresses, telephone numbers, electronic mail addresses, and/or Internet Web site addresses which might identify associates which may relate to potential investors of the Source Code.

4. Any telephone bills and records, and/or calling cards numbers which may relate to potential investors of the Source Code.

5. Any corporate documents, corporate charters, articles of incorporation, list of corporate officers, and/or registered agent applications which may relate to potential investors of the Source Code.

6. Any bank statements, deposit or withdrawal slips, bank checks, money orders, cashier's checks, passbooks, wire transfers, and any other items evidencing the movement of money which may relate to payments made and/or received from potential investors of the Source Code.

7. Any personal or business correspondence, both written forms and electronically stored, to include envelopes and packaging materials which indicate indica of occupancy.

8. Any computer files protected by copyright, including software and movie files, log files, user names and passwords to Internet, mIRC, ftp, or other sites, programs or software used for communication between individuals relating to Dennis Lee Montgomery and other unknown individuals.

9. Any computer hardware, meaning any and all computer equipment including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

10. Any computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the

operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

11. Any computer-related documentation, meaning any written, recorded, printed, or electronically-stored material which explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

12. Any computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

13. Any computer or electronic records, documents, and materials, including those used to facilitate interstate communications, in whatever form and by whatever means such records, documents, or materials, their drafts or their modifications, may have been created or stored, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

14. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

15. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data, in the form of electronic records, documents, and materials, including those used to facilitate interstate communications. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

EXHIBIT “6”

United States District Court

District of Nevada

Bruce R. Thompson U.S. Courthouse and Federal Building
400 South Virginia Street, Room 404
Reno, Nevada 89501

Chambers of Valerie P. Cooke
United States Magistrate Judge

Telephone: (775) 686-5855
Facsimile: (775) 686-5864

FAX TRANSMITTAL

DATE: November 28, 2006

THE FOLLOWING PAGES ARE BEING FAXED TO:

NAME: Michael J. Flynn, Esq. (#1-888-235-4279)
Phillip Stillman, Esq. (#1-888-235-4279)
Ronald Logar, Esq. (#786-7544)
Eric A. Pulver, Esq. (#786-7544)
Paul Pugliese, Esq. (#784-5181)

RE: In the Matter of the search of 12720 Buckthorn Lane

NUMBER OF PAGES INCLUDING COVER SHEET: 34

FROM: The Honorable Valerie P. Cooke
United States Magistrate Judge

PHONE: (775) 686-5855

FAX NO.: (775) 686-5864

If you do not receive all the pages indicated above or the message is poorly received, please contact our office as soon as possible at the phone number above. If the reader of this message is not the intended recipient, please contact our office as soon as possible at the phone number listed above.

ADDITIONAL COMMENTS:

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

In the matter of the search of: 12720 BUCKTHORN LANE, RENO, NEVADA, and 888 MAESTRO DRIVE, RENO, NEVADA, STORAGE UNITS 136, 140, 141, 142, and 143,	3:06-CV-0263-LRH (VPC) 3:06-MJ-0023-VPC **ORDER**

Before the court is a motion by Dennis Montgomery, Brenda Montgomery and the Montgomery Family Trust ("Montgomery") (1) to unseal search warrant affidavits; (2) for the return of property pursuant to Fed. R. Crim. P. 41(g); and (3) for the segregation and sealing of all attorney client and trade secret material seized (#21, 50). The Government opposed (#s 23, 24, & 25) and Montgomery replied (#26). The parties engaged in additional briefing (#s 45, 46, 47, 48, 49, 50, & 51), and the court held an evidentiary hearing on June 29, July 31, and August 17, 2006. Thereafter, the parties submitted post-hearing briefs (#s 74, 76, & 77).

The court has thoroughly reviewed the record and the papers submitted herein, and Montgomery's motion is granted as follows: 1) the search warrant affidavits shall be unsealed, and 2) Montgomery's property shall be returned.[1]

I. HISTORY & PROCEDURAL BACKGROUND

A. Basis for Probable Cause for Search Warrant Applications and Affidavits

Dennis and Brenda Montgomery ("Montgomery") own a home located at 12720 Buckthorne Lane, Reno, Nevada and lease storage space located at 888 Maestro Drive, Reno, Nevada, storage unit numbers 136, 140, 141, 142, and 143 (#21). The Federal Bureau of Investigation ("FBI") searched both

[1]Since the court is ordering the return of Montgomery's property, the request to segregate and seal all attorney-client and trade secret material is denied as moot.

the residence and storage units pursuant to search warrants executed on March 1 and March 3, 2006. *Id.* This court granted the Government's motions to seal the affidavits in support of the warrants (#3, 14). A copy of the warrant and receipt for items seized was left with counsel for Montgomery (#15). On March 8, 2006, returns on the search warrants were executed, and the requisite inventories of items seized were provided to this court. (#15-20).

The Government set forth the original basis for probable cause in the affidavits accompanying the applications for the search warrants (#s 1, 4, 6, 8, 10, & 12).[2] With respect to the search of the Montgomery residence at 12720 Buckthorne Lane, Reno, Nevada, Michael West, Special Agent, Federal Bureau of Investigation ("SA West"), states that he first became involved in the investigation of Dennis Montgomery based on a complaint made by Warren Trepp ("Trepp"), management committee chair of eTreppid Technologies, LLC, of Reno, Nevada (#1). Trepp alleged that Dennis Montgomery, eTreppid's chief technical officer, removed eTreppid computer equipment and storage media containing "source code" files derived from eTreppid's development of certain data compression and pattern recognition software, removed hard disk drives containing "Secret" information provided to the Department of Defense ("DOD"), and systematically deleted source code files from the remaining eTreppid data servers, all in violation of 18 U.S.C. § 1832, Theft of Trade Secrets, and 18 U.S.C. § 793(e), Unlawful Retention of National Defense Information. *Id.*

The basis for probable cause is described in detail below; in sum, the majority of information was provided by Trepp or eTreppid employees. The only other information appears to have come from Neil Azzinaro, a businessperson with whom Montgomery allegedly had a conversation about seeking investors for the source code and/or a new business venture of Montgomery's, and Air Force Special Agent Haraldsen ("SA Haraldsen") with whom Montgomery had conversations about continuing to perform work for the government, independent of eTreppid. To better understand the chronology of events and the complex factual issues giving rise to these searches, the court has divided its discussion of the affidavit into six segments.

---

[2]For the ease of reference, this order will refer to docket #1 as the search warrant affidavit.

1. The Documents Offered in Support of the Affidavit

To establish probable cause for the search warrant SA West relied on three categories of eTreppid documents: 1) a contribution agreement between Montgomery and eTreppid ("contribution agreement"); 2) the eTreppid amended and restated operating agreement ("operating agreement"); and 3) ten patent assignments from Montgomery to eTreppid.

a. The Contribution Agreement - page 2, lines 3-12[3]

SA West attested that Montgomery signed a contribution agreement in which he assigned his rights to "contributed assets" to eTreppid in exchange for fifty percent management interest in eTreppid. According to the affidavit, "contributed assets" included trade secrets, patent rights, copyrights, licenses and permits, software programs and source codes, etc. (#1, 2:3-12). The court drew the inference from this summary of the contribution agreement that Montgomery assigned *all* intellectual property and related property he owned to eTreppid because that is what the plain meaning of the excerpt of the contribution agreement states.

b. The eTreppid Amended and Restated Operating Agreement - 2:13-25; 3:1-4

Montgomery also signed an amended and restated operating agreement of eTreppid Technologies, and SA West quoted a provision of that agreement which states that Montgomery agreed to devote substantially all of his time and efforts to the business and affairs of eTreppid and also restricted Montgomery's independent activities; in other words, it is a non-compete agreement. According to the affidavit, Trepp considered eTreppid's trade secrets to be various software programs relating to data compression pattern recognition, change and anomaly detection, among other things. *Id.* at 3:10-13.

c. Ten Patent Assignments from Montgomery to eTreppid - 3:5-16

Finally, SA West identified ten patents that Montgomery, as an eTreppid employee, assigned to eTreppid in 2000-2001. *Id.* at 3:5-9. The affidavit states that through these patent assignments,

---

[3]The references that follow are to the page and line numbers in SA West's affidavit in support of the search warrant (#1).

Montgomery assigned full and exclusive use of the technologies described in the patents to eTreppid. The next paragraph of the affidavit describes "trade secrets," which the court inferred were the patented technologies Montgomery assigned to eTreppid in 2000-2001: software programs relating to data compression, pattern recognition, and change and anomaly detection. *Id.* at 10-16.

2. The Source Code and eTreppid Security - 3:17-26; 4:1-12

The next section of the affidavit is devoted to a description of the protocols eTreppid established to insure the security for the source code files, which contained data compression and pattern recognition software. *Id.* at 3:17-26. The affidavit states that only two eTreppid employees, Montgomery and Sloan Venables ("Venables"), had access rights to duplicate, modify or delete source code. The affidavit describes Montgomery's responsibility to maintain a back-up copy of the source code server data on specifically described hardware units, and that Trepp required Montogomery to provide him with current source code files, which Trepp stored at a secure off-site location. *Id.* at 4:7-9. The affidavit then summarizes eTreppid's locks, alarm system and video surveillance system. *Id.* at 4:10-12.

3. The SOCOM Contract and Montgomery's Security Clearance - 4:13-26; 5:1-4

Having established ownership of the technology in eTreppid, Montgomery's role in the work of eTreppid, and the sophisticated security system in place at eTreppid, the affidavit turns to a March 2003 agreement between eTreppid and U.S. Special Operations Command ("SOCOM"), which required eTreppid to have access to secret material. *Id.* at 4:13-18. The affidavit states that eTreppid was permitted to store secret material onsite pursuant to DD Form 254. *Id.* at 4:16-18.

The affidavit then states that Montgomery received and signed two security briefings in August and September of 2003, which outlined his obligation to protect classified material of concern to the United States, to protect unauthorized disclosures, and to prevent negligent handling of marked or unmarked classified information, which could irreparably damage the United States and be used to advantage by a foreign nation. *Id.* at 4:19-26; 5:1-4.

4. November 2005 Visit to Nellis Air Force Base and the Nine Secret Hard Drives - 5:5-13

In the next section of the affidavit, SA West develops the chronology of events concerning the "nine eTreppid hard drives," which are then characterized as the "nine Secret hard drives," and ultimately transformed into "classified material." In November 2005, Patty Gray ("Gray") of eTreppid visited the Predator Drone Operations Center at Nellis Air Force Base where she recorded "Secret Predator Drone video images" onto nine eTreppid hard drives for use in developing "Automatic Target Recognition" software. *Id.* at 5:5-8. The affidavit states that pursuant to instructions from "contractor personnel at Nellis AFB," Gray marked these nine hard drives with "red standard U.S. Government Secret labels" and mailed them to eTreppid's facility in Reno. *Id.* at 5:8-11. The nine secret hard drives were stored in a GSA-approved safe as required by the DOD. Gray, Trepp and Montgomery were the only persons with access to the safe. *Id.* at 5:11-13.

5. December 2005: Montgomery's Breaches of Protocol, Deletion of Classified Material and Trade Secrets, and Removal of Classified Material and Trade Secrets from eTreppid - 5:14-26; pages 6, 7, 8, 9, and 10

This portion of the affidavit recounts the events which led to the allegations of theft of trade secrets and unlawful retention of national defense information. According to SA West's affidavit, during December 2005, Gray and other eTreppid employees noticed that Montgomery was not following the standard protocols for use and storage of the nine secret hard drives. Gray discovered on two occasions that Montgomery was not properly securing them in the safe, and they were returned after Montgomery was questioned. *Id.* at 5:14-26;6:1-7. Despite these incidents, Gray continued to find the nine secret hard drives missing from the safe, and Trepp intervened to insure that all "classified material" be kept in the top drawer of the safe. *Id.* at 6:13-17. Gray changed the combination to the top drawer of the safe, and she was the only eTreppid employee who had it. *Id.* at 6:15-17.

Montgomery requested access to the classified material, and Trepp not only gave Montgomery authorization; he also instructed Gray to give Montgomery the combination to the top drawer of the safe, which she did. *Id.* at 6:18-22. From December 18th until December 21st, other eTreppid employees reported that Montgomery was deleting eTreppid source code files and that certain computer hardware

was missing. *Id.* at 6:23-26;7:1-6. When asked about the missing equipment, Montgomery responded that he had taken the equipment home, although the eTreppid employee who reported the missing equipment had never known Montgomery to take this equipment home. *Id.* at 7:6-12.

Prior to leaving for the holidays, Venables installed software to back up all of eTreppid's server data, including the source code server, and he verified that it was operating properly before his departure. *Id.* at 7:13-17. Two key eTreppid employees, Gray and Venables, departed for the holidays on December 22, 2005, and did not return until January 3, 2006. *Id.* at 7:18-19. During their absence, one eTreppid employee discovered portions of the eTreppid source code he was working on had been deleted, and when he asked Montgomery about this, Montgomery advised he would provide the employee with the source code he needed to do his work. *Id.* at 7:20-26;8:1-3. Montgomery also asked another eTreppid employee to load some boxes into Montgomery's truck, which had never happened before. *Id.* at 8:4-8. After Venables returned from the holidays in January, he noticed that the source code server cabinet and keyboard were in disarray and the screen was active. *Id.* at 8:9-10. When he asked Montgomery about this, Montgomery responded that he was "cleaning up stuff," but when Venables went into the warehouse, he also noticed that the units Montgomery used to back up the source code server were still missing. *Id.* at 8:13-17. Montgomery told Venables he would bring back the equipment, as he no longer needed it. *Id.* at 8:17-19. When he looked at the source code server, Venables discovered that most of the folders used by the eTreppid software developers had been deleted, and he could not access the ISA server either. *Id.* at 8:20-23.

Shortly thereafter, Trepp became aware source code was missing when employees complained that they could not operate their computer systems, and Venables reported that all source code had been deleted from the source code server, the ISA server, and all of the software developers' work stations. *Id.* at 8:24-26;9:1-2. Although Montgomery then told Trepp that the source code could be located on removable hard drives, a two-day analysis failed to locate the source code. *Id.* at 9:3-5. It was also at this time that Gray found seven hard drives containing copies of the nine original secret hard drives from Nellis AFB in Montgomery's file cabinet, and she found seven additional hard drives also containing copies of the nine original hard drives in the safe. *Id.* at 9:6-10. A search of the eTreppid facility failed

to locate the nine original secret hard drives, and Gray and Montgomery were the only employees with access to the top drawer of the safe. *Id.* at 9:10-14. At Trepp's request, Venables reviewed all of the video surveillance cameras and found that none was recording video, and he also discovered that all stored video had been deleted. *Id.* at 9:15-18.

Despite Montgomery's assurances that the source code was stored on hard drives in the building, the hard drives were never located, and on his last day at eTreppid, Montgomery was reported to have said that if Trepp wanted the source code, "he [Trepp] needs to give me big money if he wants it." *Id.* at 9:19-24. Montgomery never returned to eTreppid and he was terminated on January 18, 2006. *Id.* at 10:14-16. Warren Trepp told SA West that Montgomery had devoted eight years of his life to developing software products at eTreppid, that Montgomery worked on these products every day and on weekends, that Montgomery would never delegate these projects to anyone else, and that in order to continue this work, Montgomery would require substantial computing power, similar to the workstation and RAID unit removed from the warehouse, and have access to the nine secret hard drive video images. *Id.* at 10:4-13.

6. Montgomery's Conversations with Neil Azzinaro and Special Agent Paul Haraldsen ("SA Haraldsen") – p. 10:17-24; 11:1-26; 12:1-7

Apart from the information provided SA West from Trepp and eTreppid employees, SA West also relied on two other individuals who had conversations with Montgomery during this same time period. The first is Neil Azzinaro, a casino host and Montgomery's friend. In a January 2006 conversation, Montgomery recounted the business dealings of Trepp, Montgomery's unhappiness that he had not received a raise, and Montgomery's interest in looking for individuals who would invest several million dollars. *Id.* at 10:17-23. Montgomery specified the investor would have to be an individual with United States citizenship. *Id.* at 10:23-24. SA West stated that based on this conversation with Azzinaro, and possibly others, it appeared that Montgomery may have provided source code to others and was looking for investors for the source code. *Id.* at 11:1-3.

In mid-February 2006, SA West was contacted by SA Haraldsen, Air Force Office of Special Investigations, Pentagon. During this period SA Haraldsen placed consensual, recorded telephone calls

with Montgomery. During these calls, Montgomery made several representations to SA Haraldsen: 1) that Trepp did not have the capability to continue the work; 2) that Montgomery had made certain that the assets of the U.S. Government were protected; 3) that if the work is to continue, it must be through Montgomery; and, 4) that the capability to do the work continued to exist. *Id.* at 11:4-10. SA Haraldsen and Montgomery had two additional telephone calls on February 24, 2006, during which Montgomery indicated he might just give the technology to the government, and when SA Haraldsen asked for proof that the technology still exists, Montgomery became agitated. *Id.* at 11:11-17. Later that same day, Montgomery purchased computer disks, and business card stock. *Id.* at 11:18-21.

Finally, on February 26, 2006, Montgomery telephoned SA Haraldsen again and expressed concerns about supplying SA Haraldsen with information about anomaly detection and pattern recognition technical capabilities, as to do so might violate a temporary restraining order filed against him by eTreppid. *Id.* at 12:1-7.

Based upon SA West's affidavit, the court found probable cause existed that Montogmery may have unlawfully retained classified material and stolen trade secrets, and it issued the search warrant. The court also granted the Government's motion to seal the affidavit (#3).

B. The Search Warrants for the Storage Units

With respect to the search of the storage units, SA West's affidavit sets forth the following basis for probable cause: the CPU and RAID storage unit used by Montgomery and the nine original secret hard drives were not located during the search of the residence of Buckthorne Lane (#4, 6, 8, 10, 12). Montgomery rented five storage units at Double R Storage in Reno, Nevada. *Id.* The storage units were accessed a total of ninety-two times between November 1, 2005 and March 3, 2006. *Id.* Double R Storage's video surveillance showed that a truck registered to Brenda Montgomery entered the facility on March 3, 2006, an individual walked between the storage unit and the truck, but no observable items were taken from or transported to the truck. *Id.* SA West stated that this constituted probable cause to believe that the storage units contained the evidence of theft of trade secrets and unlawful retention of national defense information. *Id.* Based upon SA West's affidavit, the court found probable cause

existed for issuance of these search warrants, and the court also ordered these search warrant affidavits sealed (#14).

The court granted the Government's motion to seal the search warrants and affidavits because the Government argued that the information contained therein related to proprietary intellectual property and national security classified materials (#3, 14).

C. Search Warrant Returns

The following items were seized from the Montgomery residence:

HP Pavilion laptop
6 SanDisk compact flash cards
letter on white paper and yellow pages of ripped up paper
rolodex
15 computer CDs
white shredded paper
miscellaneous post-it notes
Network Solutions account paperwork 4 pages
check stubs – Montgomery Family Trust
Western Digital hard drive serial number WEAL 71844911
Grante digital devserver labled 12/17/2005 serial number F05090650042-A
silver CPV (tower) labeled ATI 3
16 computer CDs
3 pieces of paper containing phone numbers
Grante digital server labeled DEO 1/2/06 PROG
8 containers of medicine, each with 40-168 tablets

(#15).

The following items were seized from storage unit 140:

1 yellow/gray case containing eTreppid disks
7 compact disks
9 mini DV cassettes
1 Sony Hi8 video cassette
1 USB (black 2.0 flashback)
1 256MB SanDisk compact flash card
1 IBM travel star hard drive serial number V29CH7080N5
11 sealed Western Digital hard drives
1 TDK mini DV video cassette
10 various manufacturer hard drives
1 box containing 78 compact disks
bank statements 12/2005 through 1/2006
financial documents and phone bills
1 removable hard drive labeled "Dennis Eyes Only" and 1 compact disk labeled eTreppid

(#17).

No items were seized from the other four storage units searched (#16, 18, 19, 20).

D. Chronology of Motions

On March 10, 2006, Montgomery filed a motion to unseal the search warrants and affidavits and for the return of property pursuant to Fed. R. Crim. P. 41(g) and for the segregation and sealing of all attorney-client privileged materials seized (#21). Montgomery argued that he has a Fourth Amendment right to view the search warrant affidavits and that the Government cannot show a compelling governmental interest that cannot be served by a less restrictive means than withholding the entire affidavits. *Id.* Next, he contended that the warrants are facially invalid because they lack specificity and are overbroad. *Id.* Therefore, Montgomery asserted that he is entitled to the return of his property. *Id.* Finally, Montgomery also sought to have attorney-client privileged information segregated prior to any inspection by the Government. *Id.* Montgomery's overarching argument is that the entire investigation stems from Trepp having convinced the United States Attorney to use the power of the federal government to achieve what Trepp could not accomplish through a civil action – a search of Montgomery's property in an effort to obtain certain technology. *Id.*

The Government filed three separate responses (#23, 24, 25). In its response to the Rule 41(g) motion, the Government first argued that because the balance of the equities favored the Government, the court should decline to consider the merits of this pre-indictment Rule 41(g) motion (#23). The Government further asserted that it would produce evidence at an evidentiary hearing to demonstrate that probable cause for the searches existed, that the warrants were valid, and to refute Montgomery's assertions regarding how the searches were executed. *Id.* In its response to the motion to unseal the search warrant affidavits, the Government contended that Montgomery failed to support his position that he has a constitutional right for pre-indictment review of the affidavits (#24). The Government also asserted that its interests in maintaining the secrecy of the information in the affidavits including: (1) the premature identification of possible witnesses; (2) the possibility that such witnesses could be compromised or influenced; (3) the possibility that potential subjects could alter, remove, or destroy information sought by the Government; and, (4) that the affidavits identify specific, sensitive information. *Id.* Finally, the Government opposed the motion to seal and segregate all attorney-client privileged information and trade secrets prior to the DOD conducting an analysis of the seized electronic

storage media and documents for classified information and information relating to the national defense (#25). Montgomery replied to the government's oppositions (#26).

The court set a sealed evidentiary hearing for May 3, 2006, on the motion to unseal the affidavits, return the property pursuant to Rule 41(g) and segregate attorney-client privileged information and trade secrets (#27). On April 19, 2006, the court further ordered that the parties file simultaneous supplemental briefs concerning certain specific issues identified by the court (#28). On April 28, 2006, the Government filed a partial compliance with court order of April 19, 2006 (#31). The Government explained that it had provided redacted affidavits to Montgomery and did not oppose supplemental filings by Montgomery subsequent to his review of the affidavits. *Id.* The Government argued that the redacted information could (1) expose witnesses; (2) identify investigative techniques prior to completion of the investigation; (3) interfere with the identification of other suspects; and (4) interfere with the recovery of equipment that may contain evidence of criminal violations. *Id.* Also on April 28, 2006, the court vacated the hearing set for May 3, 2006 and vacated the order for supplemental briefing (#32). The court stated that there appeared to be serious concerns about the search warrants issued by the court as they relate to certain classified information. *Id.*

On May 8, 2006, the Government moved for a protective order prohibiting disclosure of classified information (#34). Montgomery opposed (#36, 39), and the Government replied (#38). The court held a hearing and denied the motion (#42). At the hearing, the Government provided Montgomery with redacted versions of the applications and affidavits for the search warrants,[4] which were supplemented on June 1, 2006 (#40, 41, 43, 44). The only portions of the affidavits that remain redacted, after the supplements, are the conversation between Montgomery and a business friend about finding investors for the source code, and Montgomery's telephone conversations with SA Haraldsen. *Id.*; *compare* #40 at 10-12 to #1 at 10-12.

[4]It is unclear whether this is the second redacted version of affidavits provided by the Government, or the same version referred to in Government's partial compliance with court order of April 19, 2006 (#31).

On June 2, 2006, Montgomery filed a supplemental memorandum in support of his motion to unseal the affidavits, return the property, and seal attorney-client communications (#45). Montgomery again stated that the court need not hold an evidentiary hearing on the Rule 41(g) issues. *Id.* The Government filed a response to issues identified in court minute order of April 19, 2006 (#46). The Government noted in parentheses that recent information provided by the DOD indicated that the information was not classified. *Id.* at 2. The Government argued that the search warrants set forth probable cause and described the items sought as specifically as possible. *Id.* The Government did not explain whether the determination that the information was improperly classified affects whether probable cause for the search existed, and thus apparently took the position that probable cause existed independent of the belief that classified information was sought. *Id.* The Government provided a declaration by SA West which describes the execution of the searches in detail (#47). The Government still sought to establish a protocol to screen attorney-client privileged material and suggested two alternatives (#46).

