

~~TOP SECRET~~

DoDIG: (b)(1), 1.4  
(c)

~~NOFORN//MR~~

Report No. 05-INTEL-18  
June 16, 2005  
Review

# OFFICE OF THE INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE



DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

## Review of the Actions Taken to Deter, Detect and Investigate the Espionage Activities of Ana Belen Montes (U)

Derived from: Multiple Sources  
Declassify on: MR

Copy \_\_\_\_ of \_\_\_\_

~~TOP SECRET~~

DoDIG: (b)(1), 1.4  
(c)

~~NOFORN//MR~~

### Additional Copies

If you have questions on the report, or to request additional copies, contact

<sup>DoD IG: (b) (6)</sup> at (703) 604-<sup>DoD IG: (b) (6)</sup> (DSN 664-<sup>DoD IG: (b) (6)</sup>) or <sup>DoD IG: (b) (6)</sup> at (703) 604-<sup>DoD IG: (b) (6)</sup> (DSN 664-<sup>DoD IG: (b) (6)</sup>).

### Suggestions for Evaluations

To suggest ideas for or to request evaluations of Defense intelligence issues, contact the Office of the Deputy Inspector General for Intelligence at (703) 604-8800 (DSN 664-8800) or fax (703) 604-0045. Ideas and requests can also be mailed to:

Office of the Deputy Inspector General for Intelligence  
Department of Defense Office of Inspector General  
400 Army Navy Drive (Room 703)  
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE

**hotline**

**To report fraud, waste, mismanagement, and abuse of authority.**

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900  
Phone: 800.424.9098 e-mail: [hotline@dodig.osd.mil](mailto:hotline@dodig.osd.mil) [www.dodig.osd.mil/hotline](http://www.dodig.osd.mil/hotline)

### Acronyms

ASD(C<sup>3</sup>I)

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

<sup>CIA: (b) (3), 50</sup>

<sup>CIA: (b) (3), 50 U.S.C. § 403, Sec. 6</sup>

CIA

Central Intelligence Agency

CDI

Center for Defense Information

CIFA

Counterintelligence Field Activity

CSP

Counterintelligence Scope Polygraph

DIA

Defense Intelligence Agency

DCI

Director of Central Intelligence

DoD

Department of Defense

DoJ

Department of Justice

DoS

Department of State

FBI

Federal Bureau of Investigation

FISA

Foreign Intelligence Surveillance Act

HUMINT

Human Intelligence

JCEO

Joint Counterintelligence Evaluation Office

ONCIX

Office of the National Counterintelligence Executive

NSA

National Security Agency

SAFE

Support for the Analyst's File Environment

SAP

Special Access Program

SCI

Sensitive Compartmented Information

SECDEF

Secretary of Defense

SIGINT

Signals Intelligence

USSOUTHCOM

U.S. Southern Command





~~TOP SECRET~~ DoD IG: (b) (1), 1.4(e) ~~NOFORN//MR~~

INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

June 16, 2005

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Review of the Actions Taken to Deter, Detect and Investigate the Espionage Activities of Ana Belen Montes (Report No. 05-INTEL-18) (U)

(U) We are providing this report for information and use. We conducted the review in response to a request from the Chairman, House Permanent Select Committee on Intelligence. We considered management comments on a draft of this report in preparing the final report.

(C) Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3. Although management concurred with all recommendations, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics periodically provide us with the status of the plan to implement the DoD central registry for personnel with access to Special Access Program.

CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(5), (b)(7)(E)  
CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(5), (b)(7)(E)

(U) We appreciate the courtesies extended to the staff. Questions should be directed to DoD IG: (b)(6) at (703) 604-DoD IG: (b)(6) (DSN 664-DoD IG: (b)(6) or DoD IG: (b)(6) at (703) 604-DoD IG: (b)(6) (DSN 664-DoD IG: (b)(6) See Appendix F for the report distribution. Team members for this review are listed on the inside back cover.

*Thomas F. Gimble*  
Thomas F. Gimble  
Deputy Inspector General  
for Intelligence

This page is downgraded to  
~~CONFIDENTIAL~~ when separated  
from attachment

~~TOP SECRET~~ DoD IG: (b) (1), 1.4(e) ~~NOFORN//MR~~

DoD OIG 000003

~~TOP SECRET~~ <sup>DoD IG: (b)  
(1), 1.4(c)</sup> ~~NOFORN//MR~~

DISTRIBUTION

UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND  
LOGISTICS

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

DEPUTY UNDER SECRETARY OF DEFENSE FOR COUNTERINTELLIGENCE  
AND SECURITY

DIRECTOR, DEFENSE INTELLIGENCE AGENCY

DIRECTOR, NATIONAL SECURITY AGENCY

NATIONAL COUNTERINTELLIGENCE EXECUTIVE

INSPECTOR GENERAL, CENTRAL INTELLIGENCE AGENCY

INSPECTOR GENERAL, DEPARTMENT OF JUSTICE

DIRECTOR, COUNTERINTELLIGENCE FIELD ACTIVITY

~~TOP SECRET~~ <sup>DoD IG: (b)  
(1), 1.4(c)</sup> ~~NOFORN//MR~~



THIS PAGE INTENTIONALLY LEFT BLANK (U)



(U) Ana Montes receives the DCI National Intelligence Certificate of Distinction from then-Deputy DCI George Tenet in <sup>DIA: (b)(3), 10 U.S.C. §  
424</sup>



**Department of Defense Office of the Inspector General**

**Report No. 05-INTEL-18**

**June 16, 2005**

(Project No. D2004-DINTEL-0012)

**(U) Review of the Actions Taken to Deter, Detect and Investigate  
the Espionage Activities of Ana Belen Montes**

**(U) Executive Summary**

**(U//~~FOUO~~) Who Should Read This Report and Why?** Congressional intelligence oversight committees and the Intelligence Community should read this report to gain a better appreciation for the Cuban espionage threat to the United States. The lessons learned from the Ana Montes case should help to counter future threats to national security.

**(U) Introduction.** On September 21, 2001, following months of intense scrutiny, Federal Bureau of Investigation officials arrested Ana Belen Montes at the Defense Intelligence Agency in Washington, D.C., on charges of conspiracy to commit espionage against the United States. Ms. Montes had been an employee of the U.S. Government for 22 years and had been employed as an intelligence analyst with the Defense Intelligence Agency for the better part of those years. She was recruited by the Cuban Intelligence Service in 1984 while employed by the Department of Justice. Montes pleaded guilty to one count of the indictment and was sentenced to 25 years in prison on October 16, 2002. She is currently serving her sentence at the Carswell Federal Medical Center, Fort Worth, Texas.

**(U//~~FOUO~~)** In April 2002, the Director of Central Intelligence directed the Office of the National Counterintelligence Executive to conduct a comprehensive damage assessment of the espionage activities of Ana Montes. The Office of the National Counterintelligence Executive organized the Montes Damage Assessment Team to focus on the identification of U.S. classified and sensitive information that was put at risk and possibly compromised to the Cuban Intelligence Service by Ms. Montes between 1985 and 2001. The Damage Assessment report was published in January 2005.

**(U//~~FOUO~~)** On August 27, 2003, the House Permanent Select Committee on Intelligence requested that the Department of Defense Inspector General initiate a full review of the Montes security breach and the response of the U.S. Intelligence Community to that activity. The Committee further requested that the Inspector General include recommendations to correct identified weaknesses in Defense Intelligence Agency security and counterespionage procedures and practices.

**(U//~~FOUO~~)** If possible, to acquire a complete mosaic of the life of Ana Montes and the totality of her espionage activities in support of Cuba, this report should be read in conjunction with the Office of the National Counterintelligence Executive Damage Assessment on Ms. Montes.

**(U) Objective.** Our objective was to examine the espionage activities of Ana Belen Montes to determine the effectiveness of the Defense Intelligence Agency's security and counterespionage policy, procedures, and practices relating to that case, to assess the



Intelligence Community's reactions to the Montes security breach, and identify lessons learned that might prevent recurrence of espionage activities perpetrated against the United States.

(U) Results. Based on our review, we conclude that:

- (S) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]
- (S) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]
- (S) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]
- (S) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]
- (S) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]

(U) During the review, we made several observations. While the observations do not necessarily encompass the scope of the review, they have an effect on the ability of the Intelligence Community to deter, detect, and investigate espionage activities perpetrated against the United States.

- (U//FOUO) Once Ana Montes was identified as a suspect, the investigation leading to her arrest and conviction was a model of efficiency and effectiveness.
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]

- (U//~~FOUO~~) <sup>FBI, (b)(7)(E)</sup> [REDACTED]
- (S//NF) <sup>FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1), (b)(7)(E)</sup> [REDACTED]
- (U//~~FOUO~~) The Defense Intelligence Agency's adoption of risk management as the operating information technology philosophy successfully postulates that it is possible to balance the risk of disclosure against the cost of protection.

(S//NF) **Summary of Recommendations.** We recommend that the Under Secretary of Defense for Intelligence request that the Intelligence Community Inspectors General Forum conduct a comprehensive, joint evaluation of counterespionage information sharing; formulate a plan to establish permanent Foreign Counterintelligence Program billets to build a DoD counterespionage organization similar to the <sup>CIA, (b)(3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED]; and direct all DoD entities with polygraph programs to digitize and retain for a minimum of 35 years all counterintelligence scope polygraph examination charts.

(C) We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics continue the process of establishing a DoD central registry for personnel with access to Special Access Programs.

(C) <sup>DIA, (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]

(U//~~FOUO~~) We recommend that the Deputy Under Secretary of Defense for Counterintelligence and Security continue working with Congress to change DoD polygraph provisions in Title 10, United States Code, section 1564a, and then update DoD Directive 5210.48 and DoD Regulation 5210.48-R, accordingly.

(U//~~FOUO~~) <sup>DIA, (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)</sup> [REDACTED]



DIA: (b)(3), 10 U.S.C. § 424, (b)(5), (b)(7)(E)

(U//~~FOUO~~) Finally, we would like to acknowledge that we are deeply indebted to the Office of the National Counterintelligence Executive Montes Damage Assessment Team for its outstanding cooperation, guidance, and advice. We are also grateful for the support given to us by Special Agents and counterintelligence officials from the Federal Bureau of Investigation Washington Field Office and counterintelligence officials from the Defense Intelligence Agency. Their professional support helped us to better understand the complexities of counterespionage in general and Ana Montes' betrayal of her country in particular.

**(U) Management Comments.** We received comments on a draft of this report from the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Intelligence; the Director, Defense Intelligence Agency; the National Security Agency; the Central Intelligence Agency; and the Inspector General, Department of Justice. All organizations concurred with our recommendations, however, some suggestions were made to clarify the report. See Part VIII for the complete text of those comments. While not required to comment on a draft of this report, the Office of the National Counterintelligence Executive offered meaningful, informal suggestions and advice that clarified the factual content of the report.

**(U) Review Response.** Management comments were responsive. Although management concurred with all recommendations, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics periodically provide us with the status of the plan to implement the DoD central registry for personnel with access to Special Access Program.

