AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT,
ARREST WARRANT, AND SEARCH WARRANTS

I, Stephen A. McCoy, being duly sworn, hereby state the following under penalty of perjury:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed for approximately 20 years. I am currently assigned to the Washington Field Office to a squad responsible for counter-intelligence relating to Cuba. I have worked in the counter-intelligence field for approximately 15 years and have worked specifically on counter-intelligence matters involving Cuba for the last 12 years. As a result of my experience in counter-intelligence investigations and foreign counter-intelligence training, I am familiar with the strategy, tactics, methods, tradecraft and techniques of the Cuban foreign intelligence service and its agents.

2. This affidavit is submitted in support of an application for a complaint and arrest warrant charging ANA BELEN MONTES with conspiracy to commit espionage, in violation of 18 U.S.C. § 794(c), and for applications for four (4) search warrants to search the following items and locations:

(1) the residence of ANA BELEN MONTES, such premises known and described as a cooperative apartment located at 3039 Macomb Street, N.W., apartment 20, Washington, D.C. 20008, and further described in Attachment A to this affidavit;

(2) a red 2000 Toyota Echo, bearing vehicle identification number JTDT1231Y0007841 and District of Columbia license plate number 993 190, which is registered to ANA BELEN MONTES and anticipated to be within the District of Columbia;

(3) room C6-146A, 200 MacDill Boulevard, Washington, D.C. 20340, which is the office/work space assigned to ANA BELEN MONTES at the Defense Intelligence Analysis Center located on Bolling Air Force Base;

(4) safe deposit box #526 leased by ANA BELEN MONTES at Riggs Bank, N.A., Friendship Branch, 4249 Wisconsin Avenue, N.W., Washington, D.C.

3. Information in this affidavit is based on my personal knowledge and on information provided to me by other counter-intelligence investigators and law enforcement officers during the course of this investigation. Searches and various forms of surveillance have been conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (FISA) and orders of the Foreign Intelligence Surveillance Court (FISC).

I. Background

4. ANA BELEN MONTES is a United States citizen born on February 28, 1957, on a U.S. military installation in Nurnberg, Germany. She graduated from the University of Virginia in 1979 and obtained a masters degree from the Johns Hopkins University School of Advanced International Studies in 1988. She is single and lives alone at 3039 Macomb Street, N.W., apartment 20, Washington, D.C. 20008, which residence is further described in Attachment A. She has registered in her name a red 2000 Toyota Echo, bearing vehicle identification number JTDT1231Y0007841 and District of Columbia license plate number 993 190, which is regularly parked in the vicinity of her residence, and which she regularly uses to commute to her place of employment.

5. MONTES is currently employed by the Defense Intelligence Agency (DIA) as a senior intelligence analyst. Her current office is at 200 MacDill Boulevard, located on Bolling Air Force Base, Washington, D.C. 20340. Her assigned office space is C6-146A. She has been employed by DIA as an analyst since September 1985. Since 1992, she has specialized in Cuba matters. She is currently the senior analyst responsible for matters pertaining to Cuba. During the course of her

employment, MONTES has had direct and authorized access to classified information relating to the national defense.

6. Records obtained from Riggs Bank reveal that MONTES has continually leased safe deposit box number 526 at Riggs Bank, N.A., Friendship Branch, 4249 Wisconsin Avenue, N.W., Washington, D.C. since September 2, 1993.

7. Classified information is defined by Executive Order No. 12,958, 60 Fed. Reg.19,825 (1995), as follows: information in any form that (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in section 1.5 of the order (including intelligence sources and methods, cryptology, military plans, and vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security), and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Under the executive order, the designation "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. The designation "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. The designation "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

8. In addition, Executive Order No. 12,958 provides that the secretaries of State, Defense and Energy are authorized to create "special access programs" upon certain specific findings including that the vulnerability of, or threat to, specific classified information is exceptional. Under such a

program, the safeguarding and access requirements to information covered by the program exceed those normally required for information at the same classification level.

9. Under 32 C.F.R. § 159a.9, Sensitive Compartmented Information (SCI) refers to information and material that requires special controls for restricted handling.