Upon receipt of the redacted affidavits and the supplements, Montgomery filed a second supplemental memorandum in support of its motion to unseal the search warrant affidavits, for the return of property pursuant to Rule 41(g), and to segregate privileged material (#48, 49, 50). Montgomery then requested an evidentiary hearing, arguing that a hearing is the only way to pin down the Government's shifting positions (#50). He asserted: "The Government has essentially admitted that it did not raid Mr. Montgomery's property to retrieve 'classified information being in a place it shouldn't be;' but rather to do the bidding of wealthy Warren Trepp and thrust itself into a private, civil dispute between the two owners and founders of eTreppid Technologies. The search for 'classified information' was obviously only the cover story seeking to justify the search." *Id.* Montgomery also stated that Assistant United States Attorney Pugliese informed Montgomery's counsel that the "classified information thought to be in Mr. Montgomery's possession had been found." *Id.* at 3. Montgomery's counsel included his declaration that he had conversations with AUSA Pugliese and SA West, during which they discussed approximately ten compact discs, which were the only materials marked "classified" and the only

material sought in the search (#49). Montgomery questioned why the Government did not list that information or the storage media containing it in the search warrants (#50).

The court held an evidentiary hearing over the course of three days, which concluded on August 17, 2006. At the conclusion of the final day of the hearing, the court directed the parties to file post-hearing briefs (#67). The Government filed three separate post-hearing briefs addressing Montgomery's motion to unseal search warrant affidavits (#74), the motion to seal and segregate all attorney-client and trade secret information (#76), and the motion for return of the seized property (#77). Montgomery filed a consolidated brief regarding all three issues (#80).

II. DISCUSSION AND ANALYSIS

A. Equitable Jurisdiction over Rule 41(g) Motion to Return Property

Federal Rule of Criminal Procedure 41(g) generally is used to seek the return of property after an indictment is issued; however, "district courts have the power to entertain motions to return property seized by the government when there are no criminal proceedings pending against the movant." *Ramsden v. United States,* 2 F.3d 322, 324 (9th Cir. 1993). "These motions are treated as civil equitable proceedings, and, therefore, a district court must exercise 'caution and restraint' before assuming jurisdiction." *Id.*

Before the court can reach the merits of a pre-indictment motion pursuant to Rule 41(g), the court must consider whether: (1) "the Government displayed callous disregard for the constitutional rights of the movant; (2) the movant has an individual interest in and need for the property he wants returned; (3) the movant would be irreparably injured by denying return of the property; and (4) the movant has no adequate remedy at law for the redress of his grievance." *U.S. v. Kama,* 394 F.3d 1236, 1238 (9th Cir. 2005) (internal citations omitted). If the balance of equities favors reaching the merits, the court should exercise its equitable jurisdiction to entertain the Rule 41(g) motion. *Ramsden,* 2 F.3d at 326.

1. Callous Disregard

Here, the Government has conceded that *none* of the seized material is classified; therefore, there is a question whether the Government displayed callous disregard for Montgomery's constitutional rights. SA West testified that the central focus of the search was classified information: ". . . [The search

warrant] was based on the possession of classified information. Obviously there's a lot of things going on at eTreppid, but nothing was more influential than the information that [Montgomery] may have been in possession of secret information." Tr. II, 144:17-19.[5] As will be more fully discussed herein, the court concludes that the Government acted in callous disregard of Montgomery's rights.

2. Individual's Interest in and Need for the Property

Montgomery has established that the seized property includes items covering many years of his work as a computer programmer, an inventor, as well as items of personal family property (#21, 26; Tr. Ex. 38). Many of the items seized are also integral to the two civil actions pending between Montgomery and Trepp/eTreppid. *Id. See In re Singh,* 892, F.Supp. 1, 3 (D.D.C. 1995).

3. Irreparable Harm

In addition to the concerns identified above regarding Montgomery's interest in and need for the property, he contends that some of the seized information includes attorney-client privileged information, which will be compromised if a third party reviews it. *See id.* at 3-4.

4. No Adequate Remedy at Law

The Government has denied Montgomery is a target, and there has never been any indication that either Ms. Montgomery or the Montgomery Family Trust is a search warrant target. Nine months have passed since the Government executed the search warrants, and it appears there are no current plans to prosecute any of the movants. *See Ramsden,* 2 F.3d at 326 (movant does not have the opportunity to challenge the seizure of the documents and request their return at a later date, without a current plan to prosecute). Mindful that Montgomery has not been indicted, the balance of equities favors reaching the merits of his 41(g) motion. *Id.* at 4.

The court now considers Montgomery's requested relief: (1) the unsealing of the redacted portions of the search warrants affidavits, and (2) the return of the seized property.

B. Right to View Affidavits

---

[5]Transcript I is the transcript of the June 29, 2006 evidentiary hearing.
Transcript II is the transcript of the July 31, 2006 continued evidentiary hearing.
Transcript III is the transcript of the August 17, 2006 continued evidentiary hearing.

Some courts have held that no right to inspect sealed affidavits for search warrants exists under the Constitution or the Federal Rules of Criminal Procedure prior to the initiation of a criminal proceeding against the movant. *See Matter of Eyecare Physicians of America*, 100 F.3d 514, 517 (7th Cir. 1996); *Matter of the Search of S & S Custom Cycle Shop*, 372 F.Supp.2d. 1048, 1051-52 (S.D. Ohio 2003).[6] The court in *Eyecare Physicians* applied a "right of access committed to the sound discretion of the court." *Eyecare Physicians*, 100 F.3d at 517.

Other courts have held that a search target has a pre-indictment Fourth Amendment right to examine the search warrant affidavit. *In re Search Warrants Issued on April 26, 2004*, 353 F.Supp. 2d 584, 585 (D. Md. 2004), *see also United States v. Oliver*, 208 F.3d 211, 2000 WL 263954 (4th Cir. 2000) (unpublished opinion); *In re Search Warrants Issued Aug. 29, 1994*, 889 F.Supp. 296, 299 (S.D. Ohio 1995); *In re the Search of Up North Plastics, Inc.*, 940 F.Supp. 229, 232 (D. Minn. 1996). The right is not unqualified; the Government bears the burden to "demonstrate compelling government interests in keeping the affidavit under seal and . . . that no less restrictive means, such as redaction, is available to prevent disclosure." *In re Search Warrants Issued on Apr. 26, 2004*, 353 F.Supp. 2d at 587. The United States District Court for the District of Maryland emphasized that the plain words of the Fourth Amendment protect the public from unreasonable intrusions and specifically require that probable cause support search warrants. *Id.* at 588. The Court reasoned that "implicit in that language is the public's right to challenge both the reasonableness of the search and the degree to which the warrant was supported by probable cause." *Id.* The Court invoked Justice Harlan's statement that "constitutional provisions for the security of person and property should be liberally construed" and concluded that without a right to access the affidavit upon which a search warrant is based, a search target could never challenge the warrant for probable cause. *Id.* "More than a conclusory allegation

---

[6]In *Search of S&S Custom Cycle Shop*, the court stated that "Absent the existence of a criminal action, an individual simply has no basis for bringing a motion to unseal an affidavit under the Criminal Rules. If it is a constitutional right, such as the Fourth Amendment right to be free from unreasonable search and seizures, that has been violated by federal authorities, vindication is civil in nature and can be achieved through a *Bivens* action." 372 F. Supp. 2d at 1051.

about the need to protect a continuing investigation is necessary to meet the Government's burden of showing compelling need" to keep the affidavits sealed. *Up North Plastics*, 940 F.Supp. at 232.

Apart from the arguments it advanced initially to seal the entire affidavit – generalized concerns that unsealing will reveal witnesses, investigative techniques, or compromise on ongoing criminal investigation – the Government has not explained why remaining portions of the affidavit should still remain redacted (#74). The Government contends the standard in the Ninth Circuit for unsealing such information is the balancing test established in *United States v. Napier*, 436 F.3d 1133, 1137 (9th Cir. 2006). However, *Napier* had nothing to do with a search target's pre-indictment Fourth Amendment right to review a search warrant affidavit; rather, it concerned a post-indictment challenge to a search warrant that the defendant sought to unseal in order to make the "substantial preliminary showing" required by *Franks v. Delaware,* 438 U.S. 154, 155-56 (1978). In that instance, the court rejected the view that *Franks* creates an unlimited right to all information possibly needed to meet the preliminary showing requirement and held that the court must balance the defendant's interests against those of the government. *Napier* at 1133.

The court has considered the authorities addressing a search target's pre-indictment Fourth Amendment right to review the search warrant and concurs with those courts that have required the Government to "demonstrate compelling government interests in keeping the affidavit under seal and . . . that no less restrictive means, such as redaction, is available to prevent disclosure." *In re Search Warrants Issued Apr. 26, 2004,* 353 F.Supp. 2d at 587.

Turning to the evidence in this proceeding, the redactions involve direct and recent contacts Montgomery had with other individuals, and it is difficult to imagine that the Government is concerned about revealing identities of witnesses or protecting an ongoing investigation. In fact, Montgomery has already surmised that part of the redaction relates to seeking investors for the source code (#50). Moreover, at the June 29, 2006 evidentiary hearing, SA West revealed the identity and involvement of SA Haraldsen during his testimony. Tr. I, 15. Accordingly, the court finds that the Government has not met its burden to establish a compelling government interest in keeping the remaining portions of the affidavits sealed, and it further finds that Montgomery has a right to view the affidavits in their entirety.

C. Return of Montgomery's Seized Property Based Upon Lack of Probable Cause

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. "A search warrant . . . is issued upon a showing of probable cause to believe that the legitimate object of a search is located in a particular place, and therefore safeguards an individual's interest in the privacy of his home and possessions against the unjustified intrusion of the police." *U.S. v. Adjani*, 452 F.3d 1140, 1145 (9th Cir. 2006) quoting *Steagald v. United States*, 451 U.S. 204, 213 (1981). The United States Supreme Court has

> reaffirm[ed] the totality-of-the-circumstances analysis that traditionally has informed probable-cause determinations. The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for conclu[ding] that probable cause existed.

Illinois v. Gates, 462 U.S. 213, 238-39 (1983). The Supreme Court also explained that the "probable cause standard . . . is a practical, nontechnical conception." *Id.* at 231. Further, "probable cause is a fluid concept – turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules. *Id.* at 232. "[A]n affidavit may be based on hearsay information and need not reflect the direct personal observations of the affiant, so long as the magistrate is informed of some of the underlying circumstances supporting the affiant's conclusions . . . ." *United States v. Ventresca*, 380 U.S. 102, 108 (1965).

"In assessing whether a warrant passes constitutional muster, a court is therefore obliged to make two inquiries: first, whether the scope of the search authorized by the warrant was justified by probable cause and, second, whether the warrant was sufficiently particular to limit the discretion of the officers." *In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853, 856 (9th Cir. 1997). If the court finds that a search warrant lacked probable cause and, thus, that movant was aggrieved by the unlawful search and seizure of his property, Rule 41(g) dictates the remedy: "the court must return

property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings." Since this court finds that the Government lacked probable cause, as more fully explained below, the court does not reach the particularity analysis.

Montgomery argues that no probable cause supports SA West's affidavits in support of the search warrants (#21). The Government responds that SA West properly investigated Trepp's allegations, including interviewing Trepp and other employees and compiling information SA Haraldsen provided (#23). It is now clear that no probable cause existed to believe that Montgomery had removed classified information from eTreppid and improperly stored it at his home because after the warrants issued, it was determined that the material was, in fact, not classified (#46; Tr. Ex. 4). As noted earlier, SA West testified that the central focus of the search was classified information: ". . . [the search warrant] was based on the possession of classified information. Obviously there's a lot of things going on at eTreppid, but none was more influential than the information that [Montgomery] may have been in possession of secret information." Tr. II, 144. Three months after the search was executed, the Government determined that the information sought was not classified. Tr. I, 123.

In light of this very critical fact, the court now examines SA West's affidavit and testimony at the evidentiary hearing to determine whether probable cause exists to support the search warrants.[7]

1. Documents Offered in Support of the Affidavit

SA West relied on three documents discussed below to support a finding that there was probable cause to believe Montgomery had stolen eTreppid's trade secrets.

a. The Contribution Agreement

As noted earlier, SA West referred to the 1998 contribution agreement, and he quoted an excerpt from the agreement which stated that Montgomery contributed *all* of his intellectual property, software programs, and source codes to eTreppid; therefore, this court inferred that eTreppid owned *all* of the assets described in the balance of SA West's affidavit. This inference was incorrect. At the evidentiary

[7]For ease of reference, the court considers SA West's affidavit in the same order set forth in the section of this order entitled "procedural history," *supra*, at pages 3-8.

hearing, the entire contribution agreement was admitted into evidence, and the relevant portions state as follows:

> 1.2 Contributed Assets. As used in this Agreement, the term "Contributed Assets" shall mean and include, collectively, all the following assets, together with all of Contributor's rights, title and interest therein, tangible and intangible, present or future, including, but not limited to, all development, distribution and exploitation rights, or to any proceeds derived therefrom:
>
> 1.2.1 All of Contributor's know-how; trade secrets; patent rights, copyrights, trademarks, licenses and permits, registered or unregistered, pending or approved; software programs and all programming and source codes used in connection therewith or otherwise required to operate any component thereof; and all programming documentation, designs, materials and other information, all in whatever form and wherever located, relating to or used in connection with, or otherwise describing or consisting of any part of, the software compression technology *contained on that certain Software Compression Engine Development Program contained on CD No. 1, all of which is being contributed by Contributor hereunder (collectively, the "Technology").*
>
> 1.2.2 Certain of Contributor's tangible personal property used in connection [sic] the Technology as more particularly described on SCHEDULE 1.2.2 attached hereto and made part of this Agreement.
>
> 1.2.3 All of Contributor's books and records relating to the Contributed Assets.
>
> *1.3 Excluded Assets and Liabilities. Notwithstanding any of the foregoing, Contributor is specifically not contributing, transferring or conveying to INTREPID under this Agreement or by any other means, nor is INTREPID acquiring from Contributor, any other tangible or intangible assets of Contributor not specified herein, and expressly is not assuming any claims, liabilities or obligations of Contributor of any kind or nature, whether existing as of the Closing Date or arising thereafter, on account of Contributor's ownership, development, exploitation or operation of the Contributed Assets at any time prior to the Closing Date.*

Tr. Ex. 7 (emphasis supplied).[8]

Had this court been provided the entire contribution agreement, it would have concluded that whatever is on CD No. 1 – nothing more and nothing less – belonged to eTreppid. The court would have expected the Government to demonstrate there was probable cause to believe that CD No. 1 contained the disputed trade secrets. However, SA West testified that he does not know what CD 1 contains, and

[8]INTREPID was the predecessor of eTreppid.

he never inquired as to how long Montgomery has been creating software technologies. Tr. I, 51, 53, 60. SA West did not investigate whether Montgomery had created software that was not contributed under the contribution agreement or ask what assets Montgomery had not contributed. Tr. I, 60. SA West stated that the fact that his affidavit does not refer to CD No.1 was not intended to mislead the court. Tr. II 124. His impression was that any work that Montgomery performed while at eTreppid was also part of what eTreppid owned; he did not believe that it was limited to CD No. 1. Tr. II, 124. Montgomery's counsel and SA West had the following exchange:

> Counsel: . . . as I understand your testimony today you're saying that notwithstanding paragraph 1.3 [of the Contribution Agreement], excluding everything if it's not specified, you thought that [Montgomery] conveyed everything, patents, trademarks, copyrights, didn't limit it to CD No. 1.
>
> SA West: No, I think what the – my thought at the time was that that agreement was in 1998 and that the CD and the particular CD 1 was conveyed. We're in 2005. He has worked there for eight years working on various projects for eTreppid, one as the chief technology officer. They've employed ten other programmers to do the programming, and what he took wasn't just his.

Tr. II, 124. This interchange conveys SA West's fundamental misunderstanding of the operating agreement and the business relationship between Montgomery and eTreppid.

On the final day of the evidentiary hearing SA West was once again asked about CD No. 1 and the discrepancy between the entire contribution agreement and the excerpt quoted in his affidavit. SA West testified that he received an incomplete copy of the contribution agreement from SA Haraldsen, who had sent it to him in a different "landscape format;" therefore, the crucial reference to CD No. 1 was cut off. *See* Tr. Ex. 31; Tr. III, 47-54. SA West testified that he did not realize the tops of each page were missing until Government's counsel pointed it out to him. Tr. III, 52:17-53:6. The court finds SA West's explanation difficult to comprehend, since one has only to read Exhibit 31 to realize that it is quite obviously an incomplete document with missing sentences and paragraphs. Yet, it is this fatally incomplete document that SA West relied on to obtain the warrants to search Montgomery's home and the storage units for stolen trade secrets.

b. The eTreppid Operating Agreement

SA West quoted an excerpt from the operating agreement in his affidavit, which led this court to conclude that Montgomery was contractually bound by a non-compete agreement; therefore, Montgomery was prohibited from developing or purchasing any software programs or technology competitive with eTreppid, or in engaging in any similar business to that of eTreppid. However, at the evidentiary hearing the entire operating agreement was admitted, and it, too, revealed that SA West omitted a critical phrase from the sentence he quoted in his affidavit:

> 6.6. **Restriction on Independent Activities; Agreement not to Compete.** *So long as MONTGOMERY is appointed a Committee Member and/or as Chief Technology Officer pursuant to this Agreement,* MONTGOMERY and his Affiliates agree that, during the terms of this Agreement, non of them shall compete with the LLC, whether for their own account and/or for the account of others, individually, jointly with others, or as a part of any other limited liability company, limited partnership, general partnership, joint venture, corporation, or other entity, by: (i) developing, licensing or exploiting in any manner any software programs or other technology which is competitive with the Technology or the Business of the LLC, or providing any services or supplies which are encompassed within the definition of the "Business" of the LLC as set forth in this Agreement; (ii) purchasing or otherwise acquiring, owning, holding, operating, managing, investing in or otherwise disposing of a like business of the LLC's Business and interests therein of any kind or nature; or (iii) otherwise engaging in any or all aspects of a like business of the LLC's Business. MONTGOMERY's or his Affiliates' participation in any of the activities restricted by this paragraph shall be deemed a breach of his duties and obligations as a Committee Member hereunder.

Tr. Ex. 30 (emphasis in italics supplied). SA West omitted the beginning phrase of paragraph 6.6, which expressly limits the non-compete to Montgomery's tenure as a committee member or chief technology officer. Based on SA West's omission, this court drew the incorrect inference that in addition to giving all of his intellectual property to eTreppid, Montgomery had also agreed not to compete with eTreppid. This is not true.

SA West testified that he had in his possession the entire operating agreement prior to preparing his affidavit. Tr. III, 34-35 and stated:

> No. It was not an intentional - - as I said before, I tried to capture the pertinent parts out of these voluminous documents like you've done, giving me three pages of probably a fifty-page document, and to try to capture those parts that were relevant to the investigation.

Tr. I, 173. SA West admitted that he included this excerpt of the operating agreement in his affidavit to demonstrate that Montgomery had a covenant not to compete, and he also testified that the evidence of Montgomery's efforts to sell to potential investors in violation of the operating agreement concerned the redacted portion of his affidavit, which was the single conversation Montgomery had with Azzinaro in late December or early January. Tr. I, 174-175. The affidavit states that Montgomery talked with Azzinaro about his problems at eTreppid and inquired whether Azzinaro might know of anyone willing "to invest" – nothing more (#1 at 10:17-24). Based upon the incomplete provision of the operating agreement, followed by the conversation between Montgomery and Azzinaro, the court concluded that in violation of the operating agreement, Montgomery solicited Azzinaro for new investors and intended to use stolen trade secrets as a new competitor of eTreppid. This is not true.

c. The Ten Patent Assignments

SA West identified ten patent assignments provided by SA Haraldsen, which he also referred to in his affdavit. Tr. III, 5. SA West testified that he referred to these patent assignments to "illustrate that Dennis Montgomery is employed by eTreppid and has done work at eTreppid, that he is assigned to eTreppid." Tr. III, 6. SA West believed that these documents also confirmed that Montgomery was not only an assignor of the patents, but also an "employee" of eTreppid, Tr. III, 7, and this is what SA West stated in his affidavit (#1 at 3:5-9). However, Montgomery was not an employee of eTreppid when he made these assignments; he was an independent contractor as evidenced by Montgomery's form K-1s for the period 1999-2001. Tr. Ex. 29. SA West testified that he was unaware that Montgomery had received 1099 independent contractor forms from eTreppid during the period November 2000 to November 2001. Tr. II, 174.

The patent assignments concern various items, ranging from "method and apparatus for streaming data using rotating cryptographic keys," to "system and method for generating alert conditions in a surveillance system," to "method and apparatus for encoding information using multiple passes and decoding in a single pass." Tr. Ex. 26. SA West did not ask Trepp whether Montgomery had assigned patents to eTreppid for the source code that SA West sought. Tr. II, 174-175.

Although SA West referred to the patent assignments to illustrate Montgomery's employment relationship with eTreppid, this is what the reference conveyed to this court: that since Montgomery had conveyed all of his technological know-how to eTreppid, the ten patents bore an integral relationship to the trade secrets that Montgomery allegedly stole. One has only to review SA West's affidavit to see how the juxtaposition of his reference to the ten patent assignments to eTreppid's trade secrets – software programs relating to "data compression, pattern recognition, change and anomaly detection" – led the court to draw this conclusion. (#1 at 3:5-16). It is now evident that these patents had nothing to do with the trade secrets alleged to have been stolen.

2. The SOCOM Contract and eTreppid's Security Clearance

SA West's affidavit states that a government contract from SOCOM in March 2003 required eTreppid to have access to secret material; therefore, eTreppid received government authorization to store secret material at its facility (#1 at 4:13-18). The court inferred from this portion of SA West's affidavit that eTreppid was engaged in work for the United States involving secret materials, and that eTreppid had the proper facility clearance to conduct this work. It appears eTreppid never had a facility clearance.

SA West first stated that his understanding is that eTreppid had not received approval to store certain classified material at eTreppid facilities. Tr. I, 145. Subsequently, SA West testified that, as stated in his affidavit, eTreppid was permitted to store secret material at least since August 2005. Tr. II, 156-62. To the query, "And to your knowledge despite the three years of government contracts, Trepp's facility never got a facility clearance?" SA West responded, "I don't know what the reasoning was. It could have been Montgomery that held it up." Tr. II, 186.

However, SA West testified later that SA Haraldsen told him that eTreppid had a facility clearance to store secret material, which is based upon a DOD form DD 254. Tr. III, 141-142; Tr. Ex. 34. SA West relied on this information in preparing his affidavit, but he never saw the form. Instead, he relied on SA Haraldsen's statements to him. Tr. III at 141-143. SA West included this information in his affidavit "[t]o show that eTreppid had access, had permission by the U.S. Government or the author of that form to possess secret information." Tr. III, 142. SA West only saw a copy of the actual

DD 254 form just days prior to the final August 17, 2006 evidentiary hearing when Venables faxed it to him. Tr. III, 103-104. Although a signature line is provided on form DD 254, presumably to signify certification for a facility clearance, there is no signature. Tr. Ex. 34. Therefore, the court now concludes that although SA Haraldsen and Venables represented to SA West that eTreppid possessed a facility clearance to store secret material, eTreppid did not have one.

3. Montgomery's Security Clearance

SA West attested that Montgomery received and signed two security briefings in 2003, which outlined his duty to protect classified material and to protect it from unauthorized disclosure (#1 at 4:19-26;5:1-4). Later in the affidavit, SA West recounted a conversation between Montgomery and Gray during which Gray warned Montgomery that his improper storage of classified material could result in the loss of Montgomery's security clearance. *Id.* at 6:8-17. Montgomery allegedly replied, "I don't care about my clearance. They'll always give me my clearance because they want me to do the work." *Id.* at 6:12-13. The affidavit then recites continued problems with Montgomery's storage and handling of classified material and, ultimately, the allegation that he removed it from eTreppid. *Id.* at 6:13-26-7:10.

The court concluded there was probable cause to believe that Montgomery breached his security clearance and took classified materials in violation of the law. Although SA West's affidavit never specifically states the level of Montgomery's security clearance, the inference was that it was tied to his work at eTreppid and that he lost it. However, SA West's testimony conflicts as to whether he knew what, if any, security clearance Montgomery possessed at the time of the search. SA West testified that he knew Montgomery had a top secret clearance in the fall of 2005. Tr. I, 115. SA West stated that he did not look into who at eTreppid had what level security clearance prior to November 2005. Tr. I, 114 at 9-13. SA West initially stated that he did not remember whether he contacted Defense Security Services ("DSS"), the determining agency, regarding Montgomery's security clearance before or after the search. Tr. I, 112-113. SA West subsequently testified that Jay Dixon of DSS and Venables both told him that Montgomery's security clearance was suspended, and SA West said that he believed that he learned that information prior to the search. Tr. I, 116-117. SA West later testified that Dixon told him Montgomery's clearance was suspended, but only after the search. Tr. III, 92. In any event, SA

West made no reference to Dixon in his affidavit, and the court finds that SA West did not rely on Dixon.

SA West testified that, as he understood it, Montgomery's clearance was contingent on his employment with eTreppid. Tr. II, 113. SA West stated that he is unfamiliar with Jpass, the electronic system that governs security clearance, but that Venables provided him with a computer printout indicating that Montgomery's clearance had been suspended. Tr. II, 129-132. To the question "[s]o this was an issue to you before you raided his home whether he still had his security clearance?" SA West responded: "*Yes. I mean it would be significant if he had legitimate access to classified information or not.*" Tr. II, 132 at 6-9 (emphasis supplied).