<sup>CIA: (b)(3), 50 U.S.C. § 403, Sec. 6, DIA: (b)(5), (b)(7)(E)</sup>

[REDACTED]



## **(U) Table of Contents**

---

<b>(U) Executive Summary</b>	<b>i</b>
<b>(U) Part I. Introduction</b>	<b>1</b>
(U) Background	1
(U) Objective	2
(U) Scope and Methodology	2
(U) Limitations	4
(U) Acknowledgment	4
(U) Structure of the Report	4
<b>(U) Part II. The Enigmatic Life of Ana Montes</b>	<b>6</b>
(U) Early Years	6
(U) Education	6
(U) Religion	7
(U) Health	7
(U) Lifestyle	8
(U) Political Influence	8
(U) An Employment Opportunity at the Department of Justice	8
(U) Introduction to Espionage	9
(U) Joining the Defense Intelligence Agency	10
(U) Portrait of a Spy	13
<b>(U) Part III. Government Service and a Commitment to Espionage</b>	<b>16</b>
(U) Initial Government Employment	16
(U// <del>FOUO</del> ) Recruitment by the Cuban Intelligence Service – Moral Imperatives Justify Treason	17
(U// <del>FOUO</del> ) Valuable Asset for the Cubans	19
(U) Background Developments at DIA	19
(U) DIA Applicant Processing	20
(U) DIA Personnel Security and Clearance Adjudication Practices for New Employees	21
(U) The “Night Job” Picks Up	23
(U) Sharpening Skills as a DIA Analyst--1986-1990	24
(U// <del>FOUO</del> ) ...And as a Cuban Clandestine Reporting Source	25
(U// <del>FOUO</del> ) A Second Clandestine Trip to Cuba	26
(U) Security Reinvestigation--1991	27
(U) Coupling Analytic Expertise and Espionage Activities	28
(U) Exceptional Analyst Program	29
(U// <del>FOUO</del> ) Montes Encounters and Beats the Polygraph	30
(U// <del>FOUO</del> ) Counterespionage Efforts Against Cuba	31

<b>(U) Part IV. Maturation as Analyst and Spy</b>	33
(U// <del>FOUO</del> ) <del>DoD(G) (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403, Sec. 6</del>	33
(U) Attendance at Academic Forums	34
(U) Events Surrounding the Brothers to the Rescue Incident	35
(U) Significant Travel and Recognition	37
(U) Security Processing	39
(U) Counterespionage Efforts Against Cuba	39
(U// <del>FOUO</del> ) Support for the Analyst's File Environment System	42
(U) Prelude to Catching a Spy	43
 <b>(U) Part V. A Prominent Life Unraveled</b>	45
(U// <del>FOUO</del> ) <del>DoD(G) (b) (6)</del> Concerns	45
(U) Significant Travel and Recognition	46
(U) Respect for Montes Deepens	48
(U) Additional Access	49
(U// <del>FOUO</del> ) A Potential Fellowship at the National Intelligence Council Clouded by an Inspector General Investigation	49
(U// <del>FOUO</del> ) Counterespionage Efforts Against Cuba	51
(U) The End Game	58
(U// <del>FOUO</del> ) The Finale to More Than Sixteen Years of Espionage	63
(U) Post Arrest	63
 <b>(U) Part VI. Findings, Recommendations, and Observations</b>	65
 <b>(U) Part VII. Appendixes</b>	113
(U) Appendix A. Montes' Official and Unofficial Travel	115
(U) Appendix B. Montes' Awards, Recognition, and Training	121
(U) Appendix C. Background on the Brothers to the Rescue Incident	127
(C) Appendix D. Montes' Accesses to Sensitive Programs and Information	129
(U// <del>FOUO</del> ) Appendix E. <del>DoD(G) (b) (7)(E)</del>	131
(U) Appendix F. Report Distribution	133
 <b>(U) Part VIII. Management Comments</b>	135
(U) A. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics	136
(U) B. Under Secretary of Defense for Intelligence	137
(U) C. Director, Defense Intelligence Agency	145
(U) D. <del>DoD(G) (b) (1), 1.4(c)</del>	152
(U) E. Central Intelligence Agency	154
(U) F. Inspector General, Department of Justice	164

## (U) Part I. Introduction

### (U) Background

(U//~~FOUO~~) On September 21, 2001, following months of intense scrutiny and surveillance, Federal Bureau of Investigation (FBI) officials interviewed and then arrested Ana Belen Montes at the Defense Intelligence Analysis Center, Defense Intelligence Agency (DIA), Washington, D.C. She was charged with conspiracy to commit espionage against the United States in violation of 18 United States Code section 794(a) and (c). Montes pleaded guilty to one count of the indictment on March 19, 2002. The court sentenced her to 25 years in prison on October 16, 2002. She is currently serving her sentence in the Carswell Federal Medical Center, Fort Worth, Texas. Ms. Montes was a U.S. Government employee for 22 years, the last 16 of which (1985-2001) she was an intelligence analyst with the DIA. The Cuban Intelligence Service recruited her in late 1984, while she worked as a paralegal at the Department of Justice (DoJ) in Washington, D.C.

(S//NF) On April 17, 2002, the Director of Central Intelligence (DCI) directed the Office of the National Counterintelligence Executive (ONCIX)<sup>1</sup> to conduct a comprehensive Intelligence Community<sup>2</sup> damage assessment of the espionage activities of Ana Montes. The ONCIX organized a Montes Damage Assessment Team. The Team formulated Terms of Reference, which the DCI approved on August 6, 2002. The Terms of Reference focused on identifying U.S. classified and sensitive information that Montes put at risk and possibly compromised to the Cuban Intelligence Service between 1985 and 2001. The ONCIX published its damage assessment report on Montes in January 2005.

(U//~~FOUO~~) On August 27, 2003, the House Permanent Select Committee on Intelligence requested that the Department of Defense Inspector General initiate a full review of the Montes security breach to include the response of the U.S. Intelligence Community. The Committee further requested that the Inspector General include recommendations to correct identified weaknesses in DIA security and counterespionage procedures and practices. The Committee suggested that the Inspector General review consider the basic report framework that the Inspectors General of the Central Intelligence Agency (CIA) and the DoJ used in their investigations of the espionage cases involving Aldrich Ames, a CIA intelligence officer, and Robert Hanssen, a senior FBI Special Agent, in 1994 and 2001, respectively. On September 30, 2003, following a series of discussions

<sup>1</sup>(U) The ONCIX is responsible for improving the performance of the counterintelligence community by identifying, assessing, prioritizing and countering intelligence threats to the United States; ensuring counterintelligence community efficiency and effectiveness; and providing the integration of the counterintelligence activities of the U.S. Government.

<sup>2</sup>(U//~~FOUO~~) The Intelligence Community is composed of the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, the Department of State's Bureau of Intelligence and Research, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, and the intelligence elements of the Federal Bureau of Investigation, the Department of the Treasury, the Department of Energy, the Department of Homeland Security, the Coast Guard, and the Military Departments.



with the Chief of the ONCIX Montes Damage Assessment Team and officials who led the CIA and DoJ investigations of Ames and Hanssen, Committee staff members and Inspector General representatives agreed on an open-ended, "reasonable" time for issuing the report. We initiated the review on October 1, 2003.

## **(U) Objective**

(U) The objective of our review was to examine the espionage activities of Ana Belen Montes to determine the effectiveness of DIA security and counterespionage policy, procedures, and practices relating to that case, to assess the Intelligence Community reactions to the Montes security breach, and to identify lessons learned that might prevent recurrence of espionage activities perpetrated against the United States. To acquire a complete mosaic of the life of Ana Montes and the totality of her espionage activities in support of Cuba, this report should be read in conjunction with the January 2005 ONCIX Montes damage assessment.

## **(U) Scope and Methodology**

(U//~~FOUO~~) We used an historical research design to reconstruct the past objectively and accurately by collecting, evaluating, verifying, and synthesizing evidence to establish facts and reach defensible conclusions. We augmented that approach with compare-and-contrast methodologies, where appropriate. Our historical research design included the following eight components.

1. We reviewed and analyzed more than 250,000 pages of relevant documentation received from DoD and non-DoD entities that included the ONCIX Montes Damage Assessment Team, the FBI, the CIA, the DIA, the National Security Agency (NSA), the National Reconnaissance Office, the National Geospatial-Intelligence Agency, selected elements of the Office of the Secretary of Defense, including the Counterintelligence Field Activity (CIFA), the Department of State (DoS), the Military Departments, selected Combatant Commands, and the DoD Polygraph Institute. We obtained a large portion of the relevant documentation from the ONCIX Montes Damage Assessment Team, which had initially received the documentation from the FBI and DIA.
2. We reviewed and analyzed other relevant documentation obtained from data calls to DoD and non-DoD entities for historical e-mail records.
3. We reviewed more than 40 transcripts of Montes debriefings conducted between the spring of 2002 and mid-2004 by officials who had a major interest in her activities. Videotapes accompanied many of the transcripts.
4. We interviewed 78 current and former U.S. Government employees who had firsthand information or expert knowledge of the issues related to Montes. The interviews were primarily open-ended narratives, with additional questions and sessions as required. Before we conducted the interviews, we reviewed the results

of more than 100 FBI interviews (Letterhead Memoranda) of individuals who were directly or indirectly associated with Montes. Those reviews helped us to determine whether followup interviews of those individuals were required, and further assisted us in developing a list of officials not yet interviewed whom we needed to contact to satisfy our objective. Specifically, we interviewed cognizant civilian and military representatives from the Office of the Secretary of Defense, the CIA, FBI, DIA, NSA, DoS, the National Military Joint Intelligence Center, the Air Force Office of Special Investigations, the Naval Criminal Investigative Service, the DoD Polygraph Institute, and the CIFA. We also interviewed a former Director of the DIA and Ana Montes.

5. We discussed methodology, best practices, historical perspectives, psychological profiles, and many other issues related to the Montes case with the:

- Director, DIA
- Inspector General, DIA
- <sup>DIA (b)(3), 10 U.S.C. § 424</sup> [REDACTED] DIA
- Associate Director, Office of Oversight and Review, DoJ
- Chief, Counterintelligence Division, Americas Section, FBI Headquarters
- Special Agents, Washington, D.C., New York, San Diego, and Dallas Field Offices, FBI
- General Counsel, Office of the Inspector General, CIA
- Chief, <sup>CIA (b)(3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED], CIA
- Director, Assessments Group, ONCIX
- Chief, Montes Damage Assessment Team, ONCIX
- Executive Vice President, Academy Group, Inc., a forensic behavioral science company
- Officials at the Federal Bureau of Prisons, Carswell Federal Medical Center, Fort Worth, Texas

6. We searched the World Wide Web and the Joint Worldwide Intelligence Communications System for information on Government and non-Government organizations and information related to the Montes case.

7. We reviewed contemporary literature for historical information on espionage cases perpetrated against the United States.

8. We conferred with counterintelligence and counterespionage officials at the 2004 Defense Counterintelligence Conference to gain a better appreciation of specific issues related to the Montes case.



## (U) Limitations

(U) We encountered three limitations during our review. First, Ana Montes entered U.S. Government service in 1979 and subsequently began her career as an intelligence analyst at DIA in 1985. Thus, some individuals, particularly higher level officials with broader responsibilities, found it difficult to recall specific events or circumstances that occurred or details of actions taken several years ago. Second, we were unable to recover all of the historical records related to Montes, particularly hard copy documents such as letters, memoranda, informal notes, and records of meetings that may have been destroyed, purged, or discarded regularly before computers became widely used. Even after reviewing more than 250,000 pages of documentation, we could not state categorically that we possessed all the necessary documents. Third, we were unable to obtain the DoJ 2003 classified report, "A Review of the FBI's Performance in Detering, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." Although the House Permanent Select Committee on Intelligence charged us to use the Hanssen and Ames reports as our guide for constructing the Montes report, numerous requests to read the Hanssen report were rejected. The DoJ and the House Permanent Select Committee on Intelligence did not share the contents of the Hanssen report. The CIA gave us access to their report on Ames.