10. During her employment at DIA, MONTES has continuously held a security clearance and has had regular, authorized access to classified information. I know that a person who receives such clearances is required to be briefed on the procedures for properly handling classified information and the penalties for failing to do so, and that such a person must sign certifications of understanding and agreement in connection with those briefings. I have reviewed a "Classified Information Nondisclosure Agreement" (Standard Form 189) that MONTES signed on September 30, 1985. In that document MONTES acknowledged that she was aware that unauthorized disclosure of classified information could cause irreparable injury to the United States or could be used to advantage by a foreign nation, that she would never divulge such information to an unauthorized person, and that she understood that she was obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information, and that she further understood such a disclosure could constitute a violation of United States criminal law including 18 U.S.C. § 794. I have also reviewed a "Security Briefing/Debriefing Acknowledgment" form signed by MONTES on May 15, 1997, briefing her into a Special Access Program (SAP). On this date, specifically in connection with this SAP, MONTES signed a Sensitive Compartmented Information Nondisclosure Agreement, in which she acknowledged that the unauthorized disclosure of SCI may violate federal criminal law, including 18 U.S.C. § 794, and that such disclosure could cause irreparable injury to the United States or be used to the advantage of a foreign nation.

II. MONTES's Toshiba Laptop Computer and Shortwave Radio

A. Communication From the Cuban Intelligence Service (CuIS) to MONTES via Shortwave Radio

11. Based on my knowledge and familiarity with the methodology of the Cuban intelligence service, I am aware that the CuIS often communicates with clandestine CuIS agents operating outside Cuba by broadcasting encrypted messages at certain high frequencies. Under this method, the CuIS broadcasts on a particular frequency a series of numbers. The clandestine agent, monitoring the message on a shortwave radio, keys in the numbers onto a computer and then uses a diskette containing a decryption program to convert the seemingly random series of numbers into Spanish-language text. This was the methodology employed by some of the defendants convicted last June in the Southern District of Florida of espionage on behalf of Cuba and acting as unregistered agents of Cuba, in the case of United States of America v. Gerardo Hernandez, et al., Cr. No. 98-721-CR-Lenard(s)(s). Although it is very difficult to decrypt a message without access to the relevant decryption program, once decrypted on the agent's computer the decrypted message resides on the computer's hard drive unless the agent takes careful steps to cleanse the hard drive of the message. Simply "deleting" the file is not sufficient.

12. Based on the evidence described below, I have concluded that MONTES was a clandestine CuIS agent who communicated with her handling CuIS officer in the manner described above.

13. A receipt obtained from a CompUSA store located in Alexandria, Virginia indicated that on October 5, 1996, one "Ana B. Montes" purchased a refurbished Toshiba laptop computer, model 405CS, serial number 10568512.

14. During a court-authorized surreptitious entry into MONTES's residence, conducted by the FBI on May 25, 2001, FBI agents observed in her residence a Toshiba laptop computer with the serial number set out above. During the search, the agents electronically copied the laptop's hard drive. During subsequent analysis of the copied hard drive, the FBI recovered substantial text that had been deleted from the laptop's hard drive.

15. The recovered text from the laptop's hard drive included significant portions of a Spanish-language message, which when printed out with standard font comes to approximately 11 pages of text. The recovered portion of the message does not expressly indicate when it was composed. However, it instructs the message recipient to travel to "the Friendship Heights station" on "Saturday, November 23rd." My review of a calendar indicates that November 23 fell on a Saturday in 1996; the next time thereafter November 23 falls on a Saturday is in 2002. Accordingly, this message was composed sometime before November 23, 1996, and entered onto MONTES's laptop sometime after October 5, 1996, the date she purchased it. Based on its content, I have concluded that it is a message from a CuIS officer to MONTES.

16. Portions of the recovered message included the following: "You should go to the WIPE program and destroy that file according to the steps which we discussed during the contact. This is a basic step to take every time you receive a radio message or some disk."

17. During this same search, the agents also observed a Sony shortwave radio stored in a previously opened box on the floor of the bedroom. The agents turned on the radio to confirm that it was operable. Also found was an earpiece that could be utilized with this shortwave radio, allowing the radio to be listened to more privately. Similar earpieces were found in the residences of the defendants in the Hernandez case, as described above in paragraph 11.

18. The recovered portion of the message begins with the following passage:

> Nevertheless, I learned that you entered the code communicating that you were having problems with radio reception. The code alone covers a lot, meaning that we do not know specifically what types of difficulty you are having. Given that it's only been a few days since we began the use of new systems, let's not rule out that the problem might be related to them. In that case, I'm going to repeat the necessary steps to take in order to retrieve a message.