SA West stated that he did not know whether Montgomery had notice that his security clearance had been suspended. Tr. II, 156-157. He testified that eTreppid tried to provide Montgomery with termination documents and that he did not know if those documents informed Montgomery that his security clearance had been suspended. Tr. II, 156. Montgomery's counsel questioned SA West about DOD directives, which movant's counsel represented governed the revocation or suspension of security clearance. Tr. II, 155-156. The DOD directive outlines steps that must be taken, including providing notice and an opportunity to be heard to the applicant, before an "unfavorable clearance decision" is made. Tr. II, 159-160. SA West had no knowledge of the directive or whether the procedures were followed prior to suspending Montgomery's security clearance. Tr. II, 160. SA West testified that the basis for searching Montgomery's home was the unlawful retention of national security information and that Montgomery did not have permission to store it at home. Tr. II, 160-161. Contrary to SA West's understanding, Montgomery attests that the Government has never revoked his security clearance. Tr. Ex. 38, para. 21.

4. The November 2005 Visit to Nellis Air Force Base and Nine Secret Hard Drives

The evidentiary centerpiece of SA West's affidavit insofar as it concerns unlawful retention of classified material are the "nine Secret hard drives," which Gray recorded at Nellis Air Force Base and "marked with red standard U.S. Government Secret labels as instructed by contractor personnel" and

Based upon this section of SA West's affidavit, the court concluded that probable cause existed that the nine eTreppid hard drives were classified as secret by the appropriate government agency, that they contained information of importance of the United States government, and that the Department of Defense had provided instructions concerning their classification, access, and storage. It is now abundantly clear that this conclusion was incorrect because there was no classified material.

5. December 2005: Montgomery's Breaches of Protocol, Deletion of Classified Material, and Removal of Classified Material and Trade Secrets from eTreppid

Since it is now evident that there was no classified material, the court will only note that the chronology of events in December 2005, which SA West described in his affidavit, led the court to conclude that there was probable cause to believe that in breach of his security clearance, Montgomery had unlawfully removed classified information from eTreppid. The court now turns to the theft of trade secrets.

As a preliminary observation, the court notes that SA West never disclosed in his affidavit that Trepp and Montgomery were engaged in civil litigation concerning ownership of the trade secrets, which are intertwined with the allegation in the affidavit that Montgomery engaged in the criminal theft of trade secrets.[10] Over the course of SA West's meetings with Trepp prior to the search warrant applications, he knew that Trepp was engaged in trade secret litigation against Montgomery and that Trepp was attempting to obtain a temporary restraining order against Montgomery . Tr. I. 20-22, 47. Trepp and SA Haraldsen also provided SA West with declarations of eTreppid employees and other court

---

[10]In fact, two civil cases are pending in federal court: *Montgomery v. eTreppid Technologies, LLC, et al.*, 3:06-CV-0056-LRH (VPC); *eTreppid Technologies, LLC v. Montgomery, et al.*, 3:06-CV-0145-LRH (VPC). In Case No. 3:06-CV-00056 LRH (VPC), the complaint was filed on January 31, 2006 (#1), and as of the dates this court issued the search warrants, February 28 and March 3, 2006, there were no matters under submission to this court; therefore, the court was unaware of this pending action. On January 25, 2006, Montgomery filed a petition to remove the state court proceeding initiated by eTreppid against Montgomery to the United States District Court in Case No. 3:06-CV-00041-HDM (RAM); however, that matter was remanded to the state district court on January 31, 2006 (#14). Thereafter, the United States Department of Defense filed its notice of removal to the United States District Court on March 20, 2006, in Case No. 3:06-CV-00145-LRH (VPC). Thus, this second civil action between Montgomery and eTreppid was not pending in this court at the time the search warrants were issued.

documents. Tr. I, 22-23, 74-75; Vol. II, 199-200; Tr. Ex. 10. SA West was aware that the trade secrets at issue are valued in millions of dollars, but he did nothing during his pre-search warrant investigation to determine the extent of Montgomery's claim to ownership. Tr. I, 60-62,141; Tr. II, 176, #1 at 3:10-16. Had this court had even the slightest inkling that Trepp and Montgomery were engaged in civil litigation, it is an understatement to say that the court would have scrutinized the theft of trade secrets allegation very, very carefully.

As discussed earlier, SA West omitted critical portions of the contribution agreement and the operating agreement, which stated that whatever Montgomery contributed to eTreppid could be found on CD No. 1. However, SA West testified that he did not know what CD No. 1 contained. Tr. I, 51-53. He never inquired as to how long Montgomery had been creating software technologies, Tr. I, 60. SA West did not investigate whether Montgomery had created software that was not included under the contribution agreement or ask anyone what assets Montgomery had not contributed. Tr. I, 62; Tr. II, 123, 128, 214. SA West testified that his impression was that any work Montgomery performed while at eTreppid was also part of what eTreppid owned; he did not believe that it was limited to CD No. 1.

Putting aside the questions concerning SA West's investigation, the court understood that the trade secret Montgomery had allegedly stolen was "source code" (#1 at 1:16-23). However, to this day, it is unclear to the court exactly how "source code" is a trade secret that Montgomery allegedly stole. SA West was unable to describe the allegedly stolen trade secret because no one at eTreppid was adequately able to identify it. Tr. I, 84-85, 87, 131-132, 136, 152; Tr. II., 78-79, 192. SA West never checked eTreppid's computers for the missing source code, and it appears that Trepp referred SA West to Venables for source code questions. Tr. I, 84-87. However, Venables admitted that he did not know what source code was "ever there" at eTreppid; therefore, Venables had no way of knowing what to look for to confirm missing source code (Tr.I, 136; 152-154; Tr. Ex. 33, Vol. 1:11-120). Venables's testimony at the preliminary injunction hearing appears to contradict the assertions SA West made in his affidavit that the source codes at issue were located on the "source code server," using the "RAID Unit" and "back-up ISA" on the premises at eTreppid, and that Venables had access to them (#1 at 3:17-26; 18:1-2).

Montgomery asserts that the term "source code" is meaningless and that the Montgomery Family Trust owned the software pursuant to copyrights filed years before Montgomery's involvement with Trepp (#21). Montgomery also states:

> The sou rce codes used on military contracts are derived from my copyrighted source codes on file in the Copyright Office. None of those source codes are on CD No. 1 or in the patents I assigned to eTreppid. They were all created by me with no other input from anyone and none of them were created as part of my work at eTreppid. Approximately 90% of the codes were developed before September 28, 1998, and 99% were developed prior to November 2002, when even eTreppid treated me as an independent contractor.

Tr. Ex. 38, ¶ 16.

Had the court been apprised of the civil litigation between Trepp and Montgomery and the disputed facts summarized herein, it would have concluded – as the court does now – that there was no probable cause to issue a search warrant based upon the allegation of theft of trade secrets.[11]

6. Callous Disregard of Montgomery's Constitutional Rights

The court has reviewed the record in this proceeding in great detail, since the power of the Government to safeguard a citizen's privacy in his or her home and possessions against unjustified intrusions by government officials is a "basic purpose" of the Fourth Amendment. *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967). In this proceeding, SA West was charged with the investigation of two very serious and two potentially very complex criminal violations. After examination of his affidavit, his testimony concerning his investigation, and the protocols the Department of Justice has implemented for these crimes, this court can only conclude that SA West acted with callous disregard of Montgomery's fundamental Fourth Amendment rights. The over-arching concern in this proceeding is that SA West became an unwitting pawn in a civil dispute, and as a result of his inexperience and lack of training, he prepared search warrant affidavits that are riddled with incorrect statements, edited documents, and uncorroborated conclusions, which caused this court to

[11]Because the court has concluded that there is no probable cause as to the trade secret allegation, the court notes that the conversations Montgomery had with Azzinaro and SA Harraldsen do not change the court's finding of lack of probable cause, and they need not be addressed.

exercise its formidable power to authorize the government to search Montgomery's home and storage units.

In 2000, the Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS") published the *Prosecuting Intellectual Property Crimes Manual*. Tr. Ex. 12. With respect to theft of commercial trade secrets, it states:

> The EEA [Economic Espionage Act of 1996] is violated only where someone acts knowingly without authorization. Under certain circumstances, however, two individuals or companies may have a legitimate dispute over ownership rights in a trade secret. This type of dispute is likely to arise where the two potential owners previously worked together to develop the disputed technology and where the contractual arrangements governing each party's respective ownership interests are unclear or entirely absent. In these circumstances, unilateral action with regard to the trade secret by one of the owners may precipitate an EEA referral. *Such cases are rarely appropriate for criminal prosecution, especially where the party taking unilateral action has obtained advice of counsel.* Notwithstanding the passage of the EEA, many disputes regarding ownership of intellectual property, including trade secrets, continue to be best resolved in a civil forum.

Id. at 17, section VIII.B.6.e (emphasis supplied). Prior to this case, SA West had never investigated a trade secrets case, he was unfamiliar with Department of Justice manuals relating to intellectual property crimes, and he did not consult with anyone within the Department of Justice for guidance, such as the Department of Justice's Computer Hacking and Intellectual Property Unit ("CHIPS Unit"). Tr. I, 14, 18, 23-24; Tr. II, 187-188; 216-218; Tr. Ex. 12, 14, 21, 25. Like SA West, SA Haraldsen had no training in investigating intellectual property crimes, and his role was to act as a liason between eTreppid and the U.S. Air Force and Department of Defense on contracts eTreppid had with these government agencies. Tr. I, 17-18. SA West was aware that Trepp and Montgomery were engaged in civil trade secret litigation, and he relied on one side of that dispute – Trepp's – for critical evidence concerning potential criminal prosecution for theft of trade secrets against the adverse party, Montgomery. SA West relied on Trepp's representation that court records were sealed, but he never confirmed this representation. Tr. I, 74-76; 136-138. In fact, although certain portions of eTreppid's lawsuit were sealed, the parallel lawsuit filed by Montgomery was not. SA West blindly relied on the documents, sworn statements, and evidence supplied by eTreppid, and he never appeared to question whether he had

become an agent, not for the Government, but for private interests engaged in litigation valued in millions of dollars. The litigation that has ensued based upon the seizure of Montgomery's property is a cautionary tale to heed the admonition that trade secrets litigation is best left to the civil forum.

The court has similar concerns about SA West's investigation of unlawful retention of national defense information. SA West took SA Haraldsen, Trepp, Venables, and Gray at their word and never confirmed basic facts they alleged. Upon learning of these serious allegations, one would presume that an FBI agent with no experience in this area would consult with Department of Justice officials or his own supervisors regarding the investigation. However, SA West never confirmed with the proper government agency whether eTreppid had a facility clearance to store classified materials; he simply relied on statements of Haraldsen and Venables. SA West did not even see the actual DD Form 254 until a few days before the final day of the evidentiary hearing – six months after the search warrants were issued. SA West never confirmed the status of Montgomery's security clearance with the appropriate government agency, and once again relied on Venables's statement. Moreover, SA West had no knowledge of government procedures for suspension or revocation of an individual's security clearance. When Gray supplied SA West with a list of so-called classified materials, he never confirmed with anyone at Nellis Air Force Base that they were, in fact, classified. He continued to rely on Venables, Gray and Haraldsen's representations concerning classification, and he never verified himself whether the allegedly classified materials were actually missing.

The evidence before this court compels the conclusion that SA West acted with callous disregard of Montgomery's constitutional rights, which resulted in the improper search of Montgomery's home and storage units, and the improper seizure of his property.

7. Conclusion

Once the Government conceded that "nine Secret hard drives" were not, in fact, classified and that the material "was not properly classified by an Original Classification Authority within the U.S. Air Force," (Tr. Ex. 4), the obvious question is whether the search warrant can stand based on probable cause that Montgomery violated 18 U.S.C. § 793(e), unlawful retention of national defense information. Throughout the three days of the evidentiary hearing and in its post-hearing brief, the Government made

no showing whatsoever that probable cause still exists to justify keeping the seized material based on this criminal violation, notwithstanding this court's invitation that the Government do so. Tr. III, 211-212. Likewise, the Government has also failed to demonstrate that probable cause exists to justify the issuance of the search warrants in this case based on a violation of 18 U.S.C. § 1832, theft of trade secrets. The Government's post-hearing brief is devoid of any legal or factual argument in opposition to Montgomery's motion for a return of the seized property, other than a defense of SA West's investigation prior to the issuance of the search warrants. Having considered the evidence adduced at the hearing, and all of the papers submitted in this proceeding, the court grants Montgomery's motion for a return of the seized property (#21).[12]

III. ORDER

Based upon the foregoing,

IT IS ORDERED that Montgomery's motion to unseal the search warrant affidavits (#21) is **GRANTED,** and Montgomery's motion for the return of property pursuant to Fed.R.Crim.P. 41(g) (#21) is **GRANTED**. Montgomery's motion for the segregation and sealing of all attorney-client and trade secret material (#21) is **DENIED AS MOOT,** since the court has ordered the return of all seized property.

Pursuant to LR IB 3-1, any party wishing to object to this order shall, on or before **Tuesday, December 12, 2006,** file and serve specific a written objection to the ruling together with points and authorities in support thereof. The opposing party shall within ten days thereafter file points and authorities opposing the objection. Points and authorities filed in support of or in opposition to the order are subject to the page limits set forth in LR 7-4. This proceeding shall remain sealed until the deadline for filing a written objection has expired. If no objection to this order is filed by **Tuesday, December 12, 2006**, this order shall stand as the final order, and all papers filed in this proceeding shall be **UNSEALED** without further order of this court.

---

[12]Since this court concludes that the Government lacked probable cause, it does not reach the particularity analysis.

IT IS FURTHER ORDERED that in the event an objection is filed, this proceeding shall remain **SEALED** until such time as the District Court issues its final order. The parties shall file any written objection to this order or opposition to the objection under seal by delivering any documents to be filed in a sealed envelope addressed to Jake Herb or Lia Griffin or the U.S. District Court, District of Nevada, Reno Office.

IT IS SO ORDERED.

Dated this 28th day of November, 2006.

UNITED STATES MAGISTRATE JUDGE

EXHIBIT “7”

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30 J

1. REQUISITION NUMBER	Page 1
FX20270901S001	

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
FA8240-09-C-3203				

7. FOR SOLICITATION INFORMATION CALL	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	Phillip D. Judd	(801) 777 -3192 ext.	

9. ISSUED BY CODE FA8240
519 CBSS/PK
6082 FIR AVE, Bldg 1232
HILL AFB UT 84056-5820
BUYER: Phillip D. Judd/519CBSS/PK
phil.judd@hill.af.mil
Phone: (801) 777- 3192 Fax: (801) 777-5688 No Collect Calls

10. THIS ACQUISITION IS
[ ] UNRESTRICTED
[ ] SET ASIDE: % FOR
[ ] SMALL BUSINESS
[ ] HUBZONE SMALL BUS
[X] Oth Than Full & Open
NAICS CODE: 541519
SIZE STD: $25.0

11. DELIVERY FOR FOB DEST. UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE
[X] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

12. DISCOUNT TERMS
NET 30 DAYS

13b. RATING
DO: C9 52.211-14, 52.211-15

14. METHOD OF SOLICITATION
[ ] RFQ [ ] IFB [X] RFP

15. DELIVER TO CODE

SEE LINE ITEM SCHEDULE

16. ADMINISTERED BY CODE 1232JM
519 CBSS/PK
Attn: Phillip Judd
6082 Fir Ave
Bldg 1232
Hill AFB UT 84056-5820
United States
SCD:C

17a. CONTRACTOR/ OFFEROR CODE 59NF3 FACILITY CODE
BLXWARE LLC
600 106th Ave NE Ste 210
Bellevue WA 98004-5043
United States
(760) 862-6400
Attn: Nickolas Rhodes

18a. PAYMENT WILL BE MADE BY CODE 1QLPK
519 CBSS/FM
6082 FIR AVE BLDG 1232
HILL AFB UT 84056-5820
EFT:T

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

[X] 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED. SEE ELECTRONIC SUBMISSION OF PAYMENT REQUESTS, CLAUSE 252.232-7003.

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Routine				

The following PR is applicable to this award:

FX2027-09-013S001

All Invoices must be submitted manually to the payment office identified in block 18a as Wide Area Work Flow procedures will not be used. (See Section G)

SEE LINE ITEM SCHEDULE
(Attach Additional Sheets as Necessary)

Total

25. ACCOUNTING AND APPROPRIATION DATA **SEE FUNDS SCHEDULE**

26. AWARD AMOUNT (For Govt use only)
$ 3,000,000.00

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [X] ARE NOT ATTACHED

28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE.
[X] CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

29. AWARD OF CONTRACT: REF. OFFER DATED 13 JAN 2009. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE [ ] SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER (Type or print)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (Type or print)	31c. DATE SIGNED
Elva Blixseth Owner	1/19/09	Phillip D. Judd phil.judd@hill.af.mil	13 JAN 2009

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV 4/2002)
Prescribed by GSA - FAR (48 CFR) 53.212

EXHIBIT “8”

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

* * *

DENNIS MONTGOMERY and the MONTGOMERY FAMILY TRUST Plaintiffs, vs. ETREPPID TECHNOLOGIES, LLC; WARREN TREPP; and the UNITED STATES DEPARTMENT OF DEFENSE, Defendants. AND ALL RELATED MATTERS.	3:06-CV-00056-PMP-VPC BASE FILE 3:06-CV-00145-PMP-VPC **ORDER RE PROTECTIVE ORDER**

Prior to consolidation of these two related cases, Defendant United States Department of Defense filed Motions for Protective Order (3:06-CV-00056-PMP-VPC, Doc. #83, and 3:06-CV-00145-PMP-VPC, Doc. #51) to prevent disclosure of information that could harm the national security interests of the United States. Specifically, the United States' seeks a protective order pursuant to Federal Rule of Civil Procedure 26(c) to prevent the disclosure of information relating to (1) the existence or non-existence of any actual or proposed relationship, agreement, connection, contract, transaction, communication or meeting of any kind between an intelligence agency as defined in 50 U.S.C. § 401(a)(4), which includes intelligence elements of the military services; and (2) any actual or proposed interest in, application, or use by any intelligence agency, or any current or former official, employee, or representative thereof, of any technology, software, or source code owned or claimed by any individuals or entities associated with these lawsuits.

//

The United States' supports its application for protective order under the military and States Secret privilege by the Declaration of John D. Negroponte, formally Director of National Intelligence, and a Classified Declaration which has been reviewed by the Court in camera and ex parte, which demonstrate that disclosure of information at issue in this litigation subject to the proposed protective order could be expected to cause serious, and some cases exceptionally grave damage to national security.

Issues relating to whether information subject to a claim of military and states secrets privilege were contained in pleadings, motions, declarations and other materials filed in these consolidated cases as well as in the related in the Search Warrant case (3:06-CV-0263-PMP-VPC), have required considerable attention by the parties and the Court. In this regard, counsel for Defendant United States' and those authorized to assert the military and states secrets privilege on behalf of Defendant United States' have met with counsel in these related actions as well as with counsel in the related Search Warrant case, and have reviewed copies of all pleadings, motions, documents and exhibits filed in the above referenced cases for the purpose of identifying and redacting those portions subject to a claim of military and state secrets privilege on behalf of Defendant United States. The Court has reviewed all such papers in camera and ex parte with counsel for Defendant United States' and those authorized to assert the military and states secret privilege on behalf of Defendant United States, and has approved the redaction of material subject to the privilege claim.

Defendant United States' Department of Defense Motion for Protective Order has now been fully briefed and on June 12, 2007, the Court conducted a hearing regarding the United States' Motion for Protective Order and other pending motions.

On June 21, 2007, Defendant United States' filed a Revised Proposed Protective Order (3:06-CV-00056-PMP-VPC (Doc. #196). The Court finds that said Protective Order is warranted as to form and content and hereby approves the same.

///

IT IS THEREFORE ORDERED that Defendant United States Department of Defense Motions for Protective Order (3:06-CV-00056-PMP-VPC, Doc. #83, and 3:06-CV-00145-PMP-VPC, Doc. #51) is GRANTED.

DATED: August 29, 2007.

PHILIP M. PRO
United States District Judge

PETER D. KEISLER
Assistant Attorney General
STEVEN W. MYHRE
Acting United States Attorney
District of Nevada
GREG ADDINGTON
Assistant United States Attorney
Nevada Bar 6875
100 West Liberty, Suite 600
Reno, Nevada 89501
VINCENT M. GARVEY
Deputy Branch Director
CARLOTTA P. WELLS
Senior Trial Counsel
Federal Programs Branch
Civil Division - Room 7150
U.S. Department of Justice
20 Massachusetts Ave., NW/P.O. Box 883
Washington, D.C. 20044
Telephone: (202)514-4522
Facsimile: (202) 616-8470

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

DENNIS MONTGOMERY, et al., Plaintiffs, v. ETREPPID TECHNOLOGIES, INC., et al., Defendants.	3:06-CV-00056-PMP-VPC **BASE FILE** 3:06-CV-00145-PMP-VPC

UNITED STATES **PROTECTIVE ORDER**

Pursuant to Federal Rule of Civil Procedure 26, in order to protect the classification, confidentiality and the rights to information and documents developed and disclosed in connection with this litigation, and to facilitate discovery by and among the parties to this action and from third parties, the United States hereby proposes entry of the following protective order.

IT IS HEREBY ORDERED as follows:

1. Certain information that may or may not be relevant to the claims and/or defenses of eTreppid Technologies, LLC and its current or former officers or employees (hereinafter collectively referred to as "eTreppid"), Warren Trepp, Dennis Montgomery, the Montgomery Family Trust and/or Dennis Montgomery and Brenda Montgomery as trustees of the Montgomery Family Trust (hereinafter collectively referred to as "the Parties"), as delineated in paragraphs 2 and 3 below, is subject to the state secrets privilege, the disclosure of which reasonably could be expected to cause serious, and in some cases exceptionally grave, damage to the national security of the United States. Such information shall not be subject to discovery or disclosure by any of the Parties during all proceedings in these actions, and shall be excluded from evidence at trial.

2. The Parties shall not serve or take any discovery relating to or questioning the existence or non-existence of any actual or proposed relationship, agreement, connection, contract, transaction, communication or meeting of any kind between any entity in the intelligence community as defined by the National Security Act of 1947, 50 U.S.C. § 401(a)(4), which includes intelligence elements of the military services, or any current or former official, employee or representative thereof (hereinafter collectively referred to as "intelligence agency") and the Parties.

3. The Parties shall not serve or take any discovery relating to or questioning any actual or proposed intelligence agency interest in, application of or use of any technology, software or source code owned or claimed by the Parties.

4. This Order does not preclude the Parties from serving or taking any discovery from other Parties or third parties relating to, or questioning, the following:

Case 3:06-cv-00056-PMP-CSD Document 1216-2 Filed 08/20/22 Page 92 of 194

a. The existence and nature of the "Big Safari" contract (hereinafter referred to as "the Big Safari Contract") between eTreppid and the Unites States Air Force, including but not limited to the fact that the Big Safari Contract required eTreppid to perform data analysis and the fact that the data analysis eTreppid performed under the Big Safari Contract involved image identification technology;

b. The fact that the Big Safari Contract required employees and/or officers of eTreppid to sign secrecy agreements with the Department of Defense;

c. The computer source code, software, programs, or technical specifications relating to any technology owned or claimed by any of the Parties ("the Technology");

d. Any contract, relationship, agreement, connection, transaction, communication or meeting of any kind relating to the Technology, unless covered by paragraphs 2 or 3 above;

e. Any actual or potential commercial or government applications of the Technology, unless covered by paragraphs 2 or 3 above;

f. Facts relating to the issue of ownership by the Parties of any right or interest in the Technology, unless covered by paragraphs 2 or 3 above;

g. The revenue, income, expenses, profits and losses of the Parties, unless disclosure of such information would be covered by paragraphs 2 or 3 above; and

h. Any consideration received by any of the Parties relating to the Technology, unless covered by paragraphs 2 or 3 above.

5. The Parties shall not discuss, mention, question or introduce as evidence, either at trial, in any pleading or motion, or in any case-related correspondence, any actual or proposed relationship, agreement, connection, contract, transaction, communication or meeting of any kind between any intelligence agency and any of the Parties.

6. The Parties shall not discuss, mention, question or introduce as evidence, either at trial, in any pleading or motion, or in any case-related correspondence, any actual or proposed intelligence agency interest in, application of or use of the Technology.

7. No question and no document request in discovery or at trial shall require a response that would include any information covered by paragraphs 2, 3, 5 or 6 above, but if the responding party believes that a full and complete response could disclose information within the scope of the state secrets privilege, the responding party shall provide timely notice of such belief and the full and complete response to the United States prior to responding, and shall respond only with information that the United States has determined is not subject to the state secrets privilege.

8. The military and state secrets privilege, the claim that any discovery is covered by paragraphs 2 or 3 above, and the claim that any evidence is covered by paragraphs 2 or 3 above, can only be invoked by the United States. These claims cannot be asserted by a private individual or entity.