## (U) Acknowledgment

(U//~~FOUO~~) We are deeply indebted to the ONCIX Montes Damage Assessment Team for its outstanding cooperation, guidance, and advice. We appreciate the Team's "can do" spirit in assisting us in our objective. We are also grateful for the support given to us by Special Agents and counterintelligence officials from the FBI Washington Field Office and counterintelligence officials from the DIA. Their professional support gave us a better understanding of the complexities of counterespionage in general and Ana Montes' betrayal of her country in particular. Furthermore, with rare exceptions, officials at every Government agency that we encountered gave us unrestricted access to all pertinent documentation and to key individuals who were associated with the Montes espionage case.

## (U) Structure of the Report

(U//~~FOUO~~) This report is presented in eight parts, including Part I, the Introduction. Part II provides a comprehensive mosaic of the life of Ana Belen Montes. Parts III, IV, and V review Montes' professional career and her career as a spy. These parts also detail U.S. Government counterespionage efforts against Cuba during each period. Part III covers 1979 to 1994, Part IV, 1994 to 1998, and Part V, 1998 through Montes' arrest in 2001. Part VI addresses findings, recommendations, and observations. Part VII contains six appendixes. Appendix A discusses Montes' official and unofficial travel. Appendix B lists the awards, recognition, and training that Montes received while employed at the DIA. Appendix C provides background on the Brothers to the Rescue incident. Appendix D lists Montes' Intelligence Community accesses. Appendix E explains the role of ~~(b) (7)(E)~~. Appendix F



contains the report distribution list. Part VIII contains management comments. A list of commonly used acronyms is at the front of the report.

## (U) Part II. The Enigmatic Life of Ana Montes

“The King hath note of all that they intend by interception which they dream not of.”  
King Henry V, Act II, Scene II  
Shakespeare

This quotation was found in Montes’ work place cubicle the day of her arrest. She later explained that the quotation applied to her double life as a DIA intelligence analyst and as an espionage agent for Cuba.

### (U) Early Years

(U) Ana Belen Montes was born on <sup>DoD/G: (b) (6)</sup> , 1957, at the <sup>DIA: (b) (6)</sup>

[REDACTED]

(U) <sup>DIA: (b) (6)</sup>

[REDACTED]

(S//NF) <sup>DIA: (b) (1), 1.4(c), (b) (6)</sup>

[REDACTED]

## (U) Education

(C//NF) DIA: (b)(1), 1.4(c), (b)(6)

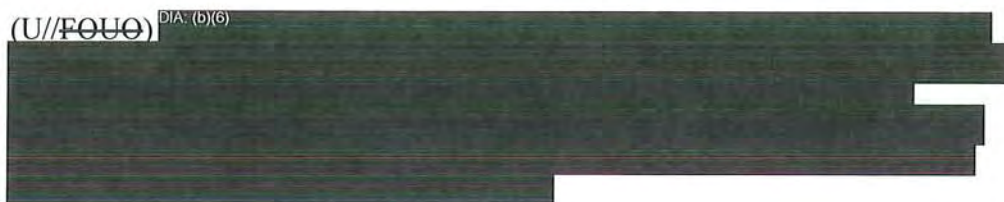


(C//NF) DIA: (b)(1), 1.4(c), (b)(6)



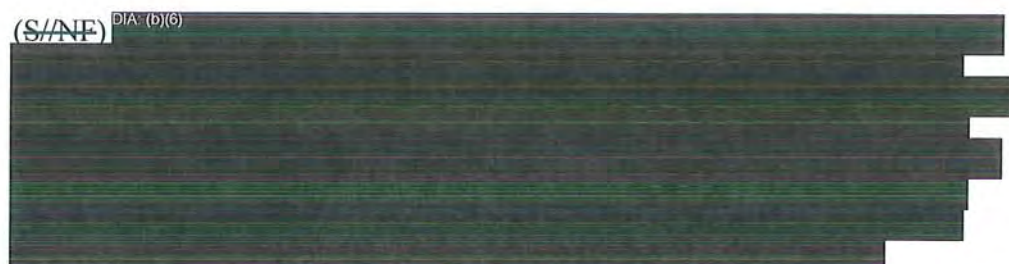
## (U) Religion

(U//FOUO) DIA: (b)(6)



## (U) Health

(S//NF) DIA: (b)(6)





DIA: (b)(6)



## (U) Lifestyle

(S//NF) Montes lived alone. During her time in Washington, she owned one modest condominium. She portrayed herself as an introverted loner who did not need people to be fulfilled. She limited her social contacts to family members, individuals she met in college and graduate school, coworkers at the DoJ, or members of the condominium association in which she was active. She rarely invited colleagues to her home. At work, she seldom left her desk, avoided office get-togethers, and cultivated a reputation for being aloof. She said she sacrificed a normal life and did not want personal relationships to interfere with her espionage activities. In so doing, she dated only intermittently until her early 40s

DIA: (b)(1), 1.4(c), (b)(6)



## (U) Political Influence

(S//NF) Despite her family's record of political and social activism, Montes was politically inactive. There is no evidence to suggest that she attempted to join a political party or a political action group. In college, she expressed a commitment

DIA: (b)(1), 1.4(c), (b)(6)



## (U) An Employment Opportunity at the Department of Justice

(S//NF) Montes received some monetary support from her father and worked numerous part-time and summer jobs to assist in financing her college education.

DIA: (b)(1), 1.4(c), (b)(6)



<sup>DIA (b)(1), 1.4(c), (b)(6)</sup>



(S//NF) In the fall of 1979, she accepted a job as a clerk typist and then became a paralegal in the Office of Privacy and Information Appeals at the DoJ in Washington, D.C. She analyzed DoJ records requested under the Freedom of Information Act and determined whether the documents could be released. She helped in processing Freedom of Information Act appeal cases in which justification for or against the release of classified information was discussed in her presence by law enforcement, policy, and intelligence officials from the FBI, the CIA, the NSA, and the National Security Council. She also wrote related affidavits for court, responded to congressional inquiries, conducted training seminars, and reviewed classified information for possible declassification. She worked at the DoJ for nearly 6 years, and it was during this time that Montes first ventured into the world of sources and methods, counterintelligence investigations, policy debates over disclosure, and declassification of classified information.

(S//NF) <sup>DIA (b)(6)</sup>



## (U) Introduction to Espionage

(S//NF) According to <sup>CIA (b)(1), 1.4(c)</sup>, ONCIX Montes Damage Assessment Team analysts, FBI investigators, and DIA counterintelligence officials, her decision to spy was coolly deliberate. The traitorous decision to betray her country was based on a combination of factors including an ingrained hostility toward U.S. policy on Latin America; an immature, self-serving personality aimed at retaliation against authority; and a misguided sense of morality.

(S//NF) The activities of a Cuban access agent at Johns Hopkins provided the impetus that launched Montes' career in espionage. The access agent, a fellow student, apparently aware of Montes' criticism of U.S. policy in Latin America, made a "soft pitch" to her in the summer of 1984. The agent asked whether Montes would be willing to meet some friends who were looking for someone to translate Spanish language news articles about Nicaragua into English. The friends turned out to be a Cuban intelligence official at the Cuban Mission to the United States in New York City. At dinner in New York City in December 1984, Montes unhesitatingly agreed to work through the Cubans to "help" Nicaragua. She agreed to provide the Cubans with a short autobiography and to visit Cuba as soon as practical. In March 1985, Montes traveled to Cuba via Madrid, Spain, and Prague, Czechoslovakia, for her first clandestine trip as an espionage agent.

(S//NF) In a series of debriefings following her arrest and conviction, Montes said that the Reagan Administration's 1980s regional policy of opportunism led to the



Grenada intervention in 1983. That event crystallized her negative views on U.S. foreign policy. She said that the United States backed the wrong side in the wars in Central America in the 1980s, and she supported the leftist insurgents in El Salvador and Guatemala. She believed that the United States did not respect the countries of Latin America and caused the death of people "who didn't deserve to be killed." In her view, Cuba was victimized by U.S. repression and she concluded that she had the "moral right" to provide information to Cuba. Throughout her career as a clandestine agent, she believed that, "destiny was offering me an opportunity to do everything that I could to help Cuba." She often exclaimed, "I couldn't give up on the people I was helping." In sum, she indicated that she "felt morally rewarded."

(S//NF) Montes saw U.S. support for the Contras in Nicaragua as unjust and wrong. She had a negative impression of U.S. policy on Cuba, believing that Cuba was not an enemy of or even a threat to the United States. She believed that the fall of the Soviet Union increased the probability that the United States would invade Cuba. She said, "If the United States could invade Panama for no justifiable reason, then they could just as easily invade Cuba and take advantage of their weakness." In her view, Cuba needed her help to defend itself. She believed that U.S. policy was to try to destroy Cuba or force it to change the way it functions. She admired Castro, believing that he was a nationalist who would not have gone "running into the hands of the Russians" if the United States had not tried to overthrow his regime. Montes claimed that she was not a Communist but that she strongly sympathized with the socio-economic goals of both the Cuban and Nicaraguan revolutions. She claimed that her world view was similar to that of Castro. She continually emphasized that she tried to avoid expressing her political views while at work to minimize suspicion. The ONCIX Montes Damage Assessment Team noted that although many of her colleagues in the Intelligence Community were aware of her views on Nicaragua and Cuba, none apparently believed that they were extreme enough to worry about.

(S//NF) Montes claimed that her sensitivity to DoD IG: (b)(6), helped drive her decision to work "with" the Cubans. Montes never suggested that she worked "for" the Cubans. She noted that her relationship with the Cubans was one based on mutual respect and understanding. According to her, the Cubans were thoughtful of her, were dedicated to their cause, and sensitive to her needs. In short, Montes indicated that the Cubans "were very good to me." She was a "comrade in the struggle" against the United States policy on Cuba, whose government "hurt no people." She knew that helping Nicaragua and Cuba was a violation of the law, but stated, "My sense of moral obligation persuaded me that this is what I had to do or I could not live with myself." She said, "I was really doing something that was right." She also stated that she would have rejected any offer by the Cubans to pay for her services.<sup>3</sup>

<sup>3</sup> (S//NF) FBI: (b)(1), 1.4(e), (b)(3), 50 U.S.C. § 403-1(j)(1)



## (U) Joining the Defense Intelligence Agency

(S//NF) Following her recruitment by the Cubans in late 1984 and her first clandestine trip to Cuba in March 1985, Montes realized that she would need a job with access to classified information on the civil war in Nicaragua if she were to help the people of Nicaragua. The classified information she had access to at the DoJ was narrow in scope and historical in nature. She could not obtain unfettered access to classified information at her workplace; she was allowed to review particular documents only when her duties required such access.

(S//NF) Montes continuously and vehemently argued that the Cubans had no role in directing her to find work at the DIA. However, as part of the early 2002 plea bargain negotiations, Montes' counsel provided an attorney proffer that she was specifically targeted by the Cubans to apply for a position at the DIA and that they assisted her in preparing her application. In June 1985, a Johns Hopkins graduate, whom Montes said she did not previously know, helped to get her interviews with hiring officials at the DIA. After two interviews she was offered and accepted a position as an entry-level [REDACTED] DIA (b)(3), 10 U.S.C. § 424

[REDACTED] DIA (b)(3), 10 U.S.C. § 424. Montes began her employment with the DIA in September 1985. Prior to her departure from the DoJ, one official suggested that Montes was disloyal to the United States because of her opposition to U.S. policy on the war in Nicaragua. When questioned by the Defense Investigative Service 8 months after her arrival at the DIA, she claimed that as a citizen she had the right to disagree with the policies of her government. Throughout her tenure at the DIA, she claimed that she never advocated the overthrow of the U.S. Government. DIA security records indicate that in 1996, only one DIA employee expressed concern about Montes, and that a DIA security review found insufficient reason for further review or investigation.