The message then describes how the person reading the message should "write the information you send to us and the numbers of the radio messages which you receive." The message later refers to going "to a new line when you get to the group 10 of the numbers that you receive via radio," and still later gives as an "example" a series of groups of numbers: "22333 44444 77645 77647 90909 13425 76490 78399 7865498534." After some further instruction, the message states: "Here the program deciphers the message and it retrieves the text onto the screen, asking you if the text is okay or not." Near the conclusion of the message, there is the statement "In this shipment you will receive the following disks: . . . 2) Disk "R1" to decipher our mailings and radio."

19. Further analysis of MONTES's copied Toshiba hard drive identified text consisting of a series of 150 5-number groups. The text begins, "30107 24624," and continues until 150 such groups are listed. The FBI has determined that the precise same numbers, in the precise same order, were broadcast on February 6, 1999, at AM frequency 7887 kHz, by a woman speaking Spanish, who introduced the broadcast with the words "Attencion! Attencion!" The frequency used in that February 1999 broadcast is within the frequency range of the shortwave radio observed in MONTES's residence on May 25, 2001.

B. Communication Between the CuIS and MONTES via Computer Diskette

20. Based on my knowledge of the methodology employed by the CuIS, I am aware that a clandestine CuIS agent often communicates with his or her handling CuIS officer by typing a message onto a computer, and then encrypting and saving it to a diskette. The agent thereafter physically delivers the diskette, either directly or indirectly, to the officer. In addition, as an alternative to sending an encrypted shortwave radio broadcast, a CuIS officer often will similarly place an encrypted message onto a diskette and again simply physically deliver the diskette, clandestinely, to the agent. Upon receipt of the encrypted message, either by the CuIS officer or the agent, the recipient employs a decryption program contained on a separate diskette to decrypt the message. The exchange of diskettes containing encrypted messages, and the use of decryption programs contained on separate diskettes, was one of the clandestine communication techniques utilized by the defendants in the Hernandez case described above in paragraph 11. Although it is difficult to decrypt a message without the decryption program, the very process of encrypting or decrypting a message on a computer causes a decrypted copy of the message to be placed on the computer's hard drive. Unless affirmative steps are taken to cleanse the hard drive, beyond simply "deleting" the message, the message can be retrieved from the hard drive.

21. Based on the evidence described below, I have concluded that MONTES was a CuIS agent who communicated with her CuIS handling officer by passing and receiving computer diskettes containing encrypted messages.

22. The message described above that was contained on the hard drive of MONTES's laptop computer contained the following passage:

> Continue writing along the same lines you have so far, but cipher the information every time you do, so that you do not leave prepared information that is not ciphered in the house. This is the most

> sensitive and compromising information that you hold. We realize that this entails the difficulty of not being able to revise or consult what was written previously before each shipment, but we think it is worth taking this provisional measure. It is not a problem for us if some intelligence element comes repeated or with another defect which obviously cannot help, we understand this perfectly.-- Give "E" only the ciphered disks. Do not give, for the time being, printed or photographed material. Keep the materials which you can justify keeping until we agree that you can deliver them.-- Keep up the measure of formatting the disks we send you with couriers or letters as soon as possible, leaving conventional notes as reminders only of those things to reply to or report.

The message goes on to refer to a "shipment" that contains "Disk 'S1' - to cipher the information you send," and, as indicated in the previous section, to "Disk 'R1' to decipher our mailings and radio." Earlier in the message, there is a reference to "information you receive either via radio or disk."

23. During the court-authorized search of the residence on May 25, 2001, two boxes containing a total of 16 diskettes were observed. During a subsequent such search on August 8, 2001, a box containing 41 diskettes, later determined to be blank, were observed. Finally, records obtained from a Radio Shack store located near MONTES's residence indicate that MONTES purchased 160 floppy diskettes during the period May 1, 1993, to November 2, 1997.

III. Communication from MONTES to the CuIS by Pager

24. Based on my knowledge of the methodology employed by the CuIS, I am aware that a clandestine CuIS agent often communicates with his or her handling CuIS officer by making calls to a pager number from a pay telephone booth and entering a pre-assigned code to convey a particular message. This methodology was utilized by the defendants in the Hernandez case described above in paragraph 11.

25. Based on the evidence described below, I believe that MONTES has been communicating with her handling CuIS officer in this fashion.

26. In the same message copied from MONTES's hard drive that has been described earlier in this affidavit, there is a passage that states:

> C) Beepers that you have. The only beepers in use at present are the following: 1) (917) [first seven-digit telephone number omitted from this application], use it with identification code 635. 2) (917) [second seven-digit telephone number omitted from this application]. Use it with identification code 937. 3) (917) [third seven-digit telephone number omitted from this application] Use it only with identification code 2900 . . . because this beeper is public, in other words it is known to belong to the Cuban Mission at the UN and we assume there is some control over it. You may use this beeper only in the event you cannot communicate with those mentioned in 1) and 2), which are secure.