9. All Parties shall serve the attorneys for the United States with (a) a copy of all notices of depositions, (b) a copy of all requests for discovery and responses thereto, and (c) a copy of all pleadings and motions filed together with supporting memoranda (hereinafter collectively referred to as the "documents"), unless such documents request or relate to information covered by paragraphs 2 or 3 above. If the documents request or relate to information covered by paragraphs 2 or 3 above, the Parties shall submit the documents to the United States for privilege review prior to service or filing. All documents filed or sought to be used as evidence by the Parties in this case shall be unclassified. This requirement applies to all motions, pleadings, briefs, and any other document, including exhibits, correspondence, or anything appended thereto or filed therewith. If the United States determines that a document or discovery response includes

information covered by paragraphs 2 or 3 above, the United States shall redact the information and provide the parties and Court with a redacted copy of the document or discovery response.

10. The Clerk of the Court shall send attorneys for the United States a copy of all future decisions and notices for hearings in these cases.

11. As the United States deems necessary, attorneys for the United States may attend all depositions and proceedings in this case and may make objections as necessary to protect national security information. If attorneys for the United States assert an objection based on the need to protect national security information with respect to either witness testimony or documents introduced or otherwise relied upon during a deposition, then the witness shall be precluded from testifying with respect to the line of inquiry that engendered the objection, and the document shall be withdrawn from the record pending an order of the Court with respect to the scope of the government's national security objection.

12. To protect the United States' interests, attorneys for the United States may participate in any proceeding in these cases, including but not limited to motions hearings, all pre-trial proceedings, or trial by making and opposing motions, submitting briefs, and participating in arguments.

13. The United States shall be excepted from all party discovery during the pendency of its motions to dismiss the claims against the Department of Defense.

It is so ordered.

Dated: August 29, 2007

PHILIP M. PRO
United States District Judge

UNITED STATES' MOTION FOR PROTECTIVE ORDER

EXHIBIT 1

Tab-1

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEVADA

ETREPPID TECHNOLOGIES, LLC, a California Corporation, Plaintiff v. DENNIS MONTGOMERY, et. al., Defendants.	CV-N-06-00415(BES)(VPC)
DENNIS MONTGOMERY, et. al., Plaintiffs v. ETREPPID TECHNOLOGIES, INC., et. al. Defendants.	CV-N-06-00056(BES)(VPC)

DECLARATION AND FORMAL CLAIM OF STATE SECRETS AND STATUTORY PRIVILEGES BY JOHN D. NEGROPONTE, DIRECTOR OF NATIONAL INTELLIGENCE

I, JOHN D. NEGROPONTE, hereby declare as follows:

1. I am the Director of National Intelligence (DNI) of the United States. I have held this position since April 21, 2005. From June 28, 2004, until my appointment as DNI, I served as the United States Ambassador to Iraq.

From September 18, 2001, until my appointment in Iraq, I served as the United States Permanent Representative to the United Nations. I have also served as Ambassador to Honduras (1981-1985), Mexico (1989-1993), and the Philippines (1993-1996), and as Deputy Assistant to the President for National Security Affairs (1987-1989).

2. The statements made herein are based on my personal knowledge, as well as on information provided to me in my official capacity as DNI, and on my personal evaluation of that information. In personally considering this matter, I have read the information contained in the separate classified declaration filed *in camera* and *ex parte* in this case.

3. The purpose of this declaration is to assert formally, in my capacity as DNI and head of the United States Intelligence Community, the state secrets privilege to protect intelligence information ("state secrets privilege"), as well as a statutory privilege under the National Security Act, 50 U.S.C. § 403-1(i)(1), to protect intelligence sources and methods from unauthorized disclosure. Unauthorized disclosure of information covered by the state secrets and statutory privileges reasonably could be expected to cause serious, and in some cases exceptionally grave damage to the national security of the

United States, and such information should therefore be excluded from any use in this litigation.

I. STATUTORY AND EXECUTIVE ORDER AUTHORITIES

4. The position of Director of National Intelligence was created by the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1011(a), 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President of the United States, the DNI serves as the head of the United States Intelligence Community and as the principal advisor to the President, the National Security Council, and the Homeland Security Council for matters related to intelligence and national security. *See*, 50 U.S.C. § 403 (b)(1),(2).

5. The "United States Intelligence Community" includes the Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the military services, the Federal

Bureau of Investigation, and the Department of Energy; the Office of Intelligence and Analysis of the Department of the Treasury; the Drug Enforcement Administration's Intelligence Division; the Bureau of Intelligence and Research of the Department of State; elements of the Department of Homeland Security concerned with the analysis of intelligence information (including the Office of Intelligence of the Coast Guard); and such other elements of any other department or agency as the President may designate, or as may be jointly designated by the DNI and the head of the department or agency concerned, as an element of the United States Intelligence Community. *See*, 50 U.S.C. § 401(a)(4).

6. The responsibilities and authorities of the DNI, enumerated in the National Security Act, as amended, at 50 U.S.C. § 403-1, include ensuring that national intelligence is provided to the President, the heads of the departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 403-1(a)(1). The DNI is also charged with establishing the objectives of, determining the requirements and priorities for, and managing and directing the tasking, collection, analysis, production, and

dissemination of national intelligence by elements of the United States Intelligence Community. 50 U.S.C. § 403-1(f)(1)(A)(i), (ii). The DNI is responsible for developing and determining, based on proposals submitted by heads of agencies and departments within the United States Intelligence Community, an annual consolidated budget for the National Intelligence Program for presentation to the President, and for ensuring the effective execution of the annual budget for intelligence and intelligence-related activities, including managing and allotting appropriations for the National Intelligence Program. *Id.* § 403-1(c)(1)-(5).

7. In addition, the National Security Act of 1947, as amended, provides that "The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 403-1(i)(1). Consistent with this responsibility, the DNI establishes and implements the guidelines of the United States Intelligence Community for the classification of information under applicable law, Executive Orders, or other Presidential directives, and access and dissemination of intelligence. *Id.* § 403-1(i)(2)(A), (b). In particular, the DNI is responsible for the establishment of uniform standards and procedures for granting access to Sensitive

Compartmented Information to any officer or employee of any agency or department of the United States and for ensuring consistent implementation of those standards throughout such departments and agencies. *Id.* § 403-1(j)(1),(2).

8. By virtue of my position as the DNI, and unless otherwise directed by the President, I have access to all intelligence related to national security that is collected by any department, agency, or other entity of the United States. Pursuant to Executive Order 12958, as amended,[1] the President has authorized me to exercise original TOP SECRET classification authority. After personal consideration of the matter, I have determined that the classified *ex parte, in camera* declaration which accompanies this assertion of the state secrets privilege and the statutory privilege to protect intelligence sources and methods is properly classified under § 1.3 of E.O. 12958, because the unauthorized public disclosure of information contained in that declaration reasonably could be expected to cause serious, and in some cases exceptionally grave damage to the foreign policy and national security of the United States.

[1] Executive Order 12958 was amended by Executive Order 13292. *See* Exec. Order No. 13292, 68 Fed. Reg. 15315 (Mar. 28, 2003). All citations to Exec. Order No. 12958 are to the Order as amended by Exec. Order No. 13292. *See* Exec. Order No. 12,958, 60 Fed. Reg. 19825 (1995), *reprinted as amended in* 50 U.S.C.A. § 435 note at 180 (West Supp. 2006).

II. ASSERTION OF THE STATE SECRETS AND STATUTORY PRIVILEGES

9. After careful and actual personal consideration of the matter, I have determined that the unauthorized disclosure of certain information that may be implicated by the parties' claims in this matter, as set forth here and described in more detail in the classified *ex parte, in camera* declaration which accompanies this declaration, reasonably could be expected to cause serious, and in some cases exceptionally grave damage to the national security of the United States, and thus must be protected from disclosure and excluded from this case. Therefore, I formally invoke and assert the state secrets privilege to prevent the disclosure of that information.

10. Through this declaration, I also invoke and assert a statutory privilege held by the DNI under the National Security Act, as amended, to protect the intelligence sources and methods implicated by this case. *See*, 50 U.S.C. § 403-1(i)(1). My assertion of this statutory privilege for intelligence sources and methods is coextensive with my state secrets privilege assertion.

11. With my assertion of the state secrets privilege and the statutory privilege to protect intelligence sources and methods, I respectfully ask the Court to prevent any

party from testifying, eliciting testimony, producing, disclosing, entering into evidence or making any other use in discovery, at trial, or in any other way in connection with this case, information concerning: (a) the existence or non-existence of, any actual or proposed relationship, agreement, connection, contract, transaction, communication, or meeting of any kind between any entity in the United States Intelligence Community, or any current or former official, employee, or representative thereof, and any individuals or entities associated with this lawsuit, on any current or former officer or employee thereof; and (b) any actual or proposed interest in, application, or use by any entity in the United States Intelligence Agency, or any current or former official, employee, or representative thereof, of any technology, software, or source code owned or claimed by any individuals or entities associated with this lawsuit.

12. I have determined that any unauthorized disclosure of the information described in Paragraph 11 reasonably could be expected to cause serious, and in some case exceptionally grave damage to national security since the United States can neither confirm nor deny such information without compromising the effectiveness of intelligence sources and methods. Public disclosure of

information that confirms the use of particular intelligence sources and methods compromises the effectiveness of those sources and methods by alerting likely targets to their use, while public denial of the use of particular intelligence sources and methods reveals to adversaries that some practices are secure. Any truthful response to confirm or deny allegations related to intelligence sources or methods informs hostile foreign intelligence agencies about the manner in which the United States collects intelligence information, and could result in a loss of valuable intelligence when our adversaries are able to take countermeasures. Similarly, if the United States government was required to admit or deny allegations made in litigation concerning its classified contracting process, then classified contract relationships could be exposed, which would cause harm to the national security. The precise nature of the harm that would ensue from the disclosure of the information protected by the state secrets privilege and statutory privilege to protect intelligence sources and methods is set forth in detail in the *in camera, ex parte* declaration.

CONCLUSION

13. I respectfully request that the Court grant the Department of Defense's motion for a protective order.

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed this 19th day of September 2006.

JOHN D. NEGROPONTE
DIRECTOR OF NATIONAL INTELLIGENCE

EXHIBIT “9”

[redacted]

From: Ncoder <dennis@ncoder.net>
Sent: Wednesday, June 4, 2008 8:00 PM
To: 'Deborah A. Klar'
Subject: RE: Meeting

I will attend.

-----Original Message-----
From: Deborah A. Klar [mailto:dklar@linerlaw.com]
Sent: Wednesday, June 04, 2008 4:12 PM
To: Wells, Carlotta (CIV)
Subject: RE: Meeting

Counsel: If I did not acknowledge previously in writing, this email will confirm that Mr. Montgomery will attend the meetings in D.C. on June 6,
2008. Best regards, D.A.K.

-----Original Message-----
From: Wells, Carlotta (CIV) [mailto:Carlotta.Wells@usdoj.gov]
Sent: Tuesday, June 03, 2008 12:01 PM
To: Deborah A. Klar; Tuneen E. Chisolm
Cc: Gomez, Raphael (CIV)
Subject: Meeting

Deborah--

As I stated in my voice mail message, we are confirming that Mr.
Montgomery will meet with security personnel on Friday, June 6. The meeting will commence at 10 am EDT at 20 Massachusetts Avenue, NW, Washington, DC. Please acknowledge that Mr. Montgomery will attend the meeting as soon as possible.

Thanks.
Carlie Wells
Senior Trial Counsel
Civil Division/Federal Programs Branch
P.O. Box 883 (zip 20044)
20 Massachusetts Ave, NW Room 7150
Washington, DC 20530
(202) 514-4522
(202) 616-8470 (fax)

[redacted]

From: Ncoder <dennis@ncoder.net>
Sent: Friday, June 6, 2008 1:24 AM
To: 'Christian Cordero'
Subject: Leaving for DC

I will be in DC at 7am EST. I will email you when I can. Don't try to call. I am not allowed to carry phone into the building.

Night

dennismontgomery45@gmail.com

From: Ncoder <dennis@ncoder.net>
Sent: Tuesday, June 3, 2008 5:46 PM
To: 'Deborah A. Klar'
Subject: RE: Meeting with Gov't

You have no credibility with the court! Like they would believe you?

From: Deborah A. Klar [mailto:dklar@linerlaw.com]
Sent: Tuesday, June 03, 2008 1:39 PM
To: Ncoder
Cc: Ellyn S. Garofalo; Peter Bransten; Mark H. Gunderson
Subject: Meeting with Gov't

Dennis, The meeting has been confirmed for June 6. I spoke with Saul about him accompanying you. But, he did not think that was wise. We think it wise that you have counsel present. Although government counsel will not be in the room, they will be outside.
For the same reason we insisted that government counsel not be present in the room, we think it best for you to have counsel present outside the room. Gov't counsel has been directed to report to the Court re the meeting. If your counsel is not present, the gov't lawyers will be free to put their spin on what happened before Cooke. We will not be in a position to challenge any negative assertions they may feel free to make, knowing that your counsel was not present and cannot contradict what they say.

Please get back to me today if possible. Best regards, D.A.K.

Deborah A. Klar
LINER YANKELEVITZ SUNSHINE & REGENSTREIF LLP
1100 Glendon Avenue | 14th Floor
Los Angeles, CA 90024.3503
main: 310.500.3500
dir: 310.500.3614
fax: 310.500.3501
dklar@linerlaw.com
www.linerlaw.com

used, for the purpose of (i) avoiding tax-related penalties under the Internal Revenue Code or applicable state or local tax law provisions or (ii) promoting, marketing or recommending to another party any tax-related matter addressed herein.

EXHIBIT “10”

Mark H. Gunderson, Esq. (SBN: 2134)
Catherine A. Reichenberg, Esq. (SBN: 10362)
GUNDERSON LAW FIRM
5345 Kietzke Lane, Suite 200
Reno, Nevada 89511
Telephone: (775) 829-1222
Facsimile: (775) 829-1226

Randall J. Sunshine, Esq. (SBN: 137363)
Ellyn S. Garofalo, Esq. (SBN: 158795)
LINER YANKELEVITZ
SUNSHINE & REGENSTREIF LLP
1100 Glendon Avenue, 14th Floor
Los Angeles, California 90024-3503
Telephone: (310) 500-3500
Facsimile: (310) 500-3501
ADMITTED PRO HAC VICE

Attorneys for Plaintiffs
DENNIS MONTGOMERY, and the MONTGOMERY
FAMILY TRUST

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

DENNIS MONTGOMERY and the MONTGOMERY FAMILY TRUST, Plaintiffs, vs. ETREPPID TECHNOLOGIES, LLC, WARREN TREPP, and the UNITED STATES DEPARTMENT OF DEFENSE, Defendants. AND RELATED CASES.	Case No. 3:06-CV-00056-PMP-VPC BASE FILE (Consolidated with Case No. 3:06-CV-00145-PMP-VPC) **[PROPOSED] STIPULATION AND DISMISSAL WITH PREJUDICE**

WHEREAS Dennis Montgomery, the Montgomery Family Trust, eTreppid Technologies, LLC, Warren Trepp, Edra Blixseth and Opspring LLC (collectively, the "Parties") are parties to a dispute arising from the ownership of certain technology described in the Complaints and Counterclaims;

WHEREAS Plaintiffs Dennis Montgomery and the Montgomery Family Trust (collectively, the "Montgomery Parties") have asserted claims against Defendants eTreppid Technologies, LLC and Warren Trepp (collectively, the "eTreppid Parties") in Montgomery, et al. v. eTreppid Technologies, LLC, et al., Case No. 3:06 CV-00056-BES-VPC (Base File) and Case No. 3:06-CV-00145-PMP-VPC (the "Lawsuit");

WHEREAS Defendant and Counter-counterclaimant eTreppid Technologies, LLC ("eTreppid") has asserted counter-claims against the Montgomery Parties, Edra Blixseth and Opspring, LLC;

WHEREAS the Parties desire to fully resolve and settle all claims and counter-claims asserted by and against the Parties to the Lawsuit;

WHEREAS the Parties have agreed to a settlement of the claims and counter-claims asserted by and against the Parties in the Lawsuit (the "Settlement Agreement");

NOW, THEREFORE, the Parties hereby agree and stipulate as follows:

1. The Montgomery Parties shall dismiss with prejudice all claims asserted in their First Amended Complaint and Counterclaim against the eTreppid Parties in the Lawsuit.

2. eTreppid Technologies, LLC shall dismiss with prejudice all Complaints and Counter-claims asserted against the Montgomery Parties, Edra Blixseth and Opspring, LLC in the Lawsuit.

3. Notwithstanding the above-referenced dismissals with prejudice, the Court shall retain jurisdiction over the following: (1) the eTreppid Parties' claims against Atigeo LLC and Michael Sandoval as third party defendants; (2) issues relating to Michael Flynn's ("Mr. Flynn") attorney's fees (Docket Nos. 502 and 584); (3) Mr. Flynn's motion to establish Rule 3.3 procedures pursuant to the Nevada Rules of Professional Conduct (Docket No. 540); (4) Mr. Flynn's motion for sanctions (Docket No. 545); (5) compliance with the United States Protective Orders (Docket

Nos. 252 and 253); and (6) enforcement of the confidentiality and mutual non-disparagement provision of the Parties' Settlement Agreement.

4. The terms of the Parties' Settlement Agreement shall remain confidential.

Dated: September 26, 2008

LINER YANKELEVITZ
SUNSHINE & REGENSTREIF LLP

By: /s/ Ellyn S. Garofalo
Ellyn S. Garofalo
Attorneys for DENNIS MONTGOMERY, the MONTGOMERY FAMILY TRUST, EDRA BLIXETH, AND OPSPRING LLC

Dated: September 26, 2008

HOLLAND & HART LLP

By: /s/ J. Stephen Peek
J. Stephen Peek
Attorneys for ETREPPID TECHNOLOGIES, LLC and WARREN TREPP

CERTIFICATE OF SERVICE

Pursuant to NRCP 5(b), I certify that I am an employee of the Law Offices Of Liner Yankelevitz Sunshine & Regenstreif LLP, and that on September 26, 2008, I caused to be served the within document described as **[PROPOSED] STIPULATION AND DISMISSAL WITH PREJUDICE** on the interested parties in this action as stated below:

J. Stephen Peek, Esq. Jerry M. Snyder, Esq. Adam G. Lang, Esq. Shane M. Biornstad, Esq. Holland & Hart LLP 5441 Kietzke Lane, Second Floor Reno, Nevada 89511 (775) 327-3000; 786-6179 - FAX speek@hollandhard.com; jsnyder@hollandhartcom, alang@hollandhart.com, sbiornstad@hollandhart.com Attorneys for eTreppid and Warren Trepp	Carlotta P. Wells, Sr. Trial Counsel U.S. Dept. of Justice Fed.Programs Branch Civil Division, Room 7150 20 Massachusetts Avenue, NW Post Office Box 883 Washington, D.C. 20044 (202) 514-4522; 616-8470 - FAX E-mail: Carlotta.wells@usdoj.gov Attorneys for Department of Defense
Reid H. Weingarten, Esq. Brian M. Heberlig, Esq. Robert A. Ayers, Esq, Steptoe & Johnson, LLP 1330 Connecticut Avenue, N.W. Washington, D.C. 20036-1795 (202) 429-3000; (202) 429-3902 - FAX rweingarten@steptoe.com; bheberlig@steptoe.com; rayers@steptoe.com Attorneys for eTreppid and Warren Trepp	Raphael O. Gomez, Esq., Sr. Trial Counsel U.S. Dept. of Justice, Fed. Programs Branch Civil Division, Room 6144 20 Massachusetts Avenue, NW Post Office Box 883 Washington, D.C. 20044 (202) 514-1318; 616-8470 - FAX E-mail: raphael.gomez@usdoj.gov Attorneys for Department of Defense
Greg Addington, AUSA U.S. DEPARTMENT OF JUSTICE 100 W. Liberty Street. Suite 600 Reno, Nevada 89501 E-mail: Greg.addington@usdoj.gov (775) 784-5181 - FAX Attorneys for Department of Defense	Bridget Robb Peck, Esq. Lewis and Roca LLP 50 West Liberty Street, Suite 410 Reno, Nevada 89501 Tel: (775) 823-2900; Fax: (775) 823-2929 bpeck@lrlaw.com Attorneys for Atigeo LLC & Michael Sandoval
Roland Tellis, Esq. Marshall B. Grossman, Esq. Heather L. Ristau, Esq. Bingham McCutchen LLP The Water Garden 1620 26th Street, Fourth Floor, North Tower Santa Monica, CA 90404-4060 Fax: (310) 907-2143 E-mail: roland.tellis@bingham.com; marshall.grossman@bingham.com; heather.ristau@bingham.com Attorneys for Michael Sandoval	Robert E. Rohde, Esq. Gregory Schwartz, Esq. Rohde & Van Kampen 1001 Fourth Avenue, Suite 4050 Seattle, Washington 98154 Fax: (206) 405-2825 E-mail: brohde@rohdelaw.com, gschwartz@rohdelaw.com Attorneys for Atigeo LLC

☒ **[ELECTRONIC]** By filing the document(s) electronically with the U.S. District Court and therefore the court's computer system has electronically delivered a copy of the foregoing document(s) to the persons listed above at their respective email address.

I declare under penalty of perjury under the laws of the State of California and the United States of America that the foregoing is true and correct.

Executed on September 26, 2008, at Los Angeles, California.

Ellyn S. Garofalo	/s/ Ellyn S. Garofalo
(Type or print name)	(Signature)

EXHIBIT “11”

From: Addington, Greg (USANV) <Greg.Addington@usdoj.gov>
Sent: Tuesday, December 1, 2020 3:58 PM
To: John <john@lawyerinmontana.com>
Subject: RE: Letter dated October 9 re Dennis Montgomery

I will enquire regarding the status of the review initiated last month.

GREG ADDINGTON
Assistant United States Attorney

From: John <john@lawyerinmontana.com>
Sent: Tuesday, December 1, 2020 2:48 PM
To: Addington, Greg (USANV) <GAddington@usa.doj.gov>
Subject: RE: Letter dated October 9 re Dennis Montgomery

Mr. Addington, my client has been patient for many years now. If the government wants to resolve things with my client, it best do so asap. John Doubek

From: Addington, Greg (USANV) <Greg.Addington@usdoj.gov>
Sent: Monday, October 26, 2020 11:12 AM
To: John <john@lawyerinmontana.com>
Subject: RE: Letter dated October 9 re Dennis Montgomery

Mr. Doubek:

Thank you for your patience in this matter. Your October 9 letter has been referred to me for response. Your letter references a proposed "Bivens" complaint you intend to file on behalf of Mr. Montgomery. You also reference and provide a copy of the protective order entered by the U.S. District Court in 2007 in litigation involving Mr. Montgomery. As you know, the protective order describes categories of information and materials which cannot be disclosed and which cannot be the subject of discovery or evidentiary presentation, based on the US invocation of its state secrets privilege.

In your letter, you state your view that the protective order "clearly prevents Dennis Montgomery from filing a Bivens complaint and possibly other complaints against the Government." You request this office's views as to "how you want us to proceed."

It is our view the protective order remains in place to preclude disclosure of the categories of information and related materials described in the order, based on the circumstances giving rise to the protective order – including the state secrets privilege invoked by the United States. As you know, the protective order includes a mechanism for US review of materials if there is a concern about specific information or materials which might arguably be encompassed by the order.

We cannot assess what, if anything, in the proposed Bivens complaint might be implicated by the terms of the protective order because we do not have a copy of the proposed complaint. If you will provide me with a draft copy of the Bivens complaint (and any corresponding materials you would anticipate disclosing as part of the filing of the complaint), as contemplated by the terms of the protective order, I will obtain the review of the complaint/materials consistent with the protective order and advise you accordingly. I am supposing that review would be completed within 30 days – though that expectation is tempered by the fact that I do not know if your proposed complaint is 5 pages long or 500 pages long so I cannot now commit to a firm time period for the review.

If you have any questions, do not hesitate to contact me.

GREG ADDINGTON
Assistant United States Attorney
Bruce R. Thompson U.S. Courthouse & Fed. Bldg.
400 South Virginia Street, Suite 900
Reno, NV 89501
(775) 334-3347 - direct
(775) 784-5438 - office
(775) 784-5181 - facsimile
Greg.Addington@usdoj.gov

From: John <john@lawyerinmontana.com>
Sent: Tuesday, October 20, 2020 3:16 PM
To: Addington, Greg (USANV) <GAddington@usa.doj.gov>
Subject: RE: Letter dated October 9 re Dennis Montgomery

Mr. Addington: My client would like to get this matter resolved sooner than later. Because Of Mr. Negroponte's SS directive, my client has been stripped of his rights to do a lot of things for too many years now. Please get back to me asap. John D

From: Addington, Greg (USANV) <Greg.Addington@usdoj.gov>
Sent: Tuesday, October 20, 2020 4:12 PM
To: John <john@lawyerinmontana.com>
Subject: Letter dated October 9 re Dennis Montgomery

Mr. Doubek:

Your above-referenced October 9 letter was received. The matters described therein are being reviewed for appropriate response.