(S//NF) At DIA, Montes was considered a stellar employee who was well regarded professionally by supervisors and many of her peers in the Intelligence Community. Although she indicated that she believed she may have been hired by the DIA because of her academic background, her ability as a Spanish linguist, and her gender, she stated that when she began her career at the DIA, "I did not know the difference between a corporal and a colonel, and I'm not kidding. I didn't even know which Service was wearing the green uniform and which Service was wearing the blue..." She was a quick learner, however. She took advantage of training courses offered by the DIA and other agencies and visited U.S. military bases to hone her skills as a military analyst. Over time, she drew rave reviews from DIA management, many of whom stated that whenever a tough job surfaced, Montes was chosen to resolve the issue.

(S//NF) Other Intelligence Community analysts and managers outside the DoD did not give her such high marks and did not refer to her as "Ms. Cuba," a view held, sometimes grudgingly, with a mixture of jealousy, by many DoD officials.

<sup>4</sup>(S//NF) Concurrent with her application for employment with DIA, Montes applied for positions at the Disarmament Committee at the Library of Congress Federal Research Division and the Naval Investigative Service (now Naval Criminal Investigative Service). The Naval Investigative Service rejected her application and the Federal Research Division offered her a position after she had committed to DIA. Earlier, she had applied for a position as a Latin American specialist with the Arms Control and Disarmament Agency but never received notification from that agency on the status of her application.



Montes was considered a loner who, at times, was emotional and unyielding in her views on Latin American political and military affairs. She exhibited a rigid posture which manifested a superiority complex. One coworker described her as a different kind of person who kept to herself. Unbeknownst to her, she was given the nickname, "la otra," which in Spanish means, "the other" or "the outsider."

(S//NF) Throughout her career at DIA, Montes had access to agency decision makers, intelligence collectors, operational plans, sensitive programs, and military exercises. From October 1985 through June 1988, she was a <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED], Directorate for Foreign Intelligence; and from July 1988 until mid-1993, she held a similar position as a <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]. She assumed the portfolio for Cuba in 1993 and remained focused on Cuban issues until her arrest in September 2001. At various times in her career, her areas of responsibility included the Dominican Republic, Guatemala, Brazil, and Panama. As an intelligence analyst, Montes was responsible for assessing military and political issues and armed forces capabilities. She prepared reports, articles, and briefings, and represented DIA in numerous interagency forums associated with her area of expertise. Among countless other enterprises, she briefed the President-elect of Nicaragua,<sup>5</sup> congressional leaders and members of their staffs; she was a member of the <sup>DIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED] that focused on innovative options for targeting Cuba; she participated in the construct of the National Human Intelligence Collection Directives on Cuba; and she served as an expert analyst in the National Military Joint Intelligence Center in the aftermath of the 1996 shoot down of Brothers to the Rescue aircraft.

(S//NF) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]  
<sup>DIA: (b)(1), 1.4(c)</sup> [REDACTED]

<sup>5</sup> (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(6)</sup> [REDACTED]

<sup>6</sup> (U) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

<sup>7</sup> (U) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

Montes traveled extensively in her official capacity and found enough opportunity to visit foreign countries for personal vacations as well as to satisfy her clandestine commitments to her Cuban handlers.<sup>8</sup>

(U//FOUO) Montes' reputation as a skilled briefer is well documented. She received accolades for a variety of presentations given to senior U.S. and foreign officials, such as the:

- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]
- DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]

(S//NF) During her 16-year career at DIA, Montes received DIA: (b)(3) promotions, a multitude of performance awards, and letters of commendation for high achievement. She also attended a variety of courses of instruction that enhanced her professionalism. A noteworthy accomplishment occurred in 1993 when she participated in the DCI Exceptional Analyst Program. CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6 [REDACTED]

[REDACTED] In 1997, she was named a recipient of the DCI National Intelligence Certificate of Distinction. She said she was treated well at DIA and never felt "looked down upon." She said the awards and promotions she received were somewhat embarrassing, given that she had devoted her life to working against the U.S. Government.

## (U) Portrait of a Spy

(S//NF) Ana Montes was arrested by agents of the FBI at the Defense Intelligence Analysis Center, DIA, Washington, D.C., on September 21, 2001. The arrest brought an end to her 22-year career in government service, more than 16 years of which were devoted to espionage activities in support of Cuba. By many DIA: (b)(1), 1.4(c) [REDACTED]

<sup>8</sup>(U) See Appendix A for a comprehensive listing of Montes' official and unofficial travel.



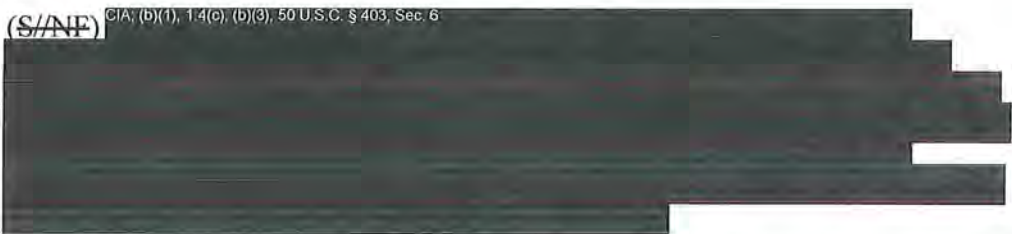
was subsequently charged with conspiracy to commit espionage in violation of 18 U.S.C. section 794(a) and (c):

...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 objects of this conspiracy in the District of Columbia and elsewhere, all in violation of 18 U.S.C. § 794(c).

Montes pleaded guilty to one count of the indictment on March 19, 2002, and on October 16, 2002, she was sentenced to 25 years in prison. By entering a plea agreement, Montes knowingly and voluntarily waived her right against self-incrimination as guaranteed by the Fifth Amendment to the Constitution of the United States, and she agreed to cooperate truthfully, completely and forthrightly in any manner that the U.S. Government deemed relevant. She is currently serving that sentence in the Carswell Federal Medical Center, Fort Worth, Texas. Currently scheduled to be released from prison in 2023, at the age of 66, Montes will be on supervised release for a period of 5 years with several restrictive conditions.


(U//~~FOUO~~) Unlike Aldrich Ames and Robert Hanssen, Ana Montes was not motivated by greed, frustration over poor work, low self esteem, reckless behavior, lack of judgment, infidelity, fascination with the art of espionage, or other frailties. Ames was a CIA intelligence officer who reportedly received up to \$2.5 million from his Soviet/Russian handlers over a 9-year period; he was arrested in February 1994 on charges that he conspired to commit espionage and evade taxes. Robert Hanssen was an FBI Supervisory Special Agent who received more than \$600,000 from his Soviet/Russian handlers spanning three distinct periods (1979-81, 1985-91, and 1999-2001) over more than 20 years. He was arrested in February 2001, just 2 months before his mandatory retirement date. Nonetheless, Montes did share some personal characteristics with Ames and Hanssen: poor interpersonal skills, a sense of intellectual superiority, and a dour demeanor. Yet overall, the portrait of Ana Montes is much different from that of her fellow traitorous felons.

(S//NF) <sup>CIA, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>



(S//NF) Montes appeared to fit what might be considered the stereotypical mold for a spy <sup>CIA, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>. We found no credible evidence that she accepted payments from the Cubans that would approximate the amounts that Ames and Hanssen received from the Soviets/Russians. Her ideological

<sup>9</sup> (S//NF) <sup>CIA, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>



disposition fostered a negative view of U.S. foreign policy, and that fixation, coupled with her sense of moral righteousness, sealed her commitment to a cause from which there was no alternative, at least in her mind. In the final analysis, Ana Montes may well have been the prototypical spy. She was intelligent, professional, self-assured, and respected, but not universally liked in the workplace. She was also a major contributor to the success of an organization and a quiet, frugal, and unassuming neighbor. One DoD counterintelligence official echoed the words of many Intelligence Community officials that we interviewed: "We only really catch the dumb spies, and the only reason we caught her is because we got lucky."



## (U) Part III. Government Service and a Commitment to Espionage

(S//NF) From 1979 to 1994, the unfolding drama of Ana Montes' life takes her from a naïve college student infatuated with leftist social causes, to a respected, professional intelligence officer with the U.S. Government, to a valued espionage agent for Cuba. She discovered her destiny as a "champion" of the downtrodden in a meeting with a Cuban intelligence official in 1984. She immersed herself in espionage for the Cuban Intelligence Service which, along with her dedication to her duties as an intelligence analyst for the DIA, served to mask her psychological insecurities. She began her espionage career with a clandestine trip to Cuba where she received tradecraft training from the Cuban Intelligence Service. She later secured employment as a Latin America intelligence analyst with the DIA, a position which would later pay significant dividends to her Cuban masters. Her early years at the DIA included training as a <sup>DIA (b)(3), 10 U.S.C. § 424</sup> [REDACTED]. During this period, she successfully navigated two security background investigations and one polygraph examination. Her double life as a Cuban espionage agent necessitated frequent clandestine meetings in the Washington, D.C., area with her Cuban handlers, and a second clandestine trip to Cuba. <sup>DIA (b)(1), 1.4(c)</sup> [REDACTED]

[REDACTED] The success of her espionage efforts was recognized in 1989, when she was awarded a medal by the Cuban Intelligence Service.

(S//NF) As a DIA analyst, she also continued to impress her superiors as she was regularly promoted and received glowing performance appraisals. In 1990, she <sup>DIA (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(6)</sup> [REDACTED]

(S//NF) <sup>FBI (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-10(i)(1)</sup> [REDACTED]

## (U) Initial Government Employment

(S//NF) Ana Montes began her career with the U.S. Government in December 1979 as a clerk typist in the Office of Privacy and Information Appeals, at the DoJ in Washington, D.C. The FBI completed an applicant investigation on her in March 1980. This personnel security investigation was entirely favorable, with sources describing Montes as loyal, very moral, extremely independent, with a flawless reputation and compassionate personality. Based on the investigative results, she was adjudicated eligible for Top Secret/Sensitive Compartmented Information (SCI) access. She was assigned

duties as a paralegal specialist to analyze DoJ records requested under the Freedom of Information Act and to determine whether documents should be released. She also wrote related affidavits for court, responded to congressional inquiries, conducted training seminars, and reviewed classified information for possible declassification. During her more than 5-year employment at the DoJ, she enrolled in a graduate degree program at Johns Hopkins. She attended classes from September 1982 to the spring semester 1984, when she completed the course requirements for a Master of Arts degree in International Economics and Latin American Studies. While attending Johns Hopkins, she worked as an unpaid staff writer for a newsletter published by the school's Center of Brazilian Studies.

### **(U//~~FOUO~~) Recruitment by the Cuban Intelligence Service-Moral Imperatives Justify Treason**

(S) Ana Montes gained her first real insight into what she described as the cruel and inhumane nature of U.S. Government policy supporting the Contra rebels in Nicaragua during her graduate studies at Johns Hopkins. She had not been politically aware during her undergraduate years, although she had been attracted to the social Communist parties in Europe during her junior academic year in Spain in 1978. She described herself at the time as a leftist, but not a follower of classic Marxist orthodoxy. Her graduate coursework at Johns Hopkins included extensive study of Latin American history and U.S. policy in that area, as well as discussions about economic and political affairs. Most of the other students and professors at Johns Hopkins shared her views about the unjustness of U.S. policies, particularly regarding the Contras. It was in this atmosphere that she developed a sense of moral outrage at the U.S. participation in the hostilities in Nicaragua. She saw the United States as waging a war against that country, killing innocent people, and attempting to overthrow a legitimate government, all of which, in her opinion, was reprehensible. The U.S. invasion of Grenada in 1983 confirmed this "personal worldview." <sup>DIA: (b)(1), 1.4(c), (b)(6)</sup>

[REDACTED]

(S) Montes expressed her moral indignation about U.S. actions in Nicaragua in informal discussions with fellow Johns Hopkins students. One of these classmates professed sympathies for the Nicaraguan people much like those of Montes. <sup>DIA: (b)(1), 1.4(c), (b)(6)</sup>

[REDACTED]

(S) <sup>DIA: (b)(1), 1.4(c), (b)(6)</sup>

[REDACTED]



DIA: (b)(1), 1.4(c), (b)(6)



(S) DIA: (b)(1), 1.4(c), (b)(6)


the Cubans, Montes emphasized that a "force of destiny" or fate intervened at just the time she was experiencing moral outrage with U.S. policies. She commented again and again: "They (the Cubans) came to me, they came to me." She was being asked to help a people who were in dire jeopardy, and she could not morally refuse; this was a situation when moral principle took precedence over the laws of a nation.