Based on my experience and knowledge, I have concluded that the reference to "control over it" in the above passage refers to the CuIS officer's suspicion that the FBI is aware that this beeper number is associated with the Cuban government and is monitoring it in some fashion.

27. In addition, as described previously, the message on the laptop's hard drive includes a portion stating that the message recipient "entered the code communicating that you were having problems with radio reception." Based on the evidence described above, I have concluded this portion of the message indicates that MONTES at some point shortly prior to receiving the message sent a page to her CuIS officer handler consisting of a pre-assigned series of numbers to indicate she was having communication problems.

28. Based on evidence obtained during the FBI's physical surveillance of MONTES conducted between May and September 2001, I have concluded that MONTES continues to send coded pages to the CuIS. This evidence is described below in paragraphs 38 to 45.

III. MONTES's Transmission of Classified Information to the CuIS

29. The same message described above, as well as other messages recovered from the laptop's hard drive, contained the following information indicating that MONTES had been tasked to provide and did provide classified information to the CuIS.

30. In one portion of the message discussed above, the CuIS officer states:

> What *** said during the meeting . . . was very interesting. Surely you remember well his plans and expectations when he was coming here. If I remember right, on that occasion, we told you how tremendously useful the information you gave us from the meetings with him resulted, and how we were waiting here for him with open arms.

31. I have replaced in this application with "***" a word that begins with a capital letter, which was not translated, and is in fact the true last name of a U.S. intelligence officer who was present in an undercover capacity, in Cuba, during a period that began prior to October 1996. The above quoted portion of the message indicates that MONTES disclosed the U.S. officer's intelligence agency affiliation and anticipated presence in Cuba to the CuIS, which information is classified "Secret." As a result, the Cuban government was able to direct its counter-intelligence resources against the U.S. officer ("we were waiting here for him with open arms").

32. The very next section in the message states:

> We think the opportunity you will have to participate in the ACOM exercise in December is very good. Practically, everything that takes place there will be of intelligence value. Let's see if it deals with contingency plans and specific targets in Cuba, which are to prioritized interests for us.

33. I have concluded that the "ACOM exercise in December" is a reference to a December 1996 war games exercise conducted by the U.S. Atlantic Command, a U.S. Department of Defense

unified command, in Norfolk, Virginia. Details about the exercise's "contingency plans and specific targets" is classified “Secret” and relates to the national defense of the United States.

34. DIA has advised that MONTES attended the above exercise in Norfolk, as part of her official DIA duties.

35. In a separate message partially recovered from the hard drive of MONTES’s Toshiba laptop, the message reveals details about a particular Special Access Program (SAP) related to the national defense of the United States, and states: “In addition, just today the agency made me enter into a program, ‘special access top secret. [First name, last name omitted from this application] and I are the only ones in my office who know about the program.” The details related about this SAP in this message are classified “Top Secret" / SCI.

36. DIA has confirmed that MONTES and a colleague with the same name as that related in the portion of the message described above were briefed into this SAP, together, on May 15, 1997. Accordingly, I have concluded that the above message from MONTES to a CuIS officer.

37. In yet another message recovered from the laptop, there is a statement revealing that “we have noticed” the location, number and type of certain Cuban military weapons in Cuba. This information is precisely the type of information that is within MONTES’s area of expertise, and is, in fact, an accurate statement of the U.S. intelligence community’s knowledge on this particular issue. The information is classified “Secret.” Accordingly, I have concluded that this message also is a message from MONTES to a CuIS officer.

FBI Physical Surveillance of MONTES and Telephone Records for May to September 2001

38. FBI physical surveillance of MONTES has shown a recent pattern of pay telephone calls by her to a pager number, a communication method that, as described above in paragraph 24, is

consistent with known CuIS communications plans and operations. In each paragraph below that refers to MONTES driving, she was utilizing the Toyota described above in paragraph 2.