GREG ADDINGTON
Assistant United States Attorney
Bruce R. Thompson U.S. Courthouse & Fed. Bldg.
400 South Virginia Street, Suite 900
Reno, NV 89501
(775) 334-3347 - direct
(775) 784-5438 - office
(775) 784-5181 - facsimile
Greg.Addington@usdoj.gov

EXHIBIT “12”

From:	Eisenberg, Joseph
To:	Terry, Billie
Cc:	Dennis
Subject:	FW: Review of former counsel files at Liner firm by United States
Date:	Monday, May 24, 2010 1:08:10 PM
Attachments:	Liner Document Inventory.pdf Liner Hard Drive Inventory.pdf Liner CD Inventory.pdf

---

-----Original Message-----
From: Gomez, Raphael (CIV) [mailto:Raphael.Gomez@usdoj.gov]
Sent: Monday, May 24, 2010 12:57 PM
To: Ellyn S. Garofalo; Kathleen Goldberg; Eisenberg, Joseph; Michael Flynn
Cc: Wells, Carlotta (CIV); Raya, Sharon M. (CIV)
Subject: Review of former counsel files at Liner firm by United States

Counsel,

As we orally have informed you, the United States has conducted an initial review of the 210 boxes of former counsel files at the Liner firm. All 210 boxes of materials, minus the documents and media pulled for further security review, require no further review by the United States.

Please find attached an inventory of the hard copies, hard drives, and CD's/DVD's that have been pulled from boxes 101 through 210 (please note that the first 100 boxes were discovery produced by eTreppid to Montgomery in the eTreppid case and were released by the United States in late January 2010).

We will forward a projected date for completion of the review of the pulled hard copies, hard drives and CD's/DVD's.

If you have any questions, please email or call.

Raphael Gomez
Carlotta Wells

202 514-1318
202 514-4522

LINER FILES CD INVENTORY

CD No.	ADDITIONAL INFO
BOX 101	
CD - 000001	
CD - 000002	
CD - 000003	
CD - 000004	DVD
CD - 000005	
CD - 000006	
CD - 000007	
CD - 000008	
CD - 000009	
CD - 000010	
CD - 000011	DVD
CD - 000012	DVD
CD - 000013	
CD - 000014	
CD - 000015	DVD
CD - 000016	DVD
CD - 000017	DVD
CD - 000018 *Microsoft XP	
CD - 000019 *Dancing w/ the stars	DVD
CD - 000020 *Dancing w/ the stars	DVD
CD - 000021	
CD - 000022	
CD - 000023	DVD
CD - 000024	DVD
CD - 000025	DVD
CD - 000026	DVD
CD - 000027	DVD
CD - 000028	DVD
CD - 000029	DVD
CD - 000030	DVD
CD - 000031	DVD
CD - 000032	
CD - 000033	
CD - 000034	DVD
CD - 000035	
CD - 000036	
CD - 000037	
CD - 000038	DVD
CD - 000039	DVD
CD - 000040	
CD - 000041	
CD - 000042	DVD
CD - 000043	DVD
CD - 000044	DVD
CD - 000045	

LINER FILES CD INVENTORY

CD - 000046	
CD - 000047	
CD - 000048	
CD - 000049	
CD - 000050	
CD - 000051	
CD - 000052	
CD - 000053	DVD
CD - 000054	
CD - 000055	DVD
CD - 000056	DVD
CD - 000057	
CD - 000058	
CD - 000059	DVD
CD - 000060	DVD
CD - 000061	DVD
CD - 000062	
CD - 000063	DVD
CD - 000064	DVD
CD - 000065	DVD
CD - 000066	DVD
CD - 000067	DVD
CD - 000068	
CD - 000069	
CD - 000070	DVD
CD - 000071	DVD
CD - 000072	DVD
CD - 000073	DVD
CD - 000074	
CD - 000075	
CD - 000076	DVD
CD - 000077	DVD
CD - 000078	DVD
CD - 000079	DVD
CD - 000080	
CD - 000081	
CD - 000082	
CD - 000083	
CD - 000084	
CD - 000085	DVD
CD - 000086	DVD
CD - 000087	DVD
CD - 000088	DVD
CD - 000089	
CD - 000090	
CD - 000091	DVD
CD - 000092	

LINER FILES CD INVENTORY

CD - 000093	DVD
CD - 000094	DVD
CD - 000095	DVD
CD - 000096	DVD
CD - 000097	DVD
CD - 000098	
CD - 000099	
CD - 000100	DVD
CD - 000101	DVD
CD - 000102	
CD - 000103	DVD
CD - 000104	DVD
CD - 000105	DVD
CD - 000106	DVD
CD - 000107	DVD
CD - 000108	DVD
CD - 000109	DVD
CD - 000110	DVD
CD - 000111	DVD
CD - 000112	DVD
CD - 000113	DVD
CD - 000114	DVD
CD - 000115	
CD - 000116	DVD
CD - 000117	DVD
CD - 000118	
CD - 000119	
CD - 000120	DVD
CD - 000121	DVD
CD - 000122	
CD - 000123	
CD - 000124	
CD - 000125	
CD - 000126	
CD - 000127	
CD - 000128	
CD - 000129	
CD - 000130	
CD - 000131	
CD - 000132	
CD - 000133	DVD
CD - 000134	
CD - 000135	
CD - 000136	
CD - 000137	
CD - 000138	
CD - 000139	

LINDER FILES: CD INVENTORY

CD - 000140	
CD - 000141	
CD - 000142	
CD - 000143	
CD - 000144	
CD - 000145	
CD - 000146	
CD - 000147	
CD - 000148	
CD - 000149	
CD - 000150	
CD - 000151	
CD - 000152	
CD - 000153	
CD - 000154	
CD - 000155	
CD - 000156	
CD - 000157	
CD - 000158	
CD - 000159	
CD - 000160	
CD - 000161	
CD - 000162	
CD - 000163	
CD - 000164	
CD - 000165	
CD - 000166	
CD - 000167	
CD - 000168	
CD - 000169	
CD - 000170	
CD - 000171	
CD - 000172	
CD - 000173	
CD - 000174	
CD - 000175	
CD - 000176	
CD - 000177	
CD - 000178	
CD - 000179	
CD - 000180	
CD - 000181	
CD - 000182	
CD - 000183	
CD - 000184	
CD - 000185	
CD - 000186	

LINTER FILES- CD INVENTORY

CD - 000187	
CD - 000188	
CD - 000189	
CD - 000190	
CD - 000191	
CD - 000192	
CD - 000193	
CD - 000194	
CD - 000195	
CD - 000196	
CD - 000197	
CD - 000198	
CD - 000199	DVD
CD - 000200	DVD
CD - 000201	DVD
BOX - 105	
CD - 000223 *Fire Connect	
CD - 000224	
CD - 000225	
CD - 000226	
CD - 000227 *Dark City (Movie)	DVD
CD - 000228 *School of Rock (Movie)	DVD
CD - 000229 *Lost in Trans (Movie)	DVD
CD - 000230 *After the Sunset (Movie)	DVD
CD - 000231	DVD
CD - 000232	DVD
CD - 000233	DVD
CD - 000234	DVD
CD - 000235	DVD
CD - 000236 *Windows XP	
CD - 000237	DVD
CD - 000238	DVD
CD - 000239 *Sync master	
CD - 000240 * Windows XP	
CD - 000241	DVD
CD - 000242 *Video Capture Software	
CD - 000243 *Windows XP	
CD - 000244	DVD
CD - 000245 *Video Capture Software	
CD - 000246 *Windows XP	
CD - 000247	DVD
CD - 000248	DVD
CD - 000249	DVD
CD - 000250	DVD
CD - 000251	
CD - 000252	DVD
CD - 000253	DVD

LINTER FILES: CD INVENTORY

CD - 000254	
CD - 000255	
CD - 000256	DVD
CD - 000257	DVD
CD - 000258	DVD
CD - 000259	
CD - 000260	DVD
CD - 000261	DVD
CD - 000262	DVD
CD - 000263	DVD
CD - 000264	DVD
CD - 000265	
CD - 000266	DVD
CD - 000267	
CD - 000268	DVD
CD - 000269	DVD
CD - 000270	DVD
CD - 000271	DVD
CD - 000272	
CD - 000273	
CD - 000274	DVD
CD - 000275	DVD
CD - 000276	
CD - 000277	
BOX 106	
CD - 000219	
BOX 114	
CD - 000278	
CD - 000279	DVD
CD - 000280	
CD - 000281	DVD
CD - 000282	
CD - 000283* (IBM Commercial)	
CD - 000284	
CD - 000285	
CD - 000286	
CD - 000287	
CD - 000288	DVD
CD - 000289	
CD - 000290	
CD - 000291	
CD - 000292	
CD - 000293	
CD - 000294	
CD - 000295	
CD - 000296	
CD - 000297* (Adobe)	

CD - 000298	
CD - 000299	
CD - 000300	
CD - 000301	
CD - 000302	
CD - 000303	
CD - 000304	
CD - 000305	DVD
CD - 000306	
CD - 000307	
CD - 000308	
CD - 000309* (Music)	
CD - 000310* (Win 95)	
CD - 000311	
CD - 000312	
CD - 000313	
CD - 000314	
CD - 000315	DVD
CD - 000316	
CD - 000317* (WIN 95)	
CD - 000318	DVD
CD - 000319	
CD - 000320	
CD - 000321	
CD - 000322	
CD - 000323	
CD - 000324* (Old Windows Upd.)	
CD - 000325	
CD - 000326	
CD - 000327	
CD - 000328	
CD - 000329* (Elvis pt. 2)	
CD - 000330	
CD - 000331	
CD - 000332	
CD - 000333	
CD - 000334	
CD - 000335	
CD - 000336	
CD - 000337	
CD - 000338	
CD - 000339	
CD - 000340	
CD - 000341	
CD - 000342	
CD - 000343	
CD - 000344	

LINTER FILES- CD INVENTORY

CD - 000345	
CD - 000346	
CD - 000347	
CD - 000348	
CD - 000349	
CD - 000350	
CD - 000351	
CD - 000352	
CD - 000353	
CD - 000354	
CD - 000355	
CD - 000356	
CD - 000357	
CD - 000358	DVD
CD - 000359	
CD - 000360** (Unreadable 360-370)	DVD
CD - 000361	
CD - 000362	
CD - 000363	
CD - 000364	
CD - 000365	
CD - 000366	
CD - 000367	DVD
CD - 000368	
CD - 000369	
CD - 000370**	
CD - 000371* (Dolby Test Files)	
CD - 000372	
CD - 000373* (Kodak Frames)	
CD - 000374* (Partition Magic 8.02)	
CD - 000375	
CD - 000376* (HP)	DVD
CD - 000377* (ADP)	
CD - 000378	
CD - 000379	DVD
CD - 000380	
CD - 000381* (Win XP)	
CD - 000382	
CD - 000383	DVD
CD - 000384* (Mic Office 2003)	
CD - 000385* (Mic XP)	
CD - 000386* (Dancing w/ Stars)	DVD
CD - 000387* (Dancing w/ Stars)	DVD
CD - 000388	DVD
CD - 000389	
CD - 000390	
CD - 000391	DVD

LINTER FILES CD INVENTORY

CD - 000392	DVD
CD - 000393	DVD
CD - 000394	
CD - 000395	
CD - 000396* (Symantec)	
CD - 000397* (Mic XP)	
CD - 000398	DVD
CD - 000399* (Mic Office 2003)	
CD - 000400* (Mic XP)	
CD - 000401* (Dancing w/ Stars)	DVD
CD - 000402* (Dancing w/ Stars)	DVD
CD - 000403	DVD
CD - 000404	
CD - 000405	
CD - 000406	DVD
CD - 000407	DVD
CD - 000408	DVD
CD - 000409	
CD - 000410	
CD - 000411* (Symantec)	
CD - 000412* (Microsoft XP)	
CD - 000413	DVD
CD - 000414* (Mic Office 2003)	
CD - 000415* (Mic XP)	
CD - 000416* (Dancing w/ Stars)	DVD
CD - 000417* (Dancing w/ Stars)	DVD
CD - 000418	DVD
CD - 000419	
CD - 000420	
CD - 000421	DVD
CD - 000422	DVD
CD - 000423	DVD
CD - 000424	
CD - 000425	
CD - 000426*(Symantec)	
CD - 000427* (Mic XP)	
BOX 117	
CD - 000220	
BOX 131	
CD - 000217	
BOX 145	
CD - 000218	
BOX 165	
CD - 000431	
CD - 000432	
BOX 180	
CD - 000221	

LINTER FILES: CD INVENTORY

BOX 181	
CD - 000202	
CD - 000203	
CD - 000204	
CD - 000205	DVD
CD - 000206	DVD
CD - 000207	
CD - 000208	DVD
CD - 000209	
CD - 000210	
CD - 000211	
CD - 000212	DVD
CD - 000213	DVD
CD - 000214	
CD - 000215	
CD - 000216	
CD - 000430	DVD
BOX 188-1	
CD - 000222	
BOX 189	
CD - 000428	
BOX 190	
CD - 000429	
BOX 207	
CD - 000433	
CD - 000434	
CD - 000435	

LINER FILES: DOCUMENT INVENTORY

Present	BOX	CONTENTS	DESCRIPTION	RELEASED	PULL DETAILS
N/A	1	DISCOVERY	N/A	Y	
N/A	2	DISCOVERY	N/A	Y	
N/A	3	DISCOVERY	N/A	Y	
N/A	4	DISCOVERY	N/A	Y	
N/A	5	DISCOVERY	N/A	Y	
N/A	6	DISCOVERY	N/A	Y	
N/A	7	DISCOVERY	N/A	Y	
N/A	8	DISCOVERY	N/A	Y	
N/A	9	DISCOVERY	N/A	Y	
N/A	10	DISCOVERY	N/A	Y	
N/A	11	DISCOVERY	N/A	Y	
N/A	12	DISCOVERY	N/A	Y	
N/A	13	DISCOVERY	N/A	Y	
N/A	14	DISCOVERY	N/A	Y	
N/A	15	DISCOVERY	N/A	Y	
N/A	16	DISCOVERY	N/A	Y	
N/A	17	DISCOVERY	N/A	Y	
N/A	18	DISCOVERY	N/A	Y	
N/A	19	DISCOVERY	N/A	Y	
N/A	20	DISCOVERY	N/A	Y	
N/A	21	DISCOVERY	N/A	Y	
N/A	22	DISCOVERY	N/A	Y	
N/A	23	DISCOVERY	N/A	Y	
N/A	24	DISCOVERY	N/A	Y	
N/A	25	DISCOVERY	N/A	Y	
N/A	26	DISCOVERY	N/A	Y	
N/A	27	DISCOVERY	N/A	Y	
N/A	28	DISCOVERY	N/A	Y	
N/A	29	DISCOVERY	N/A	Y	
N/A	30	DISCOVERY	N/A	Y	
N/A	31	DISCOVERY	N/A	Y	
N/A	32	DISCOVERY	N/A	Y	
N/A	33	DISCOVERY	N/A	Y	

N/A	34	DISCOVERY	N/A	Y	
N/A	35	DISCOVERY	N/A	Y	
N/A	36	DISCOVERY	N/A	Y	
N/A	37	DISCOVERY	N/A	Y	
N/A	38	DISCOVERY	N/A	Y	
N/A	39	DISCOVERY	N/A	Y	
N/A	40	DISCOVERY	N/A	Y	
N/A	41	DISCOVERY	N/A	Y	
N/A	42	DISCOVERY	N/A	Y	
N/A	43	DISCOVERY	N/A	Y	
N/A	44	DISCOVERY	N/A	Y	
N/A	45	DISCOVERY	N/A	Y	
N/A	46	DISCOVERY	N/A	Y	
N/A	47	DISCOVERY	N/A	Y	
N/A	48	DISCOVERY	N/A	Y	
N/A	49	DISCOVERY	N/A	Y	
N/A	50	DISCOVERY	N/A	Y	
N/A	51	DISCOVERY	N/A	Y	
N/A	52	DISCOVERY	N/A	Y	
N/A	53	DISCOVERY	N/A	Y	
N/A	54	DISCOVERY	N/A	Y	
N/A	55	DISCOVERY	N/A	Y	
N/A	56	DISCOVERY	N/A	Y	
N/A	57	DISCOVERY	N/A	Y	
N/A	58	DISCOVERY	N/A	Y	
N/A	59	DISCOVERY	N/A	Y	
N/A	60	DISCOVERY	N/A	Y	
N/A	61	DISCOVERY	N/A	Y	
N/A	62	DISCOVERY	N/A	Y	
N/A	63	DISCOVERY	N/A	Y	
N/A	64	DISCOVERY	N/A	Y	
N/A	65	DISCOVERY	N/A	Y	
N/A	66	DISCOVERY	N/A	Y	
N/A	67	DISCOVERY	N/A	Y	

N/A	68	DISCOVERY	N/A	Y	
N/A	69	DISCOVERY	N/A	Y	
N/A	70	DISCOVERY	N/A	Y	
N/A	71	DISCOVERY	N/A	Y	
N/A	72	DISCOVERY	N/A	Y	
N/A	73	DISCOVERY	N/A	Y	
N/A	74	DISCOVERY	N/A	Y	
N/A	75	DISCOVERY	N/A	Y	
N/A	76	DISCOVERY	N/A	Y	
N/A	77	DISCOVERY	N/A	Y	
N/A	78	DISCOVERY	N/A	Y	
N/A	79	DISCOVERY	N/A	Y	
N/A	80	DISCOVERY	N/A	Y	
N/A	81	DISCOVERY	N/A	Y	
N/A	82	DISCOVERY	N/A	Y	
N/A	83	DISCOVERY	N/A	Y	
N/A	84	DISCOVERY	N/A	Y	
N/A	85	DISCOVERY	N/A	Y	
N/A	86	DISCOVERY	N/A	Y	
N/A	87	DISCOVERY	N/A	Y	
N/A	88	DISCOVERY	N/A	Y	
N/A	89	DISCOVERY	N/A	Y	
N/A	90	DISCOVERY	N/A	Y	
N/A	91	DISCOVERY	N/A	Y	
N/A	92	DISCOVERY	N/A	Y	
N/A	93	DISCOVERY	N/A	Y	
N/A	94	DISCOVERY	N/A	Y	
N/A	95	DISCOVERY	N/A	Y	
N/A	96	DISCOVERY	N/A	Y	
N/A	97	DISCOVERY	N/A	Y	
N/A	98	DISCOVERY	N/A	Y	
N/A	99	DISCOVERY	N/A	Y	
N/A	100	DISCOVERY	N/A	Y	
N/A	101	OTHER	**1 Pull:** **Pull 1:** CDs that appear to be discovery materials	Y	

N/A	102	OTHER	N/A	Y	
YES	103	OTHER	**4 Pulls:** **Pull 1:** 6/19/06 Flynn Email **(001-005)** **Pull 2:** 7/19/06 Flynn Email **(001-004)** **Pull 3:** 8/14/06 Flynn Email **(001-014)** **Pull 4:** 9/26/06 Mongtomery Email **(001-016)**	N	
YES	104	OTHER	**1 Pull:** **Pull 1:** 3/1/06 Flynn Ltr **(001-008)**	N	
N/A	105	OTHER	Hard drives and CDs	N	
N/A	106	OTHER	**1 Pull:** **Pull 1:** CD	Y	
YES	107	PLEADINGS	**6 Pulls:** **Pull 1:** 3/11/06 Dec of Flynn **(001-004);** **Pull 2:** 3/11/06 Dec of Flynn **(001-004);** **Pull 3:** 4/3/06 Reply Memo **(001-029);** **Pull 4:** 4/21/08 Reply Memo **(001-035);** **Pull 5:** 3/11/06 Dec of Flynn **(001-006);** **Pull 6:** 4/3/06 Reply Memo **(001-029)**	y	
YES	108	PLEADINGS	**2 Pulls:** **Pull 1:**Flynn Declaration **(001-007)** **Pull 2:** 3/17/07 Email (**001-002)**	Y	
YES	109	OTHER	**2 Pulls:** **Pull 1:** 2/26/07 Email **(001);** **Pull 2:** 2/13/07 Email **(001)**	Y	
N/A	110	OTHER	N/A	Y	
N/A	111	OTHER	N/A	Y	
N/A	112	OTHER	N/A	Y	
YES	113	OTHER	**5 Pulls:** **Pull 1:** 2/13/07 Email **(001-009);** **Pull 2:** 2/26/07 Email **(001-004);** **Pull 3:** 3/16/07 Email **(001-012);** **Pull 4:** 3/16/07 Email **(001-008);** **Pull 5:** 3/24/07 Email **(001-003)**	N	
N/A	114	OTHER	CDs for review	N	
N/A	115	PLEADINGS	N/A	Y	
N/A	116	OTHER	Hard drives	N	

YES	117	PLEADINGS	**4 Pulls:** **Pull 1:** 3/11/06 Dec of Flynn; **(001-004)** **Pull 2:** 4/3/06 Reply Mem **(001-029);** **Pull 3:** CD pulled; **Pull 4:** List of T. Pham file pulled **(001-014)**	Y	
YES	118	PLEADINGS	**1 Pull:** **Pull 1:** 3/11/06 Dec of Flynn **(001-004)**	Y	
YES	119	PLEADINGS	**4 Pulls:** **Pull 1:** 5/21/08Reply Memo **(001-035);** **Pull 2:** 3/11/06 Dec of Flynn **(001-010);** **Pull 3:** 4/3/06 Reply Memo **(001-029); *** **Pull 4:** (001-004) 3/11/06 Dec of Flynn **(001-004)**	Y	
YES	120	OTHER	**3 Pulls:** **Pull 1:** 9/26/06 Montgomery Email **(001)** **Pull 2:** 9/26/06 Montgomery Email **(001)** **Pull 3:** 9/26/06 Montgomery Email **(001)**	**Y**	
N/A	121	OTHER	N/A	Y	
N/A	122	OTHER	N/A	Y	
N/A	123	OTHER	N/A	Y	
YES	124	OTHER	**1 Pull:** **Pull 1:** Montgomery Discovery (not Bates labeled by parties) **(001-120)**		
YES	125	OTHER	**20 Pulls:** **Pull 1:** 5/4/07 Flynn Ltr **(001-013);** **Pull 2:** 5/5/07 Flynn Ltr **(001-013);** **Pull 3:** 9/23/06 SF.95.doc **(001-013);** **Pull 4:** 8/24/06 Interrogatories **(001-018);** **Pull 5:** 3/1/06 Draft Rumsfield, et al. Ltr **(001-046);** **Pull 6:** 6/3/07 Flynn Email **(001)** **Pull 7:** 6/3/07 Flynn Email **(001-008)** **Pull 8:** 6/6/07 Flynn Email **(001)** **Pull 9:** 6/10/07 Flynn Email **(001)** **Pull 10:** Exhibit Listing and Description **(001-002)** **Pull 11:** 6/23/07 Flynn Email **(001-004)** **Pull 12:** 6/23/07 Flynn Email **(001-003)** **Pull 13:** 6/23/07 Flynn Email **(001-004)** **Pull 14:** 6/23/07 Flynn Email **(001-002)** **Pull 15:** 4/13/07 Flynn Ltr **(001-010)** **Pull 16:** Draft Flynn Ltr **(001-015)** **Pull 17:** 5/8/07 Flynn Email **(001-002)**	**Pull 18:** 5/9/07 Flynn Email **(001-003)** **Pull 19:** Rumsfeld Ltr **(001-008)** **Pull 20:** 4/9/07 Flynn Email **(001-002)** N	

YES	126	OTHER	**17 Pulls:** **Pull 1:** 5/8/07 Mont Email **(001-002);** **Pull 2:** 3/1/06 Rumsfield Ltr **(001-007;** **Pull 3:** Etreppid legal spreadsheet **(001-033);** **Pull 4:** 6/10/07 Email **(001-003);** **Pull 5:** 6/10/07 Email**(001-002);** **Pull 6:** 6/10/07 Email **(001-002);** **Pull 7:** 6/10/07 Emai **(001-002l;** **Pull 8:** 6/10/07 Email **(001-003);** **Pull 9:** 6/6/07 Email **(001-002);** **Pull 10:** 6/4/07 Email **(001-003);** **Pull 11:** 6/3/07 Email (**001-017);** **Pull 12:** 6/11/07 Montgomery Declaration **(001-004);** **Pull 13:** 6/10/07 Email **(001-021);** **Pull 14:** 3/11/06 Declaration **(001-009);** **Pull 15:** Reply Memo Buckthorne **(001-037);** **Pull 16:** 4/18/06 Email **(001-004);** **Pull 17:** Montgomery Objection to DOD (06-cv-056 Dkt# 125) **(001-010)**	N	
N/A	127	OTHER	Hard drives	N	
N/A	128	OTHER	N/A	Y	
N/A	129	OTHER	N/A	Y	
N/A	130	OTHER	N/A	Y	
N/A	131	OTHER	**1 Pull:** **Pull 1:** CD	Y	
N/A	132	OTHER	N/A	Y	
N/A	133	OTHER	N/A	Y	
YES	134	OTHER	**4 Pulls:** **Pull 1:** 7/5/06 Email **(001-014);** **Pull 2:** 5/30/06 Email **(001-002);** **Pull 3:** Notes **(001-007);** **Pull 4:** 9/26/06 Flynn Email **(001-008)**	N	
YES	135	PLEADINGS	**4 Pulls:** **Pull 1:** Montgomery Declaration **(001-004)** **Pull 2:** Response to DOD Motion **(001-202)** **Pull 3**: Montgomery Declaration **(001-023)** **Pull 4:** 10/30/06 Sealed Montgomery Decl. in Response to DOD Motion for Protective Order -Signed-**(001-023)**		Pull 1:001-004 Pull 2: 001-202