(S) In April 1985, while still employed at the DoJ, Montes and


DIA: (b)(1), 1.4(c), (b)(6)



<sup>10</sup> (S//NF) DIA: (b)(1), 1.4(c)



<sup>11</sup> (S//NF) DIA: (b)(1), 1.4(c)





Although it was apparently not on the formal training schedule, the Cubans

<sup>DIA (b)(1), 1.4(c)</sup>

[REDACTED]

### (U//~~FOUO~~) Valuable Asset for the Cubans

(S//NF) Whether Montes was targeted against the DIA by the Cubans or whether she decided entirely on her own to apply to that agency, she could not have achieved a more valuable placement than the DIA <sup>DIA (b)(3), 10 U.S.C. § 424</sup> where she could report on U.S. military capabilities and intentions toward Cuba and its interests. One of the primary collection priorities of the Cuban Intelligence Service was, and continues to be, information on U.S. plans and intentions toward Cuba and the Americas. As the DoD agency responsible for providing all-source intelligence analysis and collection management support to the Secretary of Defense (SECDEF) and the Chairman of the Joint Chiefs of Staff, the DIA is a major focus for intelligence collection and analysis on Cuba. A mole such as Montes in the DIA could afford the Cuban Intelligence Service excellent insight into U.S. military knowledge of the Cuban Armed Forces and possible forewarning of operational planning affecting Cuba.

(S//NF) Montes was highly regarded and carefully handled by the Cubans; she maintained that the Cubans did not control her, nor did they use her for tasking purposes. She told them what she was willing to do and how she was going to do it. When she had a parting of the ways with her close friend and fellow asset in approximately 1988, the Cubans went to special lengths to assure Montes that they had complete confidence in her. Montes noted that her relationship with the Cubans was one based on mutual respect and understanding. According to Montes, the Cubans were thoughtful of her, were dedicated to their cause, and sensitive to her needs. In short, the Cubans "were very good to me." She stated that she would have rejected any offer by the Cubans to pay for her services.

### (U) Background Developments at DIA

(S//NF) Following the Vietnam era in the 1970s, the DIA was subjected to severe personnel reductions. However, during the Reagan Administration, the agency grew rapidly. From 1981 to 1985, the Director, DIA expanded <sup>DIA (b)(3), 10 U.S.C. § 424</sup> capabilities within the agency. As insurgency developed in Central America, <sup>DIA (b)(3), 10 U.S.C. § 424</sup> were increased to focus on that region. For example, in 1982 and 1983, the specialized <sup>DIA (b)(3), 10 U.S.C. § 424</sup> was organized and rapidly grew from <sup>DIA (b)(3), 10 U.S.C. § 424</sup> civilian and military personnel. The <sup>DIA (b)(3), 10 U.S.C. § 424</sup> received intelligence analytical support from the <sup>DIA (b)(3), 10 U.S.C. § 424</sup> to which Montes was assigned upon her arrival at the DIA.

## (U) DIA Applicant Processing

(S//NF) Montes initially applied for an [REDACTED] position with the DIA in June 1985. She later claimed, during post-arrest debriefings, that she had contacted an alumnus from her graduate school who was working at the DIA to obtain the name of the person who was in charge of the [REDACTED]. [REDACTED] Montes contacted that individual and arranged an interview, after which the individual asked her to formally apply for a position with the DIA. When Montes submitted her job application, she indicated that she wanted to leave the DoJ to obtain "work related to career interests." Throughout her post-arrest debriefings, she consistently claimed that she could not recall that the Cubans attempted to direct her to seek employment with the DIA. Rather, she decided to apply for a position that would give her access to information of value for Cuban support to the Sandinista regime.

(S//NF) On her application form submitted to the DIA Personnel Office in June 1985, Montes indicated that she had obtained a Master of Arts degree in International Relations from Johns Hopkins in June 1984. She also indicated that [REDACTED]

(1975-1979). The Personnel Office formally notified the Personnel Security Division on July 12, 1985, of the nomination of Montes as a candidate [REDACTED]. This notification launched the prospective employee security vetting process. As part of routine applicant processing, the Personnel Office also obtained written recommendations from previous employers. Many former supervisors at the DoJ uniformly assessed Montes as an outstanding employee.

(S//NF) In August 1985, the DIA Personnel Security Division conducted the initial personnel security review of Montes' eligibility for employment, including an adjudication of her 1980 FBI background investigation and a pre-employment interview. [REDACTED]

(S//NF) Although DIA did not use Counterintelligence Scope Polygraph (CSP) examinations or psychological assessments in its hiring process at the time of Montes' application, she was notified in the Conditions of Employment statement, which she signed on June 28, 1985, that "Initial employment or continued employment is subject to a satisfactory personnel security background investigation and reinvestigation, required medical examination, interviews, and such other procedures deemed necessary to assure Agency security, suitability, and qualifications standards are met." After another adjudicative review, the Personnel Security Division notified the Personnel Office on August 23, 1985, that no objections were interposed to a formal job tender to Montes, and that she would be eligible for an interim Top Secret clearance at the time of her entry on duty with the DIA.



## (U) DIA Personnel Security and Clearance Adjudication Practices for New Employees

(S//NF) On September 30, 1985, Ana Montes entered on duty with the DIA as both a novice ~~(b)(3), 10 U.S.C. § 424~~, and a fully recruited, trained penetration agent of the Cuban Intelligence Service. Her initial assignment at the DIA was in the ~~(b)(3), 10 U.S.C. § 424~~

~~(b)(3), 10 U.S.C. § 424~~ She was granted an interim Top Secret clearance pending completion of a background investigation which was initiated by the Personnel Security Division on October 2, 1985. Montes signed a Classified Information Nondisclosure Agreement certifying that she had been given a security indoctrination on her obligation, under applicable Executive Orders and public laws, to protect classified information. Also during her first month of employment, her supervisor and the Unit Security Officer briefed Montes on DIA security procedures.

(S//NF) Unlike other major Intelligence Community agencies, such as the CIA and NSA, the DIA did not routinely use applicant polygraph screening or psychological testing. During September 1985, the DIA Personnel Security Division was establishing and staffing a polygraph capability. However, civilian employees, military personnel and contractors affiliated with the DIA were subjected to the most stringent background investigative requirement as set forth by the DCI. The results of the background investigations, as well as in-house security investigative scrutiny, where appropriate, formed the basis for evaluating an employee's initial and continuing eligibility for access to classified information.

(U//FOUO) In early 1986, the ~~(b)(3), 10 U.S.C. § 424~~ formally requested that the Personnel Security Division certify Montes as eligible for expedited SCI access on a compelling need basis prior to completion of her background investigation. A statement of justification for the request noted that intelligence support for U.S. policy makers and the large military assistance programs for El Salvador necessitated full use of the limited number of analysts in the ~~(b)(3), 10 U.S.C. § 424~~. Montes had been given access to classified material at the Secret and Top Secret levels since she arrived at the DIA. Provisions for granting a waiver of the investigative requirements for SCI access are contained in the DCI Personnel Security Directive, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (DCID 1/14)," November 1984, and are implemented by Intelligence Community security officials.

(U//FOUO) While the waivers for SCI access are not routinely granted, they are not unusual. Normally applied to newly hired personnel who lack a current investigation, the approval of an SCI waiver depends on available security information. In the case of Montes, her investigation five years earlier, along with a pre-employment security interview, and partial National Agency Checks conducted by DIA exceeded the DCI requirements for a waiver. Thus, the Personnel Security Division authorized SCI eligibility and Montes was formally indoctrinated for such access on February 5, 1986.

(S//NF) In June 1986, Montes' supervisor provided written certification to the Personnel Security Division that he was not aware of any reportable security problems concerning her. This annual management certification was required by DoD Regulation 5200.2-R, "Personnel Security Program," January 1987, which sensitized supervisory officials to employee behavior problems with security implications, such as alcohol abuse, financial difficulties, unfavorable involvement with law enforcement agencies, mental and emotional problems, or foreign contacts or drug use. Also in June 1986, the background investigation initiated shortly after Montes' entry on duty at the DIA was completed.

(S//NF)

<sup>DIA: (b)(1), 1.4(c), (b)(6)</sup>

[REDACTED]

(S//NF)

<sup>DIA: (b)(1), 1.4(c), (b)(6)</sup>

[REDACTED]

(S//NF) When the Defense Investigative Service agent broached the issue of her loyalty, Montes strongly professed her loyalty as a U.S. citizen who had never advocated the overthrow of the U.S. Government, and further mentioned that she had never been a member of any subversive group. She explained that, as a result of her extensive political discussions in school, she had often expressed views critical of certain U.S. policies, but those criticisms were fully within her rights under the Constitution. Montes would later admit during post-arrest debriefings that she realized early on in her DIA career, particularly after the June 1986 Defense Investigative Service interview, that she had to be much more careful in expressing her opinions on U.S. policy than she had been as a graduate student.

(S//NF) The Personnel Security Division adjudications staff conducted a full security evaluation of Montes as a DIA employee in July 1986 based on the results of the completed Defense Investigative Service background investigation



and other documentary material created during her initial 9 months of employment. DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(6)



(S//NF) On July 10, 1986, DIA: (b)(3), 10 U.S.C. § 424, directed that a written case referral action be staffed to the Personnel Office, the General Counsel, and appropriate management for possible probationary firing of the employee. A Personnel Security Division supervisory official later discussed the referral with the DIA: (b)(3), 10 U.S.C. § 424, who advised that the case was not sufficiently actionable for probationary dismissal of Montes. As a result of that advice, the DIA: (b)(3), 10 U.S.C. § 424 decided not to pursue a formal written referral, and Montes was therefore certified eligible for SCI access. She had been functioning on a temporary SCI waiver since September 1985.

## (U) The "Night Job" Picks Up

(S//NF) As Montes settled in as a new DIA: (b)(3), 10 U.S.C. § 424, she increased the frequency of her clandestine meetings with the Cubans. The meetings initially took place in New York City, usually at restaurants selected by the Cubans. Her Johns Hopkins classmate accompanied her to at least two meetings. Montes became concerned about traveling to New York City by train to meet with her Cuban handler. She asked the Cubans to send someone not affiliated with the Cuban Mission to the United Nations to meet with her in the Washington, D.C., area. Beginning in approximately January 1986 and continuing through late 1998, Montes met with Cuban handlers in Metropolitan Washington, D.C. She specified certain areas where she was unwilling to meet because she was fearful of street crime; she was not comfortable in the downtown area. The Cubans accommodated her request with the stipulation that meeting sites, normally restaurants selected by them, had to be close to a Metrorail station. Those contacts took place once every 2 to 3 weeks, normally on the weekends.