39. The FBI maintained periodic physical surveillance of MONTES during the period May to September 2001. On May 20, 2001, MONTES left her residence and drove to the Hecht's on Wisconsin Avenue, in Chevy Chase, Maryland. She entered the store at 1:07 p.m. and exited by the rear entrance at 1:27 p.m. She then sat down on a stone wall outside the rear entrance and waited for approximately two minutes. At 1:30 p.m., the FBI observed her walk to a pay phone approximately 20 feet from where she was sitting. She placed a one minute call to a pager number using a pre-paid calling card. At 1:45 p.m. she drove out of the Hecht's lot and headed north on Wisconsin Avenue toward Bethesda, Maryland. At 1:52 p.m. she parked her car in a lot and went into Modell's Sporting Goods store. She quickly exited the store carrying a bag and crossed Wisconsin Avenue to an Exxon station. She was observed looking over her right and left shoulders as she crossed the Exxon lot. At 2:00 p.m. she placed a one minute call from a pay phone at the Exxon station to the same pager number using the same pre-paid calling card. By 2:08 p.m., MONTES had walked back to her vehicle and was driving back to her residence where she arrived at 2:30 p.m.

40. On June 3, 2001, MONTES engaged in similar communications activity. She left her residence at approximately 2:30 p.m. and drove to a bank parking lot at the corner of Harrison Street, N.W. and Wisconsin Avenue, N.W. She exited her car at approximately 2:37 pm and entered a Borders Book Store on Wisconsin Avenue. She left the store approximately 40 minutes later. She then crossed Wisconsin Avenue to the vicinity of three public pay phones near the southern exit of the Friendship Heights Metro Station. At 3:28 p.m. she placed a one-minute call using the same pre-

paid calling card to the same pager number she had called on May 20, 2001. After a few minutes, she walked back to her car and drove to a grocery store.

41. Pursuant to court authorization, on August 16, 2001, the FBI searched MONTES's pocketbook. In a separate compartment of MONTES's wallet, the FBI found the pre-paid calling card used to place the calls on May 20, 2001 and June 3, 2001. In the same small compartment, the FBI located a slip of paper on which was written the pager number she had called. Written above this pager number was a set of digits that I believe comprise one or more codes for MONTES to use after calling the pager number, i.e., after contacting the pager, she keys in a code to be sent to the pager which communicates a particular pre-established message.

42. On August 26, 2001, at approximately 10:00 a.m., the FBI observed MONTES making a brief pay telephone call to the same pager number from a gas station/convenience store located at the intersection of Connecticut and Nebraska Avenues, N.W., in Washington, D.C.

43. On September 14, 2001, MONTES left work and drove directly to her residence. She then walked to Connecticut Avenue, N.W., in Washington, D.C., still wearing her business clothes, and made a stop at a dry cleaning shop. She then entered the National Zoo through the Connecticut Avenue entrance. She proceeded to the "Prairie Land" overlook where she stayed for only 30 seconds. She then walked further into the zoo compound and basically re-traced her route out of the zoo. At approximately 6:30 p.m. MONTES removed a small piece of paper or card from her wallet and walked to a public phone booth located just outside the pedestrian entrance to the zoo. MONTES then made what telephone records confirmed to be two calls to the same pager number she had called in May, June and August, as described above. The records reflect that the first call was unsuccessful, i.e., the call lasted zero seconds. According to the records, she made a second call

one minute later that lasted 33 seconds. Shortly after making these calls, MONTES looked at her watch and then proceeded to walk back to her residence.

43. On September 15, 2001, telephone records pertaining to the pre-paid calling card number on the card observed in her pocketbook on August 16, 2001, show that MONTES made a call to the same pager number at 11:12 a.m. that lasted one minute.

44. On September 16, 2001, MONTES left her residence in the early afternoon and took the Metro (Red Line) to the Van Ness - UDC station in Washington, D.C. She made a brief telephone call from a payphone in the Metro station at approximately 1:50 p.m., again to the same pager number.

45. MONTES is known to possess a cell phone. A cell phone was observed during a court-authorized search of her tote bag on August 16, 2001. In addition, during surveillance on September 16, 2001, MONTES was observed speaking on a cell phone. Furthermore, telephone records obtained in May 2001 confirm that she has subscribed to cell telephone service continually from October 26, 1996 to May 14, 2001. MONTES's use of public pay phones notwithstanding her access to a cell phone supports my conclusion that the pay phone calls described in this section were in furtherance of MONTES's espionage.

Probable Cause to Seize Documents, Materials and Computer Media

46. My experience has shown that individuals involved in espionage very often maintain copies of correspondence, draft documents and even classified government documents which are themselves of evidentiary value, along with evidence of criminal and other associations. This evidence includes directories, lists, news articles, photographs, travel and similar material. The items and materials utilized by persons engaged in espionage is further described in Attachment B.