YES	136	OTHER	**4 Pulls:** **Pull 1:** 7/5/06 Email **(001);** **Pull 2:** Contract Documents **(001-010);** **Pull 3:** Negroponte Questions **(001-005)** **Pull 4:** Montgomery Declaration **(001-022)**	Y	Pull 1: 001-022 Pull 2:
YES	137	OTHER	**3 Pulls**: **Pull 1:** 4/10/06 Park Email **(001-004);** **Pull 2:** 3/11/06 Flynn Declaration -Unsigned- **(001-004)** **Pull 3:** Reply Memo for Return of Property **(001-029)**	Y	Pull 2: 001-004 Pull 3: 001-029
YES	138	PLEADINGS	N/A	Y	
YES	139	OTHER	**30 Pulls:** **Pull 1:** 2/2007 Flynn Declaration **(001-016);** **Pull 2:** 2/2007 Montgomery Declaration **(001-009;** **Pull 3:** 2/26/2007 Email **(001);** **Pull 4:** 2/13/2007 Email **(001-003);** **Pull 5:** 2/2007 Montgomery Declaration **(001-005);** **Pull 6:** 2/2007 Montgomery Declaration **(001-006);** **Pull 7:** 2/2007 Flynn Declaration in Supp of Montgomery Opp. to Govt Motion to Strike **(001-018);** **Pull 8:** 2/2007 Montgomery Declaration 2 copies -Unsigned-**(001-019);** **Pull 9:** 3/2007 Email Chain **(001-011);** **Pull 10:** 3/16/07 Email **(001-004);** **Pull 11:** Complaint for violation of false claims act **Draft-1 (001-046);** **Pull 12:** Complaint for violation of false claims act **Draft-2 (001-047);** **Pull 13:** Complaint for violation of false claims act **Draft-3 (001-044);** **Pull 14:** Complaint for violation of false claims act **Draft-4 (001-040);**	**Pull 15:** Complaint for violation of false claims act Draft-5 **(001-046);** **Pull 16:** Complaint for violation of false claims act Draft-6 **(001-046);** **Pull 17:** Flynn Declaration **(001-004);** **Pull 18:** Flynn Declaration **(001-006);** **Pull 19:** Motion to Unseal **(001-017);** **Pull 20:** Flynn Declaration **(001-012);** **Pull 21:** Flynn Declaration **(001-011);** **Pull 22:** Negroponte Questions **(001-009);** **Pull 23:** Negroponte Questions **(001-006);** **Pull 24:** Negroponte Questions **(001-004);** **Pull 25:** Negroponte Questions **(001-004);** **Pull 26:** 2/9/07 Flynn Ltr **(001-005);** **Pull 27:** 2/9/07 Flynn Ltr **(001-005);** **Pull 28:** 2/9/07 Flynn Ltr **(001-003);** **Pull 29:** 3/24/07 Email **(001-002)** **Pull 30:** 1/2007 Montgomery Declaration **(001-007)** N	

YES	140	OTHER	**7 Pulls:** **Pull 1:** Transcript Excerpt **(001-005);** **Pull 2:** Transcript Excerpt **(001-005);** **Pull 3:** 8/16/06 Sealed Declaration of Montgomery -Unsigned- **(001-009);** **Pull 4:** 8/16/06 Sealed Declaration of Montgomery -Unsigned-**(001-019);** **Pull 5:** 8/16/06 Sealed Declaration of Montgomery -Unsigned- **(001-020);**	**Pull 6:** 10/06 2 Copies Sealed Declaration of Montgomery -Unsigned **(001-045)**; **Pull 7:** 11/30/06 Sealed Declaration of Montgomery -Unsigned- **(001-022)** N	
N/A	141	PLEADINGS	N/A	Y	
N/A	142	OTHER	N/A	Y	
N/A	143	OTHER	N/A	Y	
N/A	144	OTHER	N/A	Y	
N/A	145	OTHER	**1 Pull:** **Pull 1:** CD	Y	
N/A	146	PLEADINGS	N/A	Y	
YES	147	OTHER	**10 Pulls:** **Pull 1:** MONT40-43 **(001-004);** **Pull 2:** MONT 288-296 **(001-008);** **Pull 3:** MONT318-337 **(001-020);** **Pull 4:** 4/13/07 Flynn Ltr **(001-018);** **Pull 5:** 2/9/07 Flynn Ltr (2 copies) **(001-010);** **Pull 6:** 6/22/06 Email **(001-002);** **Pull 7:** 6/22/06 Email **(001-005);** **Pull 8:** 3/1/06 Flynn Ltr **(001-013);** **Pull 9:** 6/23/07 Flynn Email **(001-007);** **Pull 10:** 6/23/07 Flynn Email **(001)**	Y	
N/A	148	OTHER	N/A	Y	
N/A	149	PLEADINGS	N/A	Y	
YES	150	PLEADINGS	**2 Pulls:** **Pull 1:** 10/06 Draft Montgomery Response to DOD Motion for Protective Order **(001-044);** **Pull 2:** 03/22/07 Montgomery Response to DOD Motion for Reconsideration **(001-009)**	Y	**Pull 1: 001-044** **Pull 2:** 001-009
YES	151	OTHER	**1 Pull:** **Pull 1:** 6/11/07 Montgomery Declaration **(001-004)**	Y	
N/A	152	PLEADINGS	N/A	Y	
N/A	153	OTHER	N/A	Y	
N/A	154	OTHER	N/A	Y	
N/A	155	OTHER	N/A	Y	

N/A	156	PLEADINGS	N/A	Y	
N/A	157	PLEADINGS	N/A	Y	
YES	158	OTHER	**6 Pulls:** **Pull 1:** 4/13/07 Flynn Ltr **(001-018)**; **Pull 2**: 2/9/07 Flynn Ltr **(001-010)**; **Pull 3:** 6/22/06 Flynn Email **(001-002)**; **Pull 4:** 6/22/06 Flynn Email **(001-002);** **Pull 5:** 3/1/06 Flynn Ltr **(001-013)**; **Pull 6:** 7/26/06 Flynn Ltr **(001-007)**	Y	
N/A	159	PLEADINGS	N/A	Y	
N/A	160	OTHER	N/A	Y	
N/A	161	PLEADINGS	N/A	Y	
N/A	162	DISCOVERY	N/A	Y	
N/A	163	PLEADINGS	N/A	Y	
YES	164	OTHER	**1 Pull:** **Pull 1:** 4/13/07 Flynn Ltr. **(001-009)**	Y	
YES	165	OTHER	**2 Pulls:** **Pull 1:** CD With Document Attached **(001)** **Pull 2:** CD With Document Attached **(001-030)**	Y	
YES	166	OTHER	**3 Pulls:** **Pull 1:** DM2845-2886 **(001-042)**; **Pull 2:** DM2987-2998 **(001-012)**; **Pull 3:** DM3145-3151 **(001-007)**	Y	
N/A	167	OTHER	N/A	Y	
N/A	168	PLEADINGS	N/A	Y	
N/A	169	OTHER	N/A	Y	
N/A	170	OTHER	N/A	Y	
YES	171	OTHER	**1 Pull:** **Pull 1:** Draft Flynn Ltr **(001-008)**	Y	
YES	172	OTHER	**1 Pull:** **Pull 1:** Potential witness list with handwritten notations **(001-002)**	Y	
N/A	173	PLEADINGS	N/A	Y	
YES	174	PLEADINGS	**4 Pulls:** **Pull 1:** 2/27/07 Dec of Flynn**(001-037);** **Pull 2:** 6/2/06 Dec of Michael West **(001-008)**; **Pull 3**: 06-cv-0263 Dkt# 125 Transcript **(001-085)**; **Pull 4:** 3/3/06 Dec of Michael West **(001-014)**	Y	
N/A	175	PLEADINGS	N/A	Y	

YES	176	OTHER	**2 Pulls:** **Pull 1:** 4/13/07 Flynn Ltr to Cheney **(001-009)**; **Pull 2**: Dec of Flynn **(001-020)**	Y	
N/A	177	PLEADINGS	N/A	Y	
N/A	178	OTHER	N/A	Y	
YES	179	OTHER	**2 Pulls:** **Pull 1:** 6/3/07 Email **(001-012)**; **Pull 2:** 5/8/07 Email **(001)**	Y	
N/A	180	OTHER	**1 Pull:** CD	Y	
N/A	181	OTHER	**5 Pulls:** 5 CDs pulled	Y	
N/A	182	PLEADINGS	N/A	Y	
N/A	183	OTHER	N/A	Y	
N/A	184	OTHER	N/A	Y	
N/A	185	OTHER	N/A	Y	
N/A	186	OTHER	N/A	Y	
N/A	187	OTHER	N/A	Y	
N/A	188	PLEADINGS	**1 Pull:** CD pulled	Y	
N/A	189	OTHER	**1 Pull:** CD pulled	Y	
N/A	190	OTHER	**1 Pull:** CD pulled	Y	
N/A	191	OTHER	**2 Pulls:** 2 Hard drives removed	Y	
N/A	192	OTHER	N/A	Y	
YES	193	PLEADINGS	**2 Pulls:** **Pull 1:** 06-cv-0263 Dkt# 103, MONT318-337 **(001-020)**; **Pull 2:** MONT288-296 **(001-009)**;	Y	
N/A	194	OTHER	N/A	Y	
YES	195	PLEADINGS	**1 Pull:** 3/22/07 Montgomery's Response to DoD's Request for Protection Order **(001-009)**	Y	
YES	196	OTHER	**1 Pull:** **Pull 1:** Prayer for Relief **(001-042)**	Y	
YES	197	PLEADINGS	**1 Pull** : **Pull 1:** 3/11/06 Dec of Flynn **(001-006)**	Y	
N/A	198	DISCOVERY	N/A	Y	
N/A	199	PLEADINGS	N/A	Y	
N/A	200	PLEADINGS	N/A	Y	
N/A	201	OTHER	Hard drives	N	
N/A	202	OTHER	Hard drives	N	

N/A	203	OTHER	Hard drives	N	
N/A	204	OTHER	N/A	Y	
YES	205	OTHER	**8 Pulls:** **Pull 1:** 4/10/06 Email **(001-004);** **Pull 2:** 10/31/07 Email **(001-002);** **Pull 3**: 3/16-18/07 Email chain **(001-004);** **Pull 4:** 3/16-18/07 Email chain **(001-007);** **Pull 5**: 3/16-18/07 Email chain **(001-007);** **Pull 6:** 6/23/07 Email **(001);** **Pull 7:** 3/11/06 Dec of Montgomery for Return of Property -Unsigned- & 4/3/06 Reply Memo un Support of Motion for Return of Property **(001-033);** **Pull 8:** 3/11/06 Dec of Flynn: **(001-004)**	Y	
N/A	206	OTHER	N/A	Y	
YES	207	PLEADINGS	**6 Pulls:** **Pull 1:** 2 CDs **Pull 2:** Cover sheet and Index of Emails in "Inbox" **(001-0038)** **Pull 3:** Index of Emails in "Sent" **(001-015)** **Pull 4:** 1 CD **Pull 5:** Index of Emails in "Inbox" **(001-037)** **Pull 6:** Index of Emails in "Sent" **(001-016)**	Y	
N/A	208	OTHER	N/A	Y	
YES	209	PLEADINGS	**3 Pulls:** **Pull 1:** Sealed Montgomery Declaration **(001-036)** **Pull 2:** Working Chronology **(001-014)** **Pull 3:** Sealed Montgomery Declaration **(001-022)**	Y	Pull 3: 001-022
N/A	210	OTHER	Hard drives	N	

LINER FILES: HARD DRIVE INVENTORY

HARD DRIVE No.	SERIAL No.	ADDITIONAL INFO	DOJ COPY SERIAL No.	CLIENT COPY SERIAL No.
BOX 105				
HD - 40	WMAEH1731597	Security Bag No. 075287		
HD - 41	WCAEP1015275	Security Bag No.075277		
HD - 42	WMAMR1202131	Security Bag No. 075269		
HD - 43	ZFUG712N	Security Bag No.075256; Copy of WMA8C2315047		
HD - 44	WMAEH1732002	Security Bag No. 075292		
HD - 45	9QG8HSDQ	Security Bag No. 075273		
HD - 46	WMA9P1151187	Security Bag No.075284		
HD - 47	9QG8N147	Security Bag No. 075245; Copy of WMAMR1203238		
HD - 48	6QF462VG	Security Bag No.075279; Copy of WCAEP1015275		
HD - 49	WMAEP1123872	Security Bag No. 075263		
HD - 50	3PM08V7Q			
HD - 51	5QD337JK			
HD - 52	WMACK1617687	Security Bag No. 75261		
HD - 53	WMAEP1142476	Security Bag No. 075286		
HD - 54	RG0VEH9A	Security Bag No. 075290: Copy of WMAEH1732002		
HD - 55	WMAMR1202248	Security Bag No. 075260		
HD - 56	WMAEH1283328	Security Bag No.075289		
HD - 57	WMAMR1277950	Security Bag No.075281		
HD - 58	WMAEH1202303	Security Bag No. 075265		
HD - 59	6QF46574	Security Bag No. 075271; Copy of WMAEH1202303		
HD - 60	WCAL75136659	Security Bag No. 075285		

LINER FILES: HARD DRIVE INVENTORY

HD - 61	7BA08HPG	Security Bag No. 075288		
HD - 62	WMA8C2315047	Security Bag No. 075257		
HD - 63	WMAMR1068824	Security Bag No. 075267		
HD - 64	WMAMR1203238	Security Bag No. 075246		
HD - 65				
HD - 66				
HD - 67				
HD - 68				
HD - 69				
HD - 70				
HD - 71				
HD - 72				
HD - 73				
HD - 74				
HD - 75				
HD - 76				
HD - 77				
HD - 78				
HD - 79				
HD - 80				
HD - 81				
HD - 82				
HD - 83				
HD - 84				
HD - 85				
HD - 86				
HD - 87				
HD - 88				
HD - 89				
HD - 90				
BOX 116				
HD - 1	WMA8C4544113	Security Bag No. 033654517		
HD - 2	WCARW0431467	Security Bag No. 075298; Copy of WMAEH2602257		
HD - 3	WCARW0415948	Security Bag No. 033654510; Copy of WMAEH2694097		
HD - 4	WCA8C3998460	Security Bag No. 033654515		
HD - 5	WMAEH2694097	Security Bag No. 033654518		
HD - 6	WCAEP1014382	Security Bag No. 033654520		

LINER FILES: HARD DRIVE INVENTORY

HD - 7	WMAEH2602257	Security Bag No. 033654516		
HD - 8	WCAEP1003948	Security Bag No. 033654519		
HD - 9	9QG812MG			
HD - 10	9QJ0RXGJ			
BOX 127				
HD - 13	WMAMR1538581			
HD - 14	WMAMR1612253			
HD - 15	WMAMR1624507			
HD - 16	WMA8C3243070			
HD - 17	WMAD15194737			
HD - 18	WMAD15335294			
HD - 19	3CK00XXY			
HD - 20	WMA8C1223396			
HD - 21	WCAD13691228			
HD - 22	WMAMR1673681			
HD - 23	WMAD16644525			
HD - 24	WMAMR1538197			
HD - 25	3CK028W3			
HD - 26	WMAMR1538570			
HD - 27	WMAMR1509932			
HD - 28	WMAMR1580671			
HD - 29	WMAA61102098			
HD - 30	2544801F3NQ0C6			
HD - 31	WMAMR1523649			
HD - 32	WMAMR1580666			
HD - 33	WMAMR1066012			
HD - 34	WMAMR1537929			
HD - 35	WMAMR1539942			
HD - 36	WMAMR1539825			
HD - 37	WCAD16502878			
HD - 38	WMAD15256807			
HD - 39	WMAMR1543003			
BOX 191				
HD - 11	9QG7CDDE	Security Bag No. 072755		
HD - 12	6QG31F7K	Security Bag No.072754		
BOX 201				
HD - 65	3PM0686P			
HD - 66	9QM26YN3			
HD - 67	9QM3FKKW			
HD - 68	3QD03188			
BOX 202				
HD - 69	3QD08W2N			
HD - 70	3QD0L7T0			
HD - 71	9QJ0WW9R			
BOX 203				
HD - 72	9QJ16874			
HD - 73	PAG2NLRC			
HD - 74	3QJ01RQ1			

LINER FILES: HARD DRIVE INVENTORY

HD - 75	3PM0LVN8			
HD - 76	5QG06MMH			
BOX 210 *Labeled as defective				
HD - 77	RBRAPJNA	Security Bag No. 075274; Copy of WMA8C4544113		
HD - 78	WCARW0431405	Security Bag No. 075255; Copy of WCAEP1003948		
HD - 79	RG0VEMRA	Security Bag No. 075254; Copy of WMAEP1142476		
HD - 80	WCARW0431298	Security Bag No. 033654504; Copy of WCAEP1014382		
HD - 81	R7CRDRKK	Security Bag No. 075293; Copy of WMACK1617687		
HD - 82	RG0VAUYA	Security Bag No. 075278; Copy of WMAEH1731597		
HD - 83	RG0VEMKA	Security Bag No. 075283; Copy of WCAL75136659		
HD - 84	9QG8LXX5	Security Bag No. 075295; Copy of WMAMR1277950		
HD - 85	9Q8N28G	Security Bag No. 075248; Copy of WMAMR1202131		
HD - 86	N/A	N/A		
HD - 87	R7CRD72K	Security Bag No. 033654508; Copy of WMAEH1283328		
HD - 88	RBRAA9VA	Security Bag No. 033654501; Copy of WCA8C3998460		
HD - 89	9QG8LSVQ	Security Bag No. 075252; Copy of WMAMR1202248		

LINER FILES: HARD DRIVE INVENTORY

HD - 90	RG0ZLL8A	Security Bag No. 075262; Copy of WMAEP1123872		

EXHIBIT “13”

UNITED STATES BANKRUPTCY COURT
CENTRAL DISTRICT OF CALIFORNIA

In re: Dennis and Kathleen Montgomery)
)
Michael J. Flynn,)
)
Plaintiff,)
)
vs.) Case No.: 2:10-bk-18510-bb
)
Dennis Lee Montgomery and Brenda Kathleen Montgomery,)
)
Defendants.)

Videotaped Deposition of: DENNIS LEE MONTGOMERY
Date: November 18, 2010
Reported by: Stephanie P. Borthwick
C.S.R. No. 12088

Deposition of DENNIS LEE MONTGOMERY, taken on behalf of the Plaintiff, before Stephanie P. Borthwick, a Certified Shorthand Reporter, commencing at the hour of 9:20 a.m., Thursday, November 18, 2010, at the offices of Yates Court Reporters, 74967 Sheryl Avenue, Palm Desert, California.

APPEARANCES:

For the Plaintiff:
CONANT LAW, LLC
Attorneys at Law
BY: CHRISTOPHER J. CONANT, ESQ.
730 17th Street
Suite 200
Denver, Colorado 80202
(303) 298-1800

For the Defendants:
DION-KINDEM & CROCKETT
Attorneys at Law
BY: WILLIAM E. CROCKETT, ESQ.
LNR Warner Center
21271 Burbank Boulevard
Suite 100
Woodland Hills, California 91367-6667
(818) 883-4400

For the United States of America:
U.S. DEPARTMENT OF JUSTICE
CIVIL DIVISION
BY: CARLOTTA P. WELLS, Senior Counsel
Federal Programs Branch
20 Massachusetts Avenue, NW
Room 7150
Washington, DC 20530
(202) 514-4522

Also Present:
Michael J. Flynn, Esq.
Sharon Raya, Paralegal to Ms. Wells
Tom (last name withheld), U.S. Government
Morgan (last name withheld), U.S. Government

Videographer:
Jesse Navarro, Orravan Video Litigation Services

INDEX

Deposition of DENNIS LEE MONTGOMERY
Taken on November 18, 2010

Information Requested:
(None)

///
///

THE VIDEOGRAPHER: Good morning. Here begins Media No. 1 in the video deposition of Dennis Lee Montgomery in the matter of Michael J. Flynn versus Dennis Lee Montgomery, et al., in the United States Bankruptcy Court of California, Case No. 2:10-bk-18510-bb.

Today's date is November 18th, 2010. The time is 9:20 a.m. This deposition is being taken at 74967 Sheryl Avenue, Palm Desert, California, and was made at the request of Mr. Christopher Conant of the law offices of Conant Law, LLC.

The videographer is Jesse Navarro here on behalf of Orravan Video Litigation Services, Indian Wells, California.

Would counsel and all present please identify yourselves and state whom you represent.

MR. CONANT: Christopher Conant for the plaintiff, Michael J. Flynn.

MR. FLYNN: And Michael J. Flynn in persona.

MS. WELLS: Carlotta Wells on behalf of the United States and with the United States Department of Justice. Sharon Raya is with me from my office. With me, also, are Morgan and Tom, who are with the government and I can't disclose anything further

because to do so would violate the terms of the United States protective order, which all the parties to the bankruptcy proceeding have agreed to.

MR. CROCKETT: Bill Crockett on behalf of Dennis Montgomery.

THE WITNESS: Dennis Montgomery.

THE VIDEOGRAPHER: Would the court reporter please swear in the witness.

THE REPORTER: Please raise your right hand.

Do you solemnly state under penalty of perjury that the testimony you will give in this matter will be the truth, the whole truth, and nothing but the truth?

THE WITNESS: Yes.

THE REPORTER: Thank you.

MR. CONANT: Okay. Thank you.

Before we start examining the witness, I want to state for the record that there are present in the room four representatives from the U.S. Government, two of which apparently have no last name.

We'll ask on the record of Ms. Wells to provide their last names and the government agency that they purportedly work for.

MS. WELLS: And I cannot, because to do so would violate the terms of the United States protective order.

MR. CONANT: Ms. Wells, do you have a copy of the protective order in front of you?

MS. WELLS: I do. Do you have one?

MR. CONANT: I have a copy in front of me. I'd like to actually get it admitted as an exhibit in this deposition.

Let me -- while I work on getting extra copies to admit as an exhibit, Ms. Wells, can you review the protective order and identify which specific portion of the protective order you're --

MS. WELLS: Am I a witness now? All I can tell you is it's pretty self-evident from the face of the United States protective order what's protected, what isn't.

The information that's protected is set forth in paragraphs 2 and paragraphs 3.

MR. CONANT: How does those pertain specifically to the identities of these gentlemen and why they're here today?

MS. WELLS: I think it's self-evident and if you want to read those paragraphs into the record, feel free to.

MR. CONANT: I don't -- well --
MS. WELLS: Paragraphs 2 and 3 of the United States protective order, which is Document 253, District of Nevada Case File 30656.
MR. CONANT: Ms. Wells, who is making the decision regarding what is -- why these gentleman are here?
Who in the government made a decision why these gentlemen are here? Who in the government made a decision for these two gentlemen to be here today?
MS. WELLS: This particular deposition is being handled in the manner that all information related to this case has been handled. It's been a joint decision between those attorneys representing the United States' interests and the agencies whose information we're protecting.
That's all I'm going to say.
MR. CONANT: Were these gentleman at all involved in any way in the litigation in Nevada?
MS. WELLS: I'm not going to go any further than what I've already said.
MR. CONANT: Were you meeting with Judge Pro in the U.S. District Court for the district of Nevada yesterday?

MS. WELLS: At Judge Pro's insistence, yes. We met with him in his chambers yesterday.
MR. CONANT: Who is "we"?
MS. WELLS: The people representing the United States Department of Justice and the United States in this case.
MR. CONANT: Who were those? I'm asking for the identities, Ms. Wells.
MS. WELLS: All I'm saying is that people from the government met with him and I mean it actually -- if you really need to know, it was the four of us here.
MR. CONANT: Did Judge Pro -- when did Judge Pro contact you to meet with him?
MS. WELLS: I'm not going to say anything more other than we're complying with the terms of the order that Judge Pro entered, I believe it was October 30th, and we were there because of that order.
MR. CONANT: What order?
MS. WELLS: Let's see.
It was the order dated October 28th, 2010, Docket No. 1172, same case, Montgomery versus eTreppid Technology.
MR. CONANT: Were there any documents

reviewed in connection with your meeting with Judge Pro that were -- that originated from my client Michael Flynn?
MS. WELLS: This is not the subject of this deposition. We're not here to talk about this. If Mr. Flynn wants to have a conversation with me about this we can have it, but it's not appropriate for the record.
MR. CONANT: It is appropriate for the record. You are --
MS. WELLS: It does -- what does that have to do with the information we're here to protect now? The long and the short of it is that there were documents, as you know, from the Order that the court in Montana sent to Judge Pro.
He asked the United States to take a look at them to determine the extent to which there's information that may or may not be protected under the United States protective order.
Upon the limited review that we did in his chambers yesterday, we determined that there was enough of a question there that we need to take the documents back with us to Washington to do a more thorough review. That's it.
MR. CONANT: What documents did you review?