(S) Montes decided early on that, to avoid detection, she would never remove any classified information from DIA workspaces. She believed that she would not leave a paper trail if she communicated intelligence information to the Cubans by memorizing her recollections. DIA employees confronted defensive physical security measures on a daily basis because security guards conducted random inspections of bags and packages carried into and out of DIA facilities. These measures reinforced Montes' belief that it would be unwise to take any classified material out of her workplace.

(S) Significantly, this scheme played to Montes' grandiose perception of herself as a comrade-in-arms with the Cubans. By passing classified information



verbally and constructing notes from memory, Montes saw herself as an equal with her Cuban comrades, not as a menial espionage tool extracting classified documents from "enemy" installations. She informed the Cubans that she had no intention of passing intelligence information on countries other than those in which she had an interest, primarily Nicaragua and later Cuba, and she would not attempt to gain access to classified information that was not within her purview. In large measure, Montes decided what sensitive intelligence she would provide to the Cubans and how she would provide it, which meant that she would not be amenable to tasking that did not relate directly to her assigned duties. In her mind, these conditions gave Montes significant control of her espionage activities. However, Montes consistently left security matters such as meeting site security, counter surveillance, and transmission security to the Cubans.

### (U) Sharpening Skills as a DIA Analyst-1986-1990

(U//FOUO) Much of the first year of Montes' employment at the DIA consisted of waiting for full SCI access approval and taking required analyst training. From January to May of 1986, she completed the [REDACTED] [DIA (b)(3), 10 U.S.C. § 424, (b)(6)]

[REDACTED] In June 1986, her supervisor rendered her initial performance appraisal. Although rating her as [REDACTED] [DIA (b)(6)] he noted that she did not have the opportunity to fully demonstrate her potential because of security and training factors. He commented that her high intelligence and positive attitude presaged higher ratings when she achieved full time performance in her field. Montes was [REDACTED] [DIA (b)(3), 10 U.S.C. § 424] promoted from [REDACTED] [DIA (b)(3), 10 U.S.C. § 424] in October 1986. One month later, the directors of the Defense Security Assistance Agency and the DIA congratulated her for her outstanding assistance as an interpreter at a Defense Security Assistance Agency conference with representatives of the El Salvadoran Armed Forces. Montes took her first official overseas travel as a DIA employee in January and February of 1987 when she traveled to El Salvador (5 weeks) and Guatemala (1 week) in conjunction with an analyst area orientation program. Her annual career appraisal for the period July 1986 through June 1987 rated her as [REDACTED] [DIA (b)(3)] which was higher than the previous appraisal. She was again [REDACTED] [DIA (b)(3), 10 U.S.C. § 424] promoted to [REDACTED] [DIA (b)(3), 10 U.S.C. § 424] in November 1987. Montes continued to expand her analytic knowledge by taking several DIA technical courses as well as a 3-day Signals Intelligence (SIGINT) orientation course at the NSA. She produced a number of intelligence research papers on El Salvador and Guatemala during the period August 1987 to November 1988, works which were described by her supervisor as praised by policy makers, the Military Departments and the Intelligence Community for their timeliness and clarity. Her supervisor also provided written certification to the Personnel Security Division during the annual rating cycles in 1987 and 1988 that no reportable security problems had been noted regarding Montes' job performance. When she received her annual appraisal in June 1988, she had so impressed her superiors that she received the [REDACTED] [DIA (b)(6)] The rating review official noted that she was clearly one of the most capable analysts in the office and had high potential. In December 1988, Montes was [REDACTED] [DIA (b)(3), 10 U.S.C. § 424] promoted to [REDACTED] [DIA (b)(3), 10 U.S.C. § 424]. In the space of 3 years, she was promoted [REDACTED] [DIA (b)(3), 10 U.S.C. § 424], but it would be more than 10 years before she was promoted again.

(S//NF) Montes described her working conditions at the DIA as superb; she had no disharmonious relationships, and believed that she was granted more than



ample support and recognition. In July 1989, she received her second consecutive performance appraisal, in which she was cited for producing a

DIA: (b)(6)  
DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(6)

rating, with a recommendation for a Quality Salary Increase. Her superiors also nominated her for the DIA Meritorious Civilian Service Award. She received the award in a formal ceremony on December 3, 1990.

### (U//~~FOUO~~) ...And as a Cuban Clandestine Reporting Source


(S//NF) As Montes improved her skills as an intelligence analyst, she was also learning the intricacies of the Cuban spy trade. The first years of her clandestine activity were the most difficult for her. She had to adapt her persona in the workplace to blend in with hardworking analysts. She exercised care not to voice personal beliefs, as she had in graduate school, about U.S. policies in Central America. As a matter of self-discipline, she tried very hard not to say or write any comments that she could not validate with available intelligence information. Additionally, she believed that the DIA could monitor and trace its employees' computer use, so she was careful to search classified systems for topics and reporting that she could explain as being within her legitimate area of analytical responsibility.

(S//NF) In actual fact, the DIA ~~\_\_\_\_\_~~, which is responsible for the integrity of the Joint Worldwide Intelligence Communications System, a secure intelligence platform used by the DoD worldwide.

DIA: (b)(1),  
1.4(c), (b)(3),  
10 U.S.C. §  
424, (b)(7)(E)

(S//NF) Between 1986 and 1989, Montes had to adapt to a variety of handlers and to changes in operational tradecraft procedures and paraphernalia. For example,

DIA: (b)(1), 1.4(c)

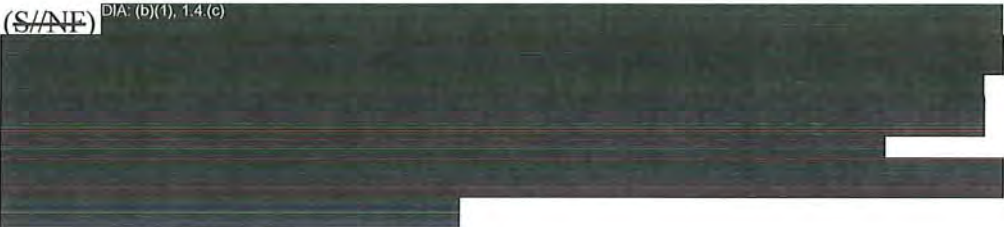


**(U//~~FOUO~~) A Second Clandestine Trip to Cuba**

(S//NF) DIA: (b)(1), 1.4(c)



(S//NF) DIA: (b)(1), 1.4(c)



**(U) Security Reinvestigation - 1991**

(U//~~FOUO~~) In March 1991, the DIA Personnel Security Division notified Montes that she was scheduled for a Periodic Reinvestigation. A Periodic Reinvestigation for DIA civilian employees, military personnel and contractors is based on the DCID 1/14 requirement that all personnel with continuing access to Top Secret/SCI be reinvestigated on a recurring 5-year cycle. The Periodic Reinvestigation covers an individual's life history since his or her previous investigation, whereas an initial Background Investigation covers a 10-15 year



period. Additionally, the Periodic Reinvestigation has less extensive investigative coverage.

(U//~~FOUO~~) On the Personnel Security Questionnaire that Montes submitted for the Periodic Reinvestigation, she indicated that she had paid her debt to Johns Hopkins and was formally granted her Masters of Arts degree in 1988. She also reiterated her ~~(b) (6)~~ prior to DIA employment; she had admitted to ~~(b) (6)~~ on her 1985 DIA application papers. The Defense Investigative Service completed the Periodic Reinvestigation of Montes in September 1991. Johns Hopkins records confirmed the award of her Master of Arts degree. Five coworker and supervisory references who were contacted by Defense Investigative Service investigators commented favorably on her.

(U//~~FOUO~~) Montes was extensively interviewed on two occasions during the reinvestigation by Defense Investigative Service agents. The first interview was wide-ranging, covering such security topics as her official and unofficial foreign travel, foreign contacts, drug use, and finances. She admitted that she had inaccurately reported ~~(b) (6)~~ when she initially applied for a position with the DIA in 1985. She explained that she had told DIA authorities that she ~~(b) (6)~~ once in 1979, when the use actually took place in 1982 while she was an employee of the DoJ. She further explained that she had misrepresented the incident out of concern that she would not be hired by the DIA and that she did not understand the seriousness of being honest and truthful at the time. Montes claimed that this misrepresentation had bothered her ever since and she wanted to set the record straight. She denied any personal knowledge of the unauthorized disclosure of classified information or involvement with any hostile intelligence activity. Two days after the interview, Montes contacted the Defense Investigative Service agent to report additional personal information. She said that she had ~~(b) (6)~~ during the summer of 1978 while in Madrid, Spain, for her undergraduate junior year study program. The second interview was conducted to obtain a sworn statement from her on her misrepresentation of facts of her past ~~(b) (6)~~. She claimed that at the time of her 1985 DIA application, she was afraid an admission of ~~(b) (6)~~ would be more detrimental than if she claimed such use had occurred several years earlier. Although she had been a Federal employee in 1982, Montes claimed that she did not have the security awareness at the DoJ that had been instilled in her by the DIA.

(U//~~FOUO~~) The Personnel Security Division conducted an adjudicative review of the Defense Investigative Service Periodic Reinvestigation in October 1991. The review noted that Montes' untruthfulness related not only to ~~(b) (6)~~. The case adjudicator commented that, while Montes seemed to have a tendency to "twist the truth" to her own needs and her honesty was still some cause for concern, adverse security action was unlikely because the original deception had occurred 6 years previously. The adjudicative review concluded that the extensive DIA interviews of Montes should impress upon her the seriousness of her omissions. Her SCI access eligibility was recertified.

(S) In March 1992, approximately 5 months after the Defense Investigative Service Periodic Reinvestigation interview, Montes submitted a Privacy Act request asking for her DIA security case history information back to 1986. Montes was well versed in Freedom of Information Act and Privacy Act




procedures from her previous employment at the DoJ. In accordance with agency Freedom of Information and Privacy Act policy, her case file was reviewed by Personnel Security Division specialists and all investigative material was released to her. Montes later claimed that her request was purely for personal reasons, but that she did photograph the investigative reports and pass them to the Cubans. The Cubans were interested, not so much in the material itself, but that a U.S. Government employee could access her own security history through provisions of the Freedom of Information Act.

## (U) Coupling Analytic Expertise and Espionage Activities

(S) From 1990 to 1994, Montes continued to build her expertise as a DIA analyst and as a Cuban spy. She was highly regarded by DIA supervisors for her professional accomplishments and consistently earned the highest marks on annual performance ratings. She also sharpened her skills through attendance at various advanced training venues and official travel to Central American countries. The second-level supervisor of Montes endorsed her annual <sup>DIA: (b)(6)</sup> appraisal for the period July 1990 to June 1991 with the comment that she was one of the leading Central American analysts at DIA, as well as a leading DoD expert on the region. While this supervisor was aware that her political views leaned to the left, he never questioned her loyalty to the United States. He observed that Montes did not develop close relationships with people at work. When she was thrust into a nonprofessional setting like an office birthday party she would get nervous, fidget, and leave as quickly as she could to get back to work. She was sometimes seen by her peers as cold.

(S) Sometime in 1990, Montes was reassigned within the <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> to work on Nicaragua issues. Although she had been doing some analytical work on Nicaragua while she was assigned to the El Salvador target, she now became a full-time Nicaragua specialist. Montes later commented how ironic it was that she was assigned the Nicaragua portfolio the same year the Nicaraguan people democratically elected Violeta Chamorro president; thus, the basis for her initial moral outrage at U.S. policy toward that country was no longer relevant. She did, however, continue to provide the Cubans with classified information on developments in Nicaragua while she tried to find a way to switch to working the Cuba account, which she achieved in February 1993. Montes explained that her moral realignment from helping Nicaragua via the Cubans to directly helping Cuba stemmed from a realization that the United States might find a pretext to invade that island. The U.S. invasions of Grenada and Panama, along with the reduction of Soviet/Russian military and economic support to the Castro regime after 1991, made it clear to Montes that Cuba was increasingly "in big trouble."