47. MONTES is known to have both a laptop and a desktop computer in her residence. In addition, she utilizes a desktop computer in her office in the DIAC. These computers may be attached to peripherals such as printers when the search warrants are executed. Searching these computer systems may require a range of data analysis techniques. In some cases, it is possible for the agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps all are anticipated to be applicable in this case. These steps may require agents to conduct more extensive searches, which can more easily be accomplished with equipment that cannot be brought to the search sites, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence in the computers, diskettes, and peripherals that are located within the places and items to be searched, and to remove these items from the places to be searched so that the items may be searched more thoroughly.

Conclusion

48. Based on the evidence described above, I believe probable cause exists that from on or about October 5, 1996, to the date of this affidavit, in the District of Columbia and elsewhere, ANA

BELEN MONTES, conspired, confederated and agreed with persons known and unknown to violate 18 U.S.C. § 794(a), that is, to communicate, deliver and transmit to the government of Cuba and its representatives, officers and agents, information relating to the national defense of the United States, with the intent and reason to believe that the information was to be used to the injury of the United States and to the advantage of Cuba, and that MONTES committed acts to effect the object of this conspiracy in the District of Columbia and elsewhere, all in violation of 18 U.S.C. § 794(c).

49. I further believe that probable cause exists that the items and locations described in Attachment A contain evidence, fruits, and instrumentalities relating to the above violation, which evidence fruits and instrumentalities are further described in Attachment B.

STEPHEN A. McCOY, Special Agent
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED BEFORE ME THIS _____ DAY OF SEPTEMBER, 2001.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The residence of ANA BELEN MONTES is located at 3039 Macomb Street, N.W., apartment 20, Washington, D.C. 20008. 3039 Macomb Street, N.W., is titled "The Cleveland Apartments," and is a three story, red brick building. Apartment 20 is on the second floor and is the first door on the left.

ATTACHMENT B

1. Espionage paraphernalia, including devices designed to conceal and transmit national defense and classified intelligence information and material, and implements used by espionage agents to communicate with their handlers and with a foreign government, to wit: white tape, mailing tape, colored chalk (all used for signaling purposes), coded pads, secret writing paper, microdots, any letters, notes or other written communications (including contact instructions) between defendant ANA BELEN MONTES and any agents of the CuIS or other intelligence service of Cuba; any computers, (including laptops), computer disks, cameras, film, codes, telephone numbers, maps, photographs and other materials relating to communication procedures, correspondence;

2. Records, notes, calendars, journals, maps, instructions, and classified documents and other papers and documents relating to the transmittal of national defense and classified intelligence information (including the identities of foreign espionage agents and intelligence officers and other foreign assets or sources providing information to the United States Intelligence Community, such as the FBI and CIA; records of previous illicit espionage transactions, national defense transactions, national defense and classified intelligence information, including copies of documents copied or downloaded by ANA BELEN MONTES from the DIA);

3. Passports, visas, calendars, date books, address books, credit card, hotel receipts and airline records, reflecting travel in furtherance of espionage activities;

4. Identity documents, including but not limited to passports, licenses, visas (including those in fictitious or alias identities), U.S. and foreign currency, instructions, maps, photographs, U.S. and foreign bank account access numbers and instructions and other papers and materials relating to emergency contact procedures and escape routes;

5. Safety deposit box records, including signature cards, bills, and payment records, safety deposit box keys, whether in the name of the defendant or a family member; any records pertaining to any commercial storage sites where the defendant may be storing other classified intelligence and counter-intelligence documents or other records of her espionage activities;

6. Federal, state and local tax returns, work sheets, W-2 forms, 1099 forms, and any related schedules;

7. Telephone bills and records, including calling cards and pager records;

8. Photographs, including photographs of co-conspirators; correspondence (including envelopes) to and from ANA BELEN MONTES and handlers, contacts and intelligence agents of Cuba;

9. Computer hardware, software, and storage media, known to be used by the defendant or to which she had access, including, but not limited to: any personal computer, laptop computer, modem, and server, which have been and are being used to commit the offenses of espionage and conspiracy to commit espionage; records, information and files contained within such computer hardware containing evidence and fruits of defendant's espionage activity between October 5, 1996, and the present, including classified documents, in whatever form and by whatever means they have been created or stored, including but not limited to any electrical, electronic, or magnetic form of storage device; floppy diskettes, hard disks, zip disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm III devices, removable hard drives, memory cards, zip drives, and any photographic forms of such records including microfilm, digital prints, slides, negatives, microfiche, photocopies, and videotapes, computer terminals and printers used by the defendant in said espionage activity.