MS. WELLS: The documents that the court in Montana sent.
MR. CONANT: What documents were those?
MS. WELLS: I didn't take a list. It's not a very big -- it's a small pile, not even an inch thick.
MR. FLYNN: This is Michael Flynn. I'm going to put a statement on the record.
The documents that were given to David Cotner, counsel for the trustee in the Montana bankruptcy proceeding, were very limited and I specifically reviewed them before giving them to Cotner.
They were apparently subsequently given to Judge Kirscher and they had all been previously reviewed by the federal government, Department of Justice, and approved. And except for the Sandoval complaint, they are publicly on file in the Nevada District Court and can be picked up online.
So unless documents were added that I don't know about -- and I don't know about any of the documents, I don't have the identity of the documents that were given to Judge Kirscher or subsequently conveyed to Judge Pro -- there are no documents that do not comply with the US protective

order in any way.
So if either documents were added by someone or there has been a change in the position of the Department of Justice with regard to the scope of the protective order, then there is nothing in any of the documents given to Cotner, apparently passed on to Judge Kirscher, which would violate the terms of the U.S. protective order.
MR. CONANT: Do you have a copy, Ms. Wells, of the letter or whatever communication there was between Judge Kirscher and Judge Pro?
MS. WELLS: No.
MR. CONANT: Who at the government have you been talking to regarding the matter involving the letter from Judge Kirscher to Judge Pro?
MS. WELLS: I'm not here to answer these questions. I'm here to enforce the terms of the United States protective order and only people with the United States have that authority and the ability to determine what's protected and what isn't and that's all we're here for.
It's a very limited role that we're playing, it's a very limited role, and I can tell you on the record that what we're doing here today is entirely consistent with what we've done ever

since we first got involved in this case and ever since Judge Pro acknowledged there was information to be protected.
That's all I'm going to say and I'll keep saying the same thing over and over again.
MR. FLYNN: It's completely inaccurate. For the record, these gentlemen, however nice gentleman they may be, never participated and never appeared in courtrooms in any of the Nevada proceedings, Ms. Wells, and you know it and I know it.
So this four-person deluge from the Department of Justice in Dennis Montgomery's deposition is apparently being done for some reasons completely extraneous to the materials in the protective order, but why don't we get started.
MR. CONANT: I just want to state one last thing for the record. When I deposed Istvan Burgyan in this very case on September 22nd, the U.S. Government showed no interest in this matter.
I had to call Mr. Gomez at his office in D.C. halfway through the deposition, because there became an issue regarding the protective order. Mr. Gomez was completely indifferent regarding this case and now, for some reason, we have four people

here from the US government, two of who, apparently, have no last names and are from some unidentified agency with the government.
And for the record, Ms. Wells is not indicating how their involvement is at all implicated in the protective order. The protective order only governs issues concerning intelligence agencies as defined in the National Security Act and we have no indication of what agencies these gentlemen are with and whether they're with an intelligence agency or whether it's an administrative branch of the government that's not included within the National Security Act as an intelligence agency.
So we simply don't know what is -- what is purportedly being protected by the protective order or not.
MR. FLYNN: We think -- at this juncture I'll put on the record that I believe -- I didn't believe it during the Nevada proceedings, I thought there were legitimate interests to be protected in terms of identities of intelligence agency individuals, but at this point I believe that the Department of Justice has gone far beyond that and is now using, under the guise of national security

for reasons related to the facts that I put in the emails to you, Carlotta, has gone far beyond the scope of national security in an effort to cover up or conceal the fraudulent activities of Mr. Montgomery as I've repeatedly said in emails.
So why don't we just start.

EXAMINATION

BY MR. CONANT:
Q. Okay. All right. Turning to Mr. Montgomery. Mr. Montgomery, let's start something.
Can you state your name for the record.
A. Dennis Montgomery.
Q. What's your -- do you have a middle name?
A. Lee.
Q. Do you understand what it means to take a deposition, Mr. Montgomery?
A. Yes.
Q. What do you understand that to mean?
A. You're going to ask me questions; I'm going to answer them.
Q. Do you know -- do you understand that your testimony today is under the penalty of perjury?
A. Yes.
Q. Do you understand what that means?

EXHIBIT “14”

dennismontgomery45@gmail.com

From: Dennis <dennis@ncoder.net>
Sent: Thursday, August 29, 2013 3:43 PM
To: 'Cameron, Carl'
Subject: RE: CIA

I know a lot going in DC today, just call me tomorrow.

From: Cameron, Carl [mailto:CARL.CAMERON@FOXNEWS.COM]
Sent: Thursday, August 29, 2013 11:57 AM
To: Dennis
Subject: Re: CIA

Understood. As I say I happen to be out there next week so we'll get together.

Carl Cameron, Chief Political Correspondent, Fox News, From Mobile, please excuse autocorrect errors.

From: Dennis
Sent: Thursday, August 29, 2013 1:23 PM
To: Cameron, Carl
Subject: CIA

I will go on the record. I am not turning back now…

From: Dennis [mailto:dennis@ncoder.net]
Sent: Thursday, August 29, 2013 10:21 AM
To: carl.cameron@foxnews.com
Subject: CIA

This is what the information is running on in my house. I would bring a film crew you may to film some of this…

From: Cameron, Carl [mailto:CARL.CAMERON@FOXNEWS.COM]
Sent: Thursday, August 29, 2013 10:15 AM
To: Dennis
Subject: Re: CIA

Will do. I arrive late Sunday and hope to see you Mon or Tues. I'll call tomorrow.

Carl Cameron, Chief Political Correspondent, Fox News, From Mobile, please excuse autocorrect errors.

From: Dennis
Sent: Thursday, August 29, 2013 12:49 PM
To: Cameron, Carl
Subject: CIA

Just email me when you know your plans.

Dennis Montgomery
dennis@ncoder.net
619.508.1964

dennismontgomery45@gmail.com

From: Dennis <dennis@ncoder.net>
Sent: Thursday, August 29, 2013 1:51 PM
To: carl.cameron@foxnews.com
Subject: CIA

The best place to stay near me is the Hyatt, Bellevue, a few miles from my house.
http://www.bellevue.hyatt.com/en/hotel/home.html

From: Cameron, Carl [mailto:CARL.CAMERON@FOXNEWS.COM]
Sent: Thursday, August 29, 2013 10:15 AM
To: Dennis
Subject: Re: CIA

Will do. I arrive late Sunday and hope to see you Mon or Tues. I'll call tomorrow.

Carl Cameron, Chief Political Correspondent, Fox News, From Mobile, please excuse autocorrect errors.

From: Dennis
Sent: Thursday, August 29, 2013 12:49 PM
To: Cameron, Carl
Subject: CIA

Just email me when you know your plans.

Dennis Montgomery
dennis@ncoder.net
619.508.1964

dennismontgomery45@gmail.com

From: Cameron, Carl <CARL.CAMERON@FOXNEWS.COM>
Sent: Monday, October 7, 2013 1:09 PM
To: 'Dennis'
Subject: RE: Morning

We have a bureau in Seattle and could arrange to send a crew out to shoot more material - - whaddya think?

dennismontgomery45@gmail.com

From: Cameron, Carl <CARL.CAMERON@FOXNEWS.COM>
Sent: Thursday, October 31, 2013 1:56 PM
To: Dennis
Subject: Re: CIA

I'd like to have a camera to you tomorrow after 3 your time. Can you do it? I think you should meet him before Tuesday. And shooting your updated demonstration and narrative is crucial now

Carl Cameron, Chief Political Correspondent, Fox News, From Mobile, please excuse autocorrect errors.

From: Dennis
Sent: Thursday, October 31, 2013 12:55 AM
To: Cameron, Carl
Subject: CIA

Look at new videos on www.blxware.net #5, #6

dennismontgomery45@gmail.com

From: Dennis <dennis@ncoder.net>
Sent: Thursday, October 31, 2013 2:09 PM
To: 'Cameron, Carl'
Subject: RE: CIA

I will be ready. I just want to make sure they will in Federal Court Tues also.

From: Cameron, Carl [mailto:CARL.CAMERON@FOXNEWS.COM]
Sent: Thursday, October 31, 2013 10:56 AM
To: Dennis
Subject: Re: CIA

I'd like to have a camera to you tomorrow after 3 your time. Can you do it? I think you should meet him before Tuesday. And shooting your updated demonstration and narrative is crucial now

Carl Cameron, Chief Political Correspondent, Fox News, From Mobile, please excuse autocorrect errors.

From: Dennis
Sent: Thursday, October 31, 2013 12:55 AM
To: Cameron, Carl
Subject: CIA

Look at new videos on www.blxware.net #5, #6

dennismontgomery45@gmail.com

From: Cameron, Carl <CARL.CAMERON@FOXNEWS.COM>
Sent: Thursday, September 26, 2013 1:52 AM
To: Dennis
Subject: Re: CIA

I can get the whole story out but need examples of the harvested data. You mention on tape the florida voter registration data, creditcard and bank records and personal passwords and log in data
For tens of millions ..all I need is a relatively small sample of each and I can do the whistle blower story and back it up without disclosing anyone's private info.

Carl Cameron, Chief Political Correspondent, Fox News, From Mobile, please excuse autocorrect errors.

From: Dennis
Sent: Wednesday, September 25, 2013 6:32 PM
To: Cameron, Carl
Subject: CIA

I am ok, thanks for your support. I am just amazed I can't get legal help in this matter. Everyone wants whistleblower to come forward, but few are willing to help. The bad press about me is making it hard to get legal representation to expose the crimes US Government officials have committed against American citizens. I guess the government's strategy of leaking false information to the press, to discredit me, really has worked.

When James Clapper lied under oath to Congress this year and gave the "the least untruthful answer possible" about document harvesting, he apologized and that was the end of it. James Clapper and John Brennan ran these "illegal" document harvesting programs that I was involved with from 2003 - 2010, and I will find a way to get the information out.

The value of this harvested data is worth tens of millions of dollars. I have never attempted to sell the data or exploit the data to benefit me or my family. I could have sold the data years ago for millions. No one would have known I had sold the data, and that would have been the end of the story.

I am fighting insurmountable odds and creating immense risk by going down the whistleblower complaint road. I am not only creating this risk for myself, but for my family also. I am trying to do this without violating the documents I have signed with the US Government or existing court orders preventing the release of certain information.

It is obvious to me that I need to get this whistleblower complaint process story out first to help repair some of the malice that has taken place by the US Government officials when they leaked this false information to the press about me.

I get I just need an attorney to protect me, and there must be one out there for me. I just hope that interview I did with you gets released while I am still alive. I suspect the US Government is deciding what to do with me, and my desire to expose James Clapper and John Brennan's involvement in these "harvesting" programs as we speak. They can't hide the HAMMER forever.

Dennis Montgomery
619.508.1964
dennis@ncoder.net

Frm: Cameron, Carl [mailto:CARL.CAMERON@FOXNEWS.COM]
Sent: Wednesday, September 25, 2013 12:20 PM
To: 'Dennis'
Subject: Hi Dennis

How did it go Monday at the hospital? Please let me know how you are doing when you are able, I'm rooting for you.

Carl Cameron
Chief Political Correspondent
FOX NEWS CHANNEL
202-320-2105

EXHIBIT “15”

PHOENIX New Times

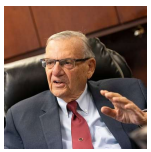
ARPAIO

Arpaio Pal Klayman Shot Down, DOJ Okayed, and More in Latest Sheriff Joe Contempt Hearing

STEPHEN LEMONS | AUGUST 12, 2015 | 9:15AM

A status conference in downtown Phoenix before federal Judge G. Murray Snow continued his court's inexorable march toward a second round of contempt hearings in the ACLU's big racial-profiling

LATEST STORIES



Joe Arpaio is Four Times a Loser

Where Does This Phoenix City Council Candidate Really Live?

And when Snow refused Arpaio's attorneys attempt to disqualify him from the case, what did Arpaio's legal team do? Play copycat to Klayman, **seeking a writ of mandamus from the Ninth**, which is currently pending.

In another development Tuesday, Snow allowed the DOJ to intervene in *Melendres*.

This means, essentially, that DOJ attorneys will work alongside lawyers from the ACLU and Covington & Burling on the case.

DOJ attorney Rafael Gomez was present to address **the 50 hard drives recently seized by the U.S. Marshals on order of the court**.

Gomez said that his "client entities" – presumably U.S. intelligence agencies such as the CIA – only wanted to review the one hard drive and two bankers boxes of material that had been made available to them previously; they then will decide what to do about the

additional 50 hard drives.

Gomez said he could not reveal who these "client entities" are, as that information may be classified pending a review of the material. He said his clients were concerned that by opening the 50 hard drives they could compromise the metadata on the files. He could not say how long it would take for a decision to be reached.

Snow seemed annoyed by this and advised Gomez that he was not going to wait for the U.S. government to make a decision before allowing the parties to examine the files.

Both Iafrate and ACLU attorney Cecillia Wang indicated that they wanted access to the 50 hard drives.

Snow ordered the parties to consult and hopefully agree to protocols in handling the material.

During the hearing, the judge tangled more than once

EXHIBIT “16”

EXECUTIVE SESSION

COMMITTEE ON THE JUDICIARY,

JOINT WITH THE

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT,

U.S. HOUSE OF REPRESENTATIVES,

WASHINGTON, D.C.

INTERVIEW OF: JAMES A. BAKER (DAY 2)

Thursday, October 18, 2018

Washington, D.C.

The interview in the above matter was held in Room 2141, Rayburn House Office Building, commencing at 10:01 a.m.

Present: Representatives Meadows, Jordan, Ratcliffe, and Gaetz.

here.

Mr. Breitenbach. Unlawful surveillance of whom?

Mr. Baker. Of Americans, including government officials. Yeah. I can go -- I mean --

Mr. Jordan. Who was his client?

Mr. Baker. Can I just -- I'm turning to the Bureau to describe this. So his client was an individual named Dennis Montgomery, who I believe, to the best of my recollection, he said that he had been a U.S. Government contractor and, in the course of that work, had come across evidence of unlawful surveillance by the government of Americans -- and including government officials -- and wanted to give that information to the Bureau, which eventually did take place.

Mr. Jordan. And was this -- I'm sorry. Go ahead.

Mr. Sommers. During what time period?

Mr. Jordan. Yeah. That's what I was going to ask.

Mr. Baker. To the best of my recollection, it's in the late summer, early fall 2016.

Mr. Sommers. And the surveillance, what time period was that?

Mr. Baker. I'm not entirely sure what the timeframe was. It was a significant -- it was -- one of the issues in the case was it was a large amount of data that he had that he wanted to provide, that these -- these disks or other media had a lot of data on them about this, allegedly.

Mr. Sommers. Surveillance by whom?

Mr. Baker. By the U.S. Government itself of Americans,

EXHIBIT “17”

From: Dickas, J (Intelligence)
To: Dennis (dennis@ncoder.net)
Subject: RE: CIA
Date: Thursday, September 18, 2014 5:18:50 PM

Hi Mr. Montgomery,

Apologies for the slow response, I was out of the office for a couple weeks. Based on my examination of your case, it looks to me like the Department of Defense Inspector General is actually best positioned to review your complaint that the work you performed for the government was illegal or improper. If you are having a hard time bringing this issue to the DoD IG's attention, I believe Sen. Cantwell's casework staff is in a good position to help you get in touch with them. Hope that is helpful.

John

From: Dennis [mailto:dennis@ncoder.net]
Sent: Thursday, September 18, 2014 3:49 PM
To: Dickas, J (Intelligence)
Cc: Wolfe, J (Intelligence)
Subject: CIA

Would you at least give me the courtesy of acknowledging my email. I have limited ways to communicate with you and your committee.

It has been over a year since you sent me this email below.

I have followed the proper channels to file my whistle blower complaints with the intelligence community. I have been told to be patient. You made it clear in you August 16, 2013 email that you would like to help me but cautioned me about releasing sensitive documents, which I have not done.

I am a American who has information regarding US government intelligence agencies mass surveillance of Americans, that you may not have been aware of. At this point, I will assume you have verified that I was working for companies that had contracts with the CIA, DOD,DNI, HOMELAND SECURITY, as well as others.

I thought at one point you and your committee would help me move my whistleblower complaints forward?

I have followed the rules you ask me to follow. I will cooperate fully with you other members of your committee regarding information that is contained in the various whistleblower complaints that I have filed with the Inspector General's within the intelligence community.

I am disabled, and have limited ways to communicate with you. I am trying to do the right thing.

Please help me.

Dennis Montgomery
dennis@ncoder.net
619.508.1964

From: Dickas, J (Intelligence) [j
Sent: Friday, August 16, 2013 12:51 PM
To: Dennis
Subject: RE: CIA

Hi Mr. Montgomery -

I would still recommend that you work with Senator Cantwell's casework staff to try to get a response from the CIA Inspector General regarding your complaint. Have you tried to contact Senator Cantwell's staff about this?

Also, you mentioned protections for whistleblower complaints - it is important to emphasize that such protections have generally not been interpreted to cover disclosures of classified information through improper channels. So I would strongly recommend that you not convey any classified information via any unclassified modes of communication, or to any staff that do not have the necessary security clearances. You seem to have been pretty careful not to do this so far, but some of your comments make me concerned that you may be considering violating classification rules in the course of your interactions with congressional staff, and many congressional staff (myself included) would feel compelled to report the violation if you did so. I would definitely like to be helpful in getting your concern addressed, but if you violate any laws regarding the protection of classified information I don't think anyone in the legislative branch will be able to help or protect you.

Let me know if you need any help getting back in touch with Senator Cantwell's office, and have a great weekend.

John

From: Dennis [dennis@ncoder.net]
Sent: 15 August 2013 00:29
To: Dickas, J (Intelligence)
Subject: CIA

This is not a complete list of individuals in Congress that had their personal data harvested. I just wanted to give you some idea how wide spread it was. I would hope the information I have provided to you and whoever you provide it to; is treated as information that being submitted as a whistleblower complaint, and protected accordingly. I continue to try to look for “Proper Channels” to go through in blowing the whistle on these illegal “document harvesting programs”, and the US Government officials that were involved in these programs. This work was nothing more than the US Government spying on US citizens, without their knowledge, consent or any court order.

I along with my family have been threatened, harassed, and when I wouldn’t agree to stop my effort to whistle blow on the US Intelligence community, discredited. It is not fair for the US Government to leak false information to the press in hopes of getting me to stop my whistle blowing campaign, and when I attempt to defend myself, hold me to the State Secrets Privilege.

It is important to remember it was the government who came to me to do the work, not me going to the government looking for work...

I am just one US citizen that is trying to get the truth out if the face of insurmountable obstacles.

I appreciate all of your help.
Dennis Montgomery
dennis@ncoder.net
619.508.1964

From: Dennis [mailto:dennis@ncoder.net]
Sent: Wednesday, August 14, 2013 8:48 PM
To: 'Dickas, J (Intelligence)'
Subject: CIA

John, In the years I was involved with these programs the following individuals had data harvested by the US Government, at least once. Over half this individuals have had their personal data harvested more than twice. As you can see, the program did not discriminate based on political party; 48 Democrats and 35 Republicans. Would you like me to provide more information? There are tens of millions of records that were harvested.

I am sure I have already violated this State Secrets Privilege by disclosing this information, even without disclosing what was actually harvested. Why wouldn't the **Inspector General of the DNI**, **Inspector General of the DOJ**, **Inspector General of the Air Force**, or the **Inspector General of the CIA** want to get to the bottom of these disclosures and let me file a whistleblower complaint? I suspect it has something to do with politics, James Clapper, John Brennan, and the other US Government officials that were involved in this "illegal" data gathering effort and what they actually used the data for.

How can the US Government classify this information as classified, secret, or top secret when these individuals obviously had nothing to do with terrorism, like the other 10 million US Citizens that had their personal information harvested, without their knowledge, consent, or court order under the disguise of "national security."

ADAM SMITH,CONGRESSMAN,D
ALCEE HASTINGS,CONGRESSMAN,D
BARBARA BOXER,SENATOR,D
BILL NELSON,SENATOR,D
BOB GOODLATTE,CONGRESSMAN,R
CARL LEVIN,SENATOR,D
CHARLES GRASSLEY,SENATOR,R
CHARLES SCHUMER,SENATOR,D
COLLIN PETERSON,CONGRESSMAN,D
DANNY DAVIS,CONGRESSMAN,D
DAVE CAMP,CONGRESSMAN,R
DAVID PRICE,CONGRESSMAN,D
DEREK KILMER,CONGRESSMAN,D
DIANNE FEINSTEIN,SENATOR,D
DONALD PAYNE,CONGRESSMAN,D

ED PASTOR,CONGRESSMAN,D
EDDIE JOHNSON,CONGRESSMAN,D
EDWARD MARKEY,CONGRESSMAN,D
ELIJAH CUMMINGS,CONGRESSMAN,D
FRANK LUCAS,CONGRESSMAN,R
FRANK PALLONE,CONGRESSMAN,D
FRED UPTON,CONGRESSMAN,R
GENE GREEN,CONGRESSMAN,D
HARRY REID,SENATOR,D
HENRY CUELLAR,CONGRESSMAN,D
HOWARD COBLE,CONGRESSMAN,R
JACK KINGSTON,CONGRESSMAN,R
JAMES CLYBURN,CONGRESSMAN,D
JAMES INHOFE,SENATOR,R
JEB HENSARLING,CONGRESSMAN,R
JEFF MILLER,CONGRESSMAN,R
JEFF SESSIONS,SENATOR,R
JIM COOPER,CONGRESSMAN,D
JOE BARTON,CONGRESSMAN,R
JOHN BOEHNER,CONGRESSMAN,R
JOHN BOOZMAN,SENATOR,R
JOHN CONYERS,CONGRESSMAN,D
JOHN DELANEY,CONGRESSMAN,D
JOHN DUNCAN,CONGRESSMAN,R
JOHN LEWIS,CONGRESSMAN,D
JOHN MCCAIN,SENATOR,R
JOSE SERRANO,CONGRESSMAN,D
KAY GRANGER,CONGRESSMAN,R
LAMAR ALEXANDER,SENATOR,R
LAMAR SMITH,CONGRESSMAN,R
LEE TERRY,CONGRESSMAN,R
LEONARD LANCE,CONGRESSMAN,R
LORETTA SANCHEZ,CONGRESSMAN,D
MARCO RUBIO,SENATOR,R
MARK KIRK,SENATOR,R
MARK SANFORD,CONGRESSMAN,R
MARSHA BLACKBURN,CONGRESSMAN,R
MAX BAUCUS,SENATOR,D
MELVIN WATT,CONGRESSMAN,D
MICHAEL MICHAUD,CONGRESSMAN,D
MICHAEL TURNER,CONGRESSMAN,R
MIKE THOMPSON,CONGRESSMAN,D
MITCH MCCONNELL,SENATOR,R
PAT ROBERTS,SENATOR,R
PATRICK LEAHY,SENATOR,D

PATTY MURRAY,SENATOR,D
PAUL RYAN,SENATOR,D
PETER DEFAZIO,CONGRESSMAN,D
RALPH HALL,CONGRESSMAN,R
RICHARD BURR,CONGRESSMAN,R
RICHARD DURBIN,SENATOR,D
RICK LARSEN,CONGRESSMAN,D
ROBERT ANDREWS,CONGRESSMAN,D
ROBERT MENENDEZ,SENATOR,D
RON WYDEN,SENATOR,D
ROSCOE BARTLETT,CONGRESSMAN,R
RUBEN HINOJOSA,CONGRESSMAN,D
SANDER LEVIN,CONGRESSMAN,D
SANFORD BISHOP,CONGRESSMAN,D
SAXBY CHAMBLISS,SENATOR,R
SHERROD BROWN,CONGRESSMAN,D
STEPHEN LYNCH,CONGRESSMAN,D
STEVE COHEN,CONGRESSMAN,D
SUSAN COLLINS,SENATOR,R
TIM RYAN,CONGRESSMAN,D
TOM COBURN,CONGRESSMAN,R
TOM HARKIN,SENATOR,D
TOM LATHAM,CONGRESSMAN,R

I appreciate all of your help.
Dennis Montgomery
dennis@ncoder.net
619.508.1964

From: Dickas, J (Intelligence) [mailto:J_Dickas@ssci.senate.gov]
Sent: Wednesday, August 14, 2013 10:57 AM
To: Dennis
Subject: RE: CIA

Hi Mr. Montgomery -

I would definitely not recommend simply disclosing classified information publicly. If you believe that the work that the CIA contracted you to do was illegal or improper, I would encourage you to keep trying to bring it to the attention of the CIA Inspector General. The CIA IG actually has a fairly good track record of investigating issues like this, and unlike the other Inspectors General that you have previously contacted, the the CIA IG is well positioned to look into the matter.