(S) The Cubans put into effect a significant upgrade in reporting and communications protocols for Montes in 1990. Although she had been <sup>DIA: (b)(1), 1.4 (c)</sup>





DIA (b)(1), 1.4(c)

## (U) Exceptional Analyst Program Affords Another Visit

CIA (b)(1), 1.4(c),  
(b)(3), 50 U.S.C. §  
403, Sec. 6

CIA  
(b)  
(1)

(S//NF) In late 1991, Montes was one of seven DIA employees selected to attend an executive development course at George Washington University in Washington, D.C. In 1991 and again in 1992, she also applied for the more advanced executive leadership development course but was not selected. She cited her interest in interagency policy planning as one of the reasons for applying. In July 1992, she attended a 2-week National Senior Intelligence course, which was an element of the career progression track for mid-level analysts. Montes' diligence as a productive member of the [redacted] was also recognized in July when she was again given an [redacted] rating on her performance appraisal, this time with a [redacted]. She ended 1992 with her selection to participate in the prestigious DCI Exceptional Analyst Program. The program was established to stimulate innovative thinking, broaden analytic horizons, and enrich the understanding of individual analysts. [redacted]

She received no assistance from the Cubans in applying for the program or in researching or composing her written proposal. However, after she was selected for the program [redacted]

[redacted] she met with her handler who gave her instructions on clandestine contacts with intelligence officials [redacted].

(S) CIA (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6

CIA (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6

(S//NF) [redacted], Montes was situated to build her professional reputation and eventually achieve status as the preeminent Cuba

analyst in the DoD, and arguably the entire Intelligence Community. Her superiors continued to be impressed with her ability, and rated her <sup>DIA: (b)(6)</sup> on the performance appraisals of 1993 and 1994. Additionally, she was awarded <sup>DIA: (b)(6)</sup> in 1994 for her exceptional analytical accomplishments.

## (U//~~FOUO~~) Montes Encounters and Beats the Polygraph

(U//~~FOUO~~) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup> <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>. As noted earlier, the DIA was establishing a polygraph capability when she began her employment in 1985. DoD policy on the use of the polygraph is included in DoD Directive 5210.48, "DoD Polygraph Program," December 24, 1985. The DoD Polygraph Institute is responsible for oversight of all DoD polygraph-related organizations. The Polygraph Institute provides centralized training, certification, and recertification of DoD polygraphers at its Fort Jackson, South Carolina facility. The Polygraph Institute also manages annual inspections of selected DoD polygraph facilities to ensure that all programs conform to DoD standards. The Polygraph Institute also conducts continuing research on polygraph methodology and issues examiner training material. <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

(U//~~FOUO~~) The DIA can only administer CSP and Security Issue Resolution examinations. CSP examinations consist of an authorized set of questions dealing with espionage, sabotage, terrorism, and unauthorized foreign contacts or disclosures of classified information. Implementation of the polygraph program within the <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

<sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>, the narrative reports of polygraph test results are retained in employee security files for the active life of that file. The actual examination charts, however, are retained for only 90 days. <sup>DIA: (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(3), 50 U.S.C. § 403-1(i)</sup>

<sup>DIA: (b)(3), 50 U.S.C. § 403-1(i)</sup>

(S//NF) <sup>DIA: (b)(1), 1.4(c)</sup>



## (U//~~FOUO~~) Counterespionage Efforts Against Cuba

(S//NF) U.S. Government Human Intelligence (HUMINT) collection operations against the Cuban target suffered a series of setbacks in the years prior to 1990. The Cuban Intelligence Service ran a highly effective double agent program against U.S. intelligence agencies from 1978 to 1987, when a defecting Directorate of Intelligence officer provided information about Cuban Intelligence Service operations and capabilities. Based on this and other reporting, the U.S. Intelligence Community assessed the Cuban Intelligence Service as a first-rate intelligence service with the ability to run highly aggressive operations against U.S. interests throughout the world. The Directorate of Intelligence focused largely on exploiting human sources of information, and its officers showed exceptional proficiency in recruiting and managing agents. The Cuban modus operandi was originally modeled on tradecraft developed by the premier Soviet intelligence service, the Committee for State Security, and the East German Ministry for State Security. The Cubans developed somewhat more flexible operational procedures, such as recruitments generally made on the basis of ideology, not money, and targeting women and Hispanic males for penetration of U.S. Government entities, which had been a long-standing intelligence priority for them.

(S//NF) DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), 50 U.S.C. § 403, Sec. 6, FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

(S) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

FBI; (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

[REDACTED]. Following a National Security Council review of Intelligence Community responses to Presidential Review Directive 44, the president issued Presidential Decision Directive 24, "U.S. Counterintelligence Effectiveness," May 3, 1994. The intent of this Directive was to "...foster increased cooperation, coordination and accountability among all U.S. counterintelligence agencies." To ensure that all relevant departments and agencies exercised the full and free exchange of information necessary to achieve maximum effectiveness of the U.S. counterintelligence effort, Presidential Decision Directive 24 ordered the establishment of a National Counterintelligence Policy Board and a National Counterintelligence Center. The following sections of this report show that the well-meaning intent of Presidential Decision Directive 24 did not inspire counterintelligence entities to cooperate or coordinate; instead interagency rivalries and personal rancor persisted through a major portion of the Montes espionage case.



## (U) Part IV. Maturation as Analyst and Spy

(S//NF) From 1994 to 1998, Ana Montes continued to mature as a DIA intelligence analyst and as a penetration agent for the Cuban Intelligence Service; she was highly valued by both. <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

<sup>CIA: (b)(1), 1.4(c), (b)(3)</sup> she was the "principal product manager and major drafter" <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

During this period, she attended gatherings where academics and Government officials discussed Cuba-related issues. According to Montes, she attended these meetings to expand her understanding of Cuba.

(S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>

She successfully passed a second Periodic Reinvestigation, which recertified her security clearance and access to SCI. These events defined a period when Montes further established herself as a consummate professional in both her public and clandestine lives.

(S//NF) <sup>DIA: (b)(1), 1.4(c)</sup>

<sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> <sup>DIA: (b)(1), 1.4(c)</sup> <sup>CIA: (b)(1)</sup>

(U//FOUO) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

(S//NF) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>

<sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>

<sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>

<sup>12</sup> (U//FOUO) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424

(S//NF)

CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424

(U) For Montes' efforts <sup>CIA: (b)(1), 1.4(c), 50 U.S.C. § 403, Sec. 6; DIA: (b)(3), 10 U.S.C. § 424</sup>, the DCI awarded her the National Intelligence Certificate of Distinction. The Certificate of Distinction is awarded for sustained superior performance of duty of high value or for a single act of specific merit and is one of the highest awards that the DCI can bestow upon a member of the Intelligence Community. The award was presented by then-Deputy DCI George Tenet, and signed by then-DCI John Deutch. The final sentence of the citation stated, "Ms. Montes' strong sense of Intelligence Community responsibility fostered the strengthening of a collegial strategy among analysts working (Cuba), reflecting great credit upon herself and the Defense Intelligence Agency." Montes was recognized as a leader in her area of expertise.

## (U) Attendance at Academic Forums

(S//NF)

DIA: (b)(1), 1.4(c)

<sup>DIA: (b)(1), 1.4(c)</sup>. With the blessing of her supervisory chain, Montes attended meetings of several different academic groups that focused on Cuba. When questioned about Montes' attendance at these meetings, one of her supervisors stated, "Being exposed to multiple ways of thinking makes a person a better analyst."

(S//NF) Ana Montes associated with at least two groups based in Washington, D.C., the Cuba Study Group and the Center for Defense Information (CDI). According to Montes, <sup>DIA: (b)(1), 1.4(c)</sup>


<sup>DIA: (b)(1), 1.4(c)</sup> In 1990, Georgetown University formed the Cuba Study Group. In early 2002, the group moved to Trinity University in Northeast Washington, D.C. According to the group's web site, it "comprises individuals from a wide ideological spectrum drawn from academia, the legislative and executive branches of government, and various non-governmental organizations. All meetings are strictly off-the-record by invitation only." The goal of the Cuba Study Group was to improve the quality of debate on Cuba and Cuba policy. Montes attended Cuba Study Group meetings from approximately 1990 to 1998.

(U) The CDI is a Washington, D.C., think tank with offices in Moscow, Russia and Brussels, Belgium. The CDI was founded in 1972 by retired senior U.S. military officers and is dedicated to strengthening security through international cooperation; reduced reliance on unilateral military power to resolve conflict;



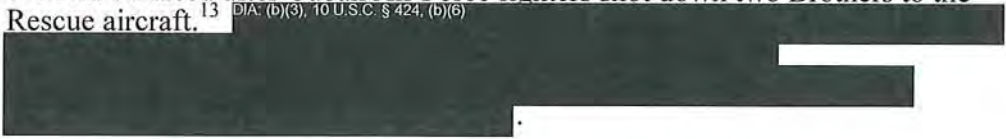
reduced reliance on nuclear weapons; a transformed and reformed military establishment; and a prudent oversight of, and spending on, defense programs. One focus for the CDI is cooperative security between the United States and Cuba.

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c)</sup>

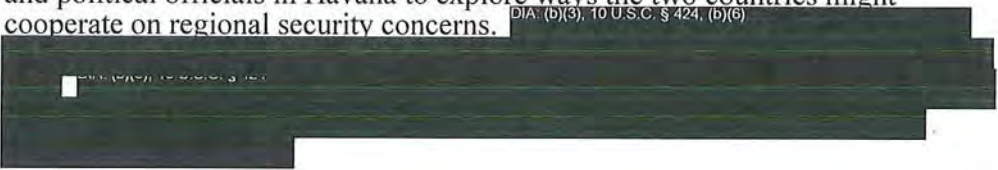


## (U) Events Surrounding the Brothers to the Rescue Incident

(S//NF) DIA had few security concerns about Ana Montes. One significant concern surfaced after Cuban Air Force fighters shot down two Brothers to the Rescue aircraft.<sup>13</sup> <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(6)</sup>




(U//FOUO) In early February 1996, the CDI arranged for several retired American flag officers to tour Cuba. The CDI web site stated that a delegation of U.S. military experts organized by the CDI met every year with Cuban military and political officials in Havana to explore ways the two countries might cooperate on regional security concerns. <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(6)</sup>



(U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup>



(U) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup>



<sup>13</sup>(U) See Appendix C for background on the Brothers to the Rescue incident.

(U//~~FOUO~~) Montes first learned of the incident on the evening of February 24 from <sup>DoD IG: (b)(6)</sup> [REDACTED]. Later that same evening, a senior intelligence officer from her division at DIA called Montes and directed her to report to work the next morning, Sunday, February 25, at the Defense Intelligence Analysis Center. Montes spent most of the morning reading incoming message traffic about the Brothers to the Rescue incident. When she arrived, a coworker and her supervisor were performing similar duties. Late in the morning, they received a call advising that the Joint Chiefs of Staff, J2<sup>14</sup> was forming a task force and requesting that Montes and her supervisor join the group at the Pentagon. They arrived at the Pentagon at approximately 11 a.m. and spent the rest of the day working there. Montes claimed that she was exhausted and left the Pentagon sometime between 8 and 10 p.m. According to the secondhand recollections of a coworker, Montes should have worked until 10 p.m., but received a phone call, became visibly agitated, and left early at 8 p.m. According to the coworker's recollections, he thought her actions were very odd, and they played a role in reporting his concerns about Montes to DIA. Montes spent approximately 2 weeks detailed to the Pentagon. She provided Cuban subject-matter expertise and intelligence support to the Joint Staff Brothers to the Rescue Task Force.