If you have not yet received a response from the CIA IG, I would recommend contacting Senator Cantwell's caseworker and asking for assistance. Congressional caseworkers are generally quite good at getting government agencies to respond to constituent inquiries and concerns. And if you need any help getting in touch with a caseworker, let me know and I'd be happy to help facilitate with Sen. Cantwell's office.

John Dickas

From: Dennis [dennis@ncoder.net]
Sent: 14 August 2013 11:00
To: Dickas, J (Intelligence)
Subject: CIA

I have to been unsuccessful with moving my whistleblower case forward within the US government. I have been rejected by the Office of Special Counsel, the Inspector General of the DNI, and the Inspector General of the DOJ. I provided my whistleblower complaint to the Inspector General of the CIA, but have not heard back from them. I have sent faxes to them, asking them to just confirm they have received my information. Still no response from Inspector General of the CIA.

I appreciate you dialog regarding the whistleblowers laws "currently in place as being inadequate." It seems like my only option now, is to release the information to the public, and let the public investigate for themselves what has really gone on. This would expose both the inadequate whistleblower laws regarding the intelligence community, the vast amount of data that was actually harvested, and the US government officials that created, supervised, and abused the programs under "the disguise" of national security or the "patriot act."

The State Secrets Privilege was issued against me to "hide crimes" committed by former US Government officials that worked on these information gathering programs. These programs are now controlled by individuals that are currently in the highest government offices in our country today. These programs gathered tens of millions of records of personal information that had absolutely nothing to do with "national security", without any court oversight. No one was exempt from these "covert programs" including some of the members of the current congress; Ron Wyden, John Boehner, Harry Reid, and many others.

According to current administration officials, Snowden did follow the correct protocol for whistleblowing on US Government officials or "illegal data harvesting programs" within the intelligence community. Given what I have gone through for the last 6 years, I doubt it would have made much difference. There are no whistleblowing laws within the US Government intelligence community, and the journey I have gone through only proves that.

I appreciate all of your help.
Dennis Montgomery
dennis@ncoder.net
619.508.1964

From: Dennis [mailto:dennis@ncoder.net]
Sent: Tuesday, August 13, 2013 3:20 PM
To: 'Dickas, J (Intelligence)'
Subject: CIA

The rejection of the whistleblower complaint rejection by the Inspector General Director of the DNI doesn't make since to me.

All of the work that was done from 2008-2010 was done under secrecy at Fort Washington, MD, and James Clapper. The program there was "document harvesting" information from millions of US Citizens personal information. As I reported to you before, when I was working there, I saw employees from CIA that I had worked with years earlier.

The work that was done at Fort Washington was under an Air Force and DNI contract. Given the fact that James Clapper is the head of the DNI, and the work that was done at Fort Washington was under his direct control, how could the Inspector General of the DNI, claim it is not under his purview to investigate?

I have also included the rejection letter by the Office of Special Counsel. That office suggested I contact my senators or congressman for help. Which I have done.

I have tried to go through the necessary steps to file my whistleblower complaint against US government programs and officials with the correct US government agency. It has become obvious to me, that US government individuals involved in these programs, don't want these investigations to move.

Dennis Montgomery
dennis@ncoder.net
619.508.1964

From: Dickas, J (Intelligence) [mailto:J_Dickas@ssci.senate.gov]
Sent: Tuesday, August 13, 2013 2:35 PM
To: Dennis
Subject: RE: CIA

Mr. Montgomery -

I definitely agree that the intelligence whistleblower laws currently in place are inadequate. I do think that the IG that is best positioned to address your concern that your work for the CIA was illegal and/or improper is the CIA IG. If the CIA IG has not responded to your attempts to communicate with them, Senator Cantwell's casework staff might be able to help you get in touch with them.

John

From: Dennis [dennis@ncoder.net]
Sent: 13 August 2013 16:52
To: Dickas, J (Intelligence)
Subject: CIA

I filed a whistleblower complaint with the Inspector General of the DOJ, and sent a copy of it to the Attorney General Eric Holder and the Deputy Attorney General, James Cole. The whistleblower complaint was against the two DOJ attorneys and the FBI Special Agent that were involved in the illegal raid on my home and property. I just received a rejection letter by the Inspector General of the DOJ, who referred it to the FBI. This is the same FBI that the judge has already ruled had

already violated my 4th Amendment rights in the first place.

The DOJ doesn't want me to provide them information regarding the illegal document harvesting programs that were run by the intelligence community, against American citizens in this country. They are hiding behind the State Secrets Privilege to "conceal the crimes" and the government officials that were involved in these programs.

The Inspector General of the DNI has also refused to investigate my whistleblower against James Clapper and the DNI. They had determined it was not under their purview.

It doesn't seem like a whistleblower process really exists in this country when it comes to the intelligence community.

Dennis Montgomery
619.508.1964

From: Dickas, J (Intelligence) [mailto:J_Dickas@ssci.senate.gov]
Sent: Tuesday, August 13, 2013 10:35 AM
To: Dennis
Subject: RE: CIA

Hi Mr. Montgomery,

If the CIA IG has not confirmed receipt of the information that you sent, the easiest thing to do might be to have the caseworker from Sen. Cantwell's office contact them and ask them to confirm receipt of the materials. If you need help getting in touch with them, just let me know.

John

From: Dennis [dennis@ncoder.net]
Sent: 12 August 2013 11:51
To: Dickas, J (Intelligence)
Subject: CIA

John,

I have no way know if the information I sent to the Inspector General of the CIA on 8/6/13 was received. I have asked for some kind of confirmation from the Inspector General of the CIA that my information was received by his office.

Dennis Montgomery
dennis@ncoder.net
619.508.1964

EXHIBIT “18”

IN THE UNITED STATES TAX COURT

In the Matter of:	)	
	)	
DENNIS L. MONTGOMERY & BRENDA K. MONTGOMERY,	)	
	)	
Petitioner,	)	
	)	
v.	)	Docket No: 9008-09
	)	
COMMISSIONER OF INTERNAL REVENUE,	)	
	)	
Respondent.	)	

Pages: 1 through 47

Place: Los Angeles, California

Date: February 23, 2015

resolved? My legal bill in 2007, Your Honor, was over a million five.

So I just want to resolve 2006, and I think the easiest resolution, Your Honor, is simply give me my deduction.

THE COURT: You may be right, and who knows, maybe Mr. Corry in the next two months will look at it and conclude that you're right -- maybe.

MR. CORRY: Your Honor, if I may?

THE COURT: Yes.

MR. CORRY: He is living in Washington now. I don't know if you want to ask Petitioner if he would --

MR. MONTGOMERY: I don't want to change people now, Your Honor.

MR. CORRY: I just wanted to give him the opportunity.

MR. MONTGOMERY: I'd rather him stay on this attempt to resolve things.

THE COURT: Okay. It is a very old case, but you're right, a trial might have to have a change in place of trial, were that to become necessary.

MR. CORRY: And, Your Honor, maybe to move forward, if Petitioner would like to go on the record and describe his gambling losses, because gambling

income is one of the issues. If he would like to go on the record and say how many --

THE COURT: Oh, for '05 and '06?

MR. CORRY: For '05 and '06. If he would like to go on the record and say an estimate of how much he believes that he lost because of gambling activities in 2005 and 2006.

THE COURT: That's completely unrelated to national security, so if you have records of your gambling losses for those years -- do you have records of gambling losses?

MR. MONTGOMERY: No, but I can get them. But how much was the gambling loss?

MR. CORRY: The gambling income for 2005 -- the adjustment on those in the deficiency was $1,400.

THE COURT: You see, that's the kind of thing you almost surely have gambling losses in excess of that.

MR. CORRY: Yes, Your Honor.

MR. MONTGOMERY: How much was it, Your Honor?

THE COURT: It was less than 2,000.

MR. CORRY: $1,400 in 2005, and in 2006 it was $43,000.

THE COURT: So you probably have losses

that exceed that. Right?

MR. MONTGOMERY: Do you see the irony, Your Honor? He's fighting me over whatever the amount is, let's say $40,000, and I spent a million dollars defending myself.

THE COURT: No. I understand. He's quite logically making the point, let's try to resolve these minor issues at least, and that sounds like the minor issue that the men in black would not have come after you to seize records about.

MR. MONTGOMERY: Well, I took a gamble on my life. The biggest gamble I ever took was working for the United States intelligence agencies.

And I want to go on the record one last time -- and yes, Your Honor, I will provide you what you've asked me to provide you in a letter -- but I want to go on the record one last time stating I did work for projects under the direction of John Brannen and James Clapper.

John Brannen at the time was not the head of the CAI which he is the head of the CIA now, and James Clapper was the head of the DNI, and at the time I worked for him was in charge of work being done at Fort Washington, Maryland.

These projects that I worked for the

government on illegally data mined U.S. Americans and their businesses without any FISA court order, search warrant or the knowledge or consent of the people that were doing the work.

THE COURT: Depending on the data mining involved, maybe they did need it and maybe they didn't. But I'm just here to figure out how much in tax, if anything, you owe for '05 and '06.

MR. MONTGOMERY: Your Honor, I'm sorry; I didn't mean to interrupt you.

THE COURT: Go ahead.

MR. MONTGOMERY: I filed a whistleblower complaint with the inspector general of the IRS outlining these things too where I was trying to be a whistleblower and provide the inspector general of exactly what happened to me as an American has happened to a lot of other people as an American, and I submitted that whistleblower complaint.

I also filed a whistleblower complaint with the inspector general of the CIA, the inspector general of the Department of Defense, the inspector general of the DOJ.

THE COURT: If you get income from any of that, it's probably taxable.

MR. MONTGOMERY: Yes. I got a reply saying

EXHIBIT “19”

U.S. Department of Justice

Vincent H. Cohen, Jr.
Acting United States Attorney

District of Columbia

Judiciary Center
555 Fourth St., N.W.
Washington, D.C. 20530

July 28, 2015

Re: In re Investigation of Possible Violations of 50 U.S.C. § 1809

Dear Counsel:

As you are aware, your client, Dennis Montgomery, has indicated that he possesses physical evidence of possible violations of 50 U.S.C. § 1809 in the form of documents, written material, electronic media and/or other physical items, to include any codes necessary to access such items (collectively referred to hereinafter as the "Physical Evidence"), which your client acquired in connection with his previous employment with the United States government. I understand that your client is interested in voluntarily producing the Physical Evidence to members of law enforcement and representatives of this Office for evaluation.

In order to assure that there are no misunderstandings concerning the terms under which your client's production of the Physical Evidence would occur:

(1) First, except as provided for in paragraphs two and three below, the act of production by your client would not be used against your client to establish either that (a) the Physical Evidence was in his possession or control or (b) the Physical Evidence is authentic.

(2) Second, the Government may make any use whatsoever of the Physical Evidence produced by your client pursuant to this agreement, provided that an evidentiary foundation other than your client's production of such items can be established.

(3) Third, in the event your client is ever a witness or presents evidence through other witnesses, at trial or any other proceeding, and your client's statements or that evidence contradicts that the Physical Evidence (a) existed, (b) was in his possession, custody, or control, or (c) was authentic, the attorney or agent for the Government may cross-examine your client and other witnesses concerning the act of production by your client. Evidence regarding the act of production may also be introduced in rebuttal at any trial. (This provision is intended to assure that your client does not abuse the opportunity for a voluntary production, does not make materially false statements to a government agency or fact finder, and does not commit perjury or otherwise provide materially false information at a trial or any other proceeding.)

(4) Fourth, it is understood and agreed to by your client and the United States that this agreement does not constitute a plea bargaining session. However, if this agreement is subsequently construed to be a plea bargaining session, your client knowingly and voluntarily

waives or gives up any rights he has pursuant to Rule 410 of the Federal Rules of Evidence and Rule 11(f) of the Federal Rules of Criminal Procedure.

(5) Finally, this agreement does not obligate the United States Attorney's Office for the District of Columbia to take any action or refrain from taking any action not described in this letter. In addition, your client understands that this Office has made no additional promises to your client not contained in writing herein.

I trust that you will find this offer fair and reasonable. If your client wishes to engage in a voluntary act of production under these ground rules, you and your client should both sign this letter where indicated below.

Sincerely yours,

VINCENT H. COHEN, JR.
UNITED STATES ATTORNEY

By: _____
DEBORAH A. CURTIS
Assistant United States Attorney

ACKNOWLEDGMENT

I have read every word of this agreement, and its meaning has been fully explained to me by my attorney. After consultation with my attorney, I understand and agree to the contents of this letter.

7/28/15
Date

Dennis Montgomery

ATTORNEY'S ACKNOWLEDGMENT

I acknowledge that I have read each page of this agreement, reviewed it in its entirety with my client, and discussed fully with my client each of the provisions of the agreement.

7/28/15
Date

_____
Attorney for Dennis Montgomery

FD-597 (Rev 8-11-94) Page 1 of 2

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 8/19/2015

item(s) listed below were:
- [x] Received From
- [ ] Returned To
- [ ] Released To
- [ ] Seized

(Name) DENNIS MONTGOMERY

(Street Address) _____

(City) MINIMAN FL

Description of Item(s):

(2) HD LABELLED DRIVE 49 2005 ALL
(1) HD LABELLED DRIVE 41 2008 BLX. OPS
(1) " " 43 2010 ETN VAULT
(1) " " 47 2008 DMT. SRC
(1) " " 39 2008 BLX. BIOMETRICS
(1) " " 32 BLX. CIA 2012
(1) " " 35 ETN. CIA OUTPUT
(1) " " DISK 31 BLX. RECORDER
(1) " " 40 2008 BLX. OPS
(1) " " DISK 24 ETN. SRC
(1) " " DISK 25 ETN. ALL
(1) " " DRIVE 48 2005 ETN. ADMIN
(1) " " DISK 33 BLX. BLX SRC
(1) " " DRIVE 37 2008 BLX. TEMP.X
(1) " " DISK 22 2004 ETN. COVA
(1) " " DRIVE 34 2008 BLX. SRC
(1) " " DRIVE 42 2010 DMT
(1) " " DISK 07 VIDEO
(1) SHEET OF PAPER "MONTGOMERY DISK DRIVES"
(1) " " DRIVE 36 2008 BLX. ADMIN
(1) " " DISK 23 2004 ETN. COVA
(1) " " DRIVE 43 2008 ETN. WIP
(1) " " DRIVE 44 2010 DMT VAULT
(1) " " DISK 05 VIDEO

Received By: _____ (Signature)

Received From: Dennis Montgomery (Signature)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) August 19, 2015

item(s) listed below were:
- [x] Received From
- [ ] Returned To
- [ ] Released To
- [ ] Seized

(Name) Dennis Montgomery

(Street Address) _____

(City) Miramar, FL.

Description of Item(s): (1) HD labeled Disk #4 Video - 2TB green
(1) HD labeled Disk 11 2009 Jory
(1) HD labeled Disk 8 Video - green label
(1) HD labeled Disk 19 2004 ETR. RND
(1) HD labeled Disk 30 BLX. LIVE
(1) HD labeled Disk #2.. VIDEO green label
(1) HD labeled Disk 03 VIDEO green label
(1) HD labeled Disk 09 VIDEO green label
(1) HD labeled Disk 18 2005 ETR. RND
(1) HD labeled Disk 26 ETR. DRONE
(1) HD labeled Disk 29 BLX. SRC
(1) HD labeled Disk 13 2007 Sandoval
(1) HD labeled Disk #1.. video green label
(1) HD labeled Disk 16 2005 ETR. WIP green label
(1) HD labeled Disk 06 video - green label
(1) HD labeled Disk 12 2009 Jory
(1) HD labeled Disk 27 BLX. TB
(1) HD labeled Disk 17 2004 ETR. WIP
(1) HD labeled Disk 10 video green label
(1) HD labeled Disk 20 2005 ETR. FACE
(1) HD Disk 29 BLX. LIVE
(1) HD Disk 15 2005 ETR. WIP
(1) HD Disk 14 2006 ETREPID WIP

Received By: _____ (Signature)

Received From: D Montgomery (Signature)

U.S. Department of Justice

Ronald C. Machen Jr.
United States Attorney

District of Columbia

Judiciary Center
555 Fourth St., N.W.
Washington, D.C. 20530

November 24, 2015

Larry Klayman, Esq.

Re: In re Investigation of Possible Violations of 50 U.S.C. § 1809

Dear Counsel:

As you are aware, your client, Dennis Montgomery, has indicated that he possesses evidence of possible violations of 50 U.S.C. § 1809, the Foreign Intelligence Surveillance Act. I understand that in support of these allegations, in addition to providing physical evidence, your client is interested in meeting with members of law enforcement for a voluntary, "off-the-record" debriefing.

In order to assure that there are no misunderstandings concerning the meaning of "off-the-record," I am writing to clarify the ground rules of this and any subsequent voluntary "off-the-record" debriefing(s) with your client.

(1) First, except as provided for in paragraphs two and three below, no statements made by or other information provided by you during the voluntary "off-the-record" debriefing(s) will be used directly against your client in any criminal proceeding, other than a prosecution for perjury, giving a false statement, or obstruction of justice.

(2) Second, the Government may make derivative use of and may pursue any investigative leads suggested by any statements made by, or other information provided by, your client. (Because any statements made during this "off-the-record" debriefing are voluntarily made on the part of your client, rather than compelled, it is the government's position that Kastigar protections do not apply. Nevertheless, your client understands that based on the terms of this agreement there will be no Kastigar hearing at which the government would have to prove that the evidence it would introduce at trial is not tainted by any statements made by or other information provided by your client.)

(3) Third, in the event your client is ever a witness or presents evidence through other witnesses, at a trial or any other proceeding, and your client's statements or that evidence contradicts statements made in your debriefing, the attorney or agent for the Government may

cross-examine your client and other witnesses concerning any statements made or other information provided by your client during the "off-the-record" debriefing(s). Evidence regarding such statements may also be introduced in rebuttal. (This provision is to assure that your client does not abuse the opportunity for a voluntary "off-the-record" debriefing(s), does not make material false statements to a government agency or fact finder, and does not commit perjury or otherwise provide materially false information at a trial or other proceeding, examples of which include, but are not limited to, sentencing hearings, parole hearings, and hearings on revocation of probation or supervised release).

(4) Finally, this debriefing agreement does not obligate the United States Attorney's Office for the District of Columbia to file any motion regarding cooperation provided by your client. In addition, your client understands that this office has made no additional promises to your client not contained in writing herein.

I trust that you will find these ground rules fair and reasonable. If your client wishes to engage in a voluntary "off-the-record" debriefing under these ground rules, would you and your client both sign this letter where indicated below. Once signed, please return the original to me and retain a copy for your files.

Sincerely yours,

CHANNING D. PHILLIPS
UNITED STATES ATTORNEY

BY: _____ 12/3/15
Deborah A. Curtis
Assistant United States Attorney

I have read every word of this debriefing agreement, and its meaning has been fully explained to me by my attorney. After consultation with my attorney, I understand and agree to the contents of this letter.

11-30-15
Date

Dennis Montgomery

ATTORNEY'S ACKNOWLEDGMENT

I acknowledge that I have read each page of this debriefing agreement, reviewed it in its entirety with my client, and discussed fully with my client each of the provisions of the agreement.

12/3/15
Date

Larry Klayman
Attorney for Dennis Montgomery

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 12/3/2015

item(s) listed below were:
- [x] Received From
- [ ] Returned To
- [ ] Released To
- [ ] Seized

(Name) DENNIS MONTGOMERY

(Street Address) 3812 94th Ave NE

(City) BELLEVUE WA 98004

Description of Item(s): (1) ATIVA 4GB THUMB DRIVE

Received By: _____ (Signature) **Received From:** _____ (Signature)

U.S. Department of Justice

Vincent H. Cohen, Jr.
Acting United States Attorney

District of Columbia

Judiciary Center
555 Fourth St., N.W.
Washington, D.C. 20530

July 28, 2015

Re: In re Investigation of Possible Violations of 50 U.S.C. § 1809

Dear Counsel:

As you are aware, your client, Dennis Montgomery, has indicated that he possesses physical evidence of possible violations of 50 U.S.C. § 1809 in the form of documents, written material, electronic media and/or other physical items, to include any codes necessary to access such items (collectively referred to hereinafter as the "Physical Evidence"), which your client acquired in connection with his previous employment with the United States government. I understand that your client is interested in voluntarily producing the Physical Evidence to members of law enforcement and representatives of this Office for evaluation.

In order to assure that there are no misunderstandings concerning the terms under which your client's production of the Physical Evidence would occur:

(1) First, except as provided for in paragraphs two and three below, the act of production by your client would not be used against your client to establish either that (a) the Physical Evidence was in his possession or control or (b) the Physical Evidence is authentic.

(2) Second, the Government may make any use whatsoever of the Physical Evidence produced by your client pursuant to this agreement, provided that an evidentiary foundation other than your client's production of such items can be established.

(3) Third, in the event your client is ever a witness or presents evidence through other witnesses, at trial or any other proceeding, and your client's statements or that evidence contradicts that the Physical Evidence (a) existed, (b) was in his possession, custody, or control, or (c) was authentic, the attorney or agent for the Government may cross-examine your client and other witnesses concerning the act of production by your client. Evidence regarding the act of production may also be introduced in rebuttal at any trial. (This provision is intended to assure that your client does not abuse the opportunity for a voluntary production, does not make materially false statements to a government agency or fact finder, and does not commit perjury or otherwise provide materially false information at a trial or any other proceeding.)

(4) Fourth, it is understood and agreed to by your client and the United States that this agreement does not constitute a plea bargaining session. However, if this agreement is subsequently construed to be a plea bargaining session, your client knowingly and voluntarily

waives or gives up any rights he has pursuant to Rule 410 of the Federal Rules of Evidence and Rule 11(f) of the Federal Rules of Criminal Procedure.

(5) Finally, this agreement does not obligate the United States Attorney's Office for the District of Columbia to take any action or refrain from taking any action not described in this letter. In addition, your client understands that this Office has made no additional promises to your client not contained in writing herein.

I trust that you will find this offer fair and reasonable. If your client wishes to engage in a voluntary act of production under these ground rules, you and your client should both sign this letter where indicated below.

Sincerely yours,

VINCENT H. COHEN, JR.
UNITED STATES ATTORNEY

By: _____
DEBORAH A. CURTIS
Assistant United States Attorney

ACKNOWLEDGMENT

I have read every word of this agreement, and its meaning has been fully explained to me by my attorney. After consultation with my attorney, I understand and agree to the contents of this letter.

7/28/15
Date

Dennis Montgomery

ATTORNEY'S ACKNOWLEDGMENT

I acknowledge that I have read each page of this agreement, reviewed it in its entirety with my client, and discussed fully with my client each of the provisions of the agreement.

7/28/15
Date

_____
Attorney for Dennis Montgomery

EXHIBIT “20”

---------- Forwarded message ----------
From: "Curtis, Deborah (USADC)" <Deborah.Curtis@usdoj.gov>
Date: Nov 24, 2015 7:24 AM
Subject: Meeting
To: "Larry Klayman" <leklayman@gmail.com>, "Dina James" <daj142182@gmail.com>
Cc: "Giardina, Walter B. (WF) (FBI)" <Walter.Giardina@ic.fbi.gov>, "Barnett, William J. (WF) (FBI)" <William.Barnett@ic.fbi.gov>

Dear Mr. Klayman,

The FBI looks forward to meeting with you and Mr. Montgomery on December 3, 2015 at 1030 am<x-apple-data-detectors://6> at the Washington Field Office.

As I indicated in our recent telephonic discussion, in furtherance of this investigation, the FBI requests the following information from your client:

-tax returns for the past ten years showing reported income and source of income

-bank statements for the past 10 years to the present showing deposits or reimbursements from Other Government Agency of the Intelligence Community ("OGA") or OGA associated entities

-any contracts between Dennis Montgomery ("DM") or DM related companies and OGA or OGA associated entities

-any orders, memoranda, taskings, or communications in any form from OGA, OGA associated entities, or government officials for the past 10 years to the present (this can exclude the many letters DM has submitted to Inspector Generals and members of Congress)

-email records between DM and OGA or government officials from 2005 to the present

-phone numbers for OGA individuals or government officials DM worked with from 2005 to the present (phone records as well if he possesses)

-address and supporting records (bills, leases, voter registration, etc) where DM lived while working at Ft. Washington, Maryland
---
These materials will be treated as falling within the scope of our existing production immunity agreement.

Further, in order allow for more direct discussions between FBI and your client, my office may be in a position to now offer a standard letter immunity agreement for purposes of this meeting. I will follow up with you later today or tomorrow on that issue.

Please let me know if you have any questions.

Deborah
DEBORAH A. CURTIS
Assistant U.S. Attorney