(S//NF) In April 1996, the coworker reported his concerns about Montes to DIA. His concerns related to the Brothers to the Rescue incident and her involvement with academic groups. Montes' coworker surmised that the CDI debriefing and press statement and the Brothers to the Rescue incident were not coincidental. He believed that the Cuban Intelligence Service orchestrated the events to influence U.S. public opinion, and he believed that Montes was involved. The coworker based his concerns primarily upon four facts:

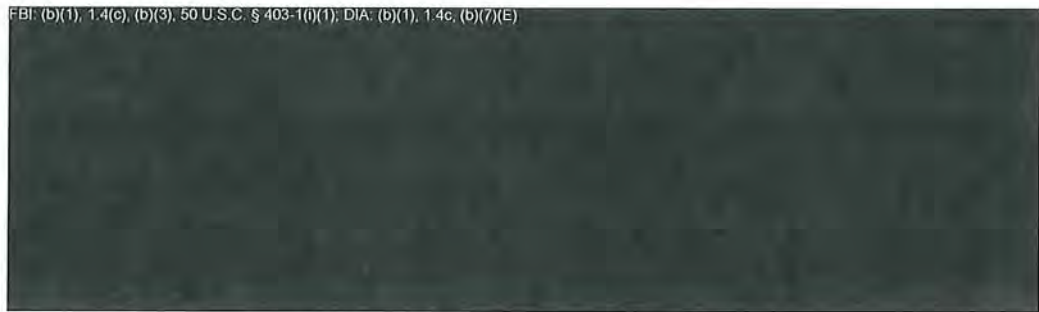
1. Montes had voiced her opposition to U.S. policy toward Cuba in the past;
2. <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-10(i)(1); DIA: (b)(1), 1.4(c)</sup> [REDACTED]
3. Montes arranged a February 23, 1996, debriefing for CDI representatives by U.S. Government employees; and
4. On or about February 25, 1996, a representative of the CDI announced to the press that the U.S. Government shared blame for the Brothers to the Rescue incident.

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-10(i)(1)</sup> [REDACTED]

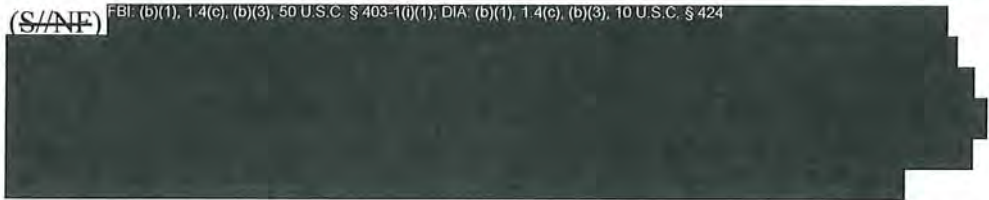
<sup>14</sup>(U//~~FOUO~~) The Directorate for Intelligence, J-2, supports the Chairman of the Joint Chiefs of Staff, the Secretary of Defense, the Joint Staff, and Unified Commands (now called Combatant Commands). It is the national-level focal point for crisis intelligence support to military operations, indications and warning intelligence in the DoD, and Combatant Commands' intelligence requirements.



FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4c, (b)(7)(E)



(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424




(U) On November 13, 1996, the DIA Special Agent interviewed Montes. At first, Montes believed the interview was part of a normal Periodic Reinvestigation for her security clearance. When she realized that the interview related to the Brothers to the Rescue incident, she relaxed and provided satisfactory responses to all questions posed. The DIA Special Agent also interviewed other U.S. Government personnel who had knowledge of the February 23, 1996, debrief meeting with the CDI. The results of those interviews validated Montes' statements. The Special Agent could not substantiate the allegations lodged by Montes' coworker.

## (U) Significant Travel and Recognition

(U) This section focuses on significant events in Montes' professional and clandestine travel from 1994 to 1998 and on the significant recognition Montes received during this period.

(S//NF) CIA: (b)(1), 1.4(c), DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424



(S//NF) DIA: (b)(1), 1.4(c)



(U) DIA: (b)(3), 10 U.S.C. § 424



<sup>15</sup>(U) A June 1996 Supplement did not significantly change the 1979 Agreement. It simply clarified, supplemented, and modernized the ambiguities that arose after more than 16 years of change in both organizations.

DIA: (b)(3), 10 U.S.C. § 424

DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424

(S//NF) DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424

her an

DIA: (b)(6)

DIA: (b)(6)

100

as the

DIA: (b)(6)

(U//FOUO) In 1996, Montes earned a [REDACTED] DIA: (b)(6)

nel po  
labale

(U//FOUO) [DIA: (b)(6)]



## (U) Security Processing

(U//~~FOUO~~) In late August 1996, Montes completed the paperwork necessary to begin the process for the regular Periodic Reinvestigation of her security clearance. In September 1996, DIA opened the reinvestigation. The Defense Investigative Service completed its portion of the investigation in December 1996 and the DIA adjudication staff completed its portion by March 1997. The Defense Investigative Service and the DIA adjudication staff did not note any areas of security concern. Montes retained her clearance and access to highly classified information.

(U//~~FOUO~~) In February 1997, the DIA indoctrinated Montes for a new sub-compartment of the DIA <sup>DIA: (b)(3), 10 U.S.C. § 424</sup>. In March 1997, DIA conducted a security review of Montes to support her nomination for indoctrination into a National Reconnaissance Office <sup>DIA: (b)(3), 10 U.S.C. § 424</sup>. In May 1997, she was indoctrinated for <sup>DIA: (b)(3), 10 U.S.C. § 424</sup>. In March 2001, DIA administratively debriefed Montes from <sup>DIA: (b)(3), 10 U.S.C. § 424</sup>. She was asked to come in person to sign the debrief forms but never showed up. Montes had access to <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> until the day of her arrest. For a complete listing of Montes' access to sensitive programs and information, see Appendix D.

## (U) Counterespionage Efforts Against Cuba

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c)</sup>

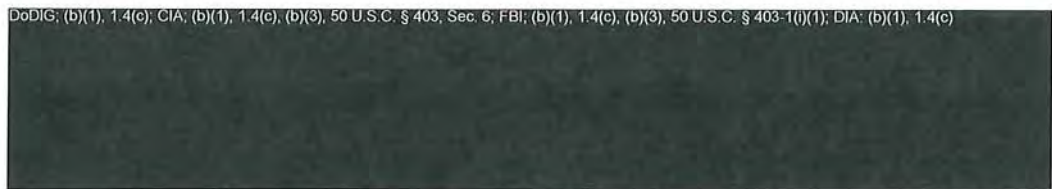
[REDACTED]

(U//~~FOUO~~) From 1994 to 1998, the relationship between the FBI and the DoD was somewhat tentative. In March 1995, a DoD employee was appointed as the first liaison officer to the FBI Headquarters National Security Division. He served in the position for 18 months. He said that when he first reported, "The FBI was still not comfortable with an outsider working in their midst. They played everything very close to the vest. It was a little better by the time I left and it has gotten better over the years." The FBI was very selective about what they told the liaison officer and the DoD did not want him to be too aggressive. He stated that, "The DoD philosophy was that they finally had someone in the room and they didn't want me to do anything to get kicked out of the room."

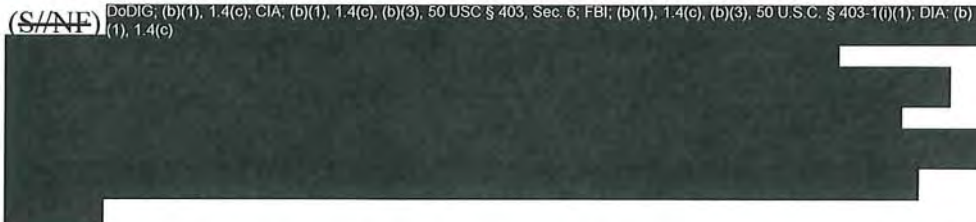
(S//NF) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c)</sup>

[REDACTED]


DoD(G) (b) (1), 1.4(c); CIA (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403, Sec. 6; FBI (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403-1(i)(1); DIA (b) (1), 1.4(c)




(S//NF) DoD(G) (b) (1), 1.4(c); CIA (b) (1), 1.4(c), (b) (3), 50 USC § 403, Sec. 6; FBI (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403-1(i)(1); DIA (b) (1), 1.4(c)



(S//NF) CIA (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403, Sec. 6; FBI (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403-1(i)(1); DIA (b) (1), 1.4(c)




(S//NF) FBI (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403-1(i)(1); DIA (b) (1), 1.4(c)




FBI (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403-1(i)(1); DIA (b) (1), 1.4(c)



FBI (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403-1(i)(1); DIA (b) (1), 1.4(c)



(S//NF) FBI (b) (1), 1.4(c), (b) (3), 50 U.S.C. § 403-1(i)(1)



<sup>16</sup>(U) See Appendix E for information about <sup>FBI (b) (7)(E)</sup>

<sup>17</sup>(U) See Appendix E for information about <sup>FBI (b) (7)(E)</sup>



FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

(S//NF) In June 1995, the DoD appointed a point of contact for the <sup>FBI: (b)(7)(E)</sup> ~~\_\_\_\_\_~~. <sup>FBI: (b)(7)(E)</sup> ~~\_\_\_\_\_~~. The point of contact was an Air Force <sup>DoD IG: (b)(6)</sup> ~~\_\_\_\_\_~~ as a Special Agent in the Air Force Office of Special Investigations. According to the Air Force Special Agent, the FBI did not have a clear understanding of the structure and functions of the DoD. Over the course of 3 to 6 months, the Air Force Special Agent met twice with FBI Special Agents. During the first meeting, he stated that he briefed the FBI on the functions of the Military Departments, their counterintelligence elements, and some of their personnel information systems. He mentioned that the FBI Special Agents seemed appreciative of the information, but also seemed overwhelmed because it was all new to them. At the time, the FBI officials were surprised that the DoD did not have a central database for the entire Department. The Air Force Special Agent told us that he did not believe that the FBI shared all of the information they could. We found that the FBI did share information with the Special Agent, but there simply was not much to share.


(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup> ~~\_\_\_\_\_~~

<sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup> ~~\_\_\_\_\_~~

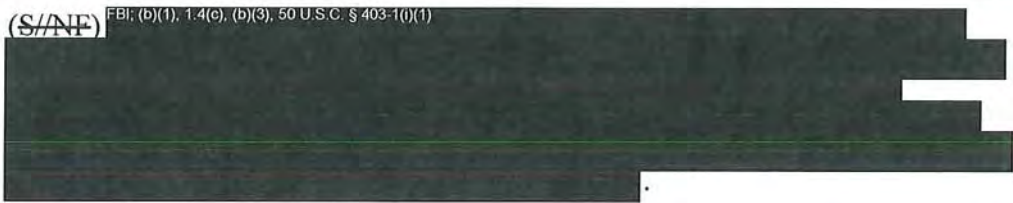
<sup>18</sup>(U) In 2003, the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) became the Office of the Under Secretary of Defense for Intelligence.

<sup>19</sup>(S//NF) The FBI and the Military Departments are the only U.S. Government organizations authorized to investigate espionage. Title 18 U.S.C. section 3052 authorizes the FBI to conduct counterintelligence investigations on U.S. persons. Title 10 U.S.C. section 802, authorizes the Military Departments jurisdiction to enforce the Uniform Code of Military Justice. Since 10 U.S.C. section 906a makes espionage a violation of the Uniform Code of Military Justice, the Military Departments are authorized to conduct counterintelligence investigations of military personnel. A significant portion of the DoD does not fall under the Uniform Code of Military Justice. To ensure that all DoD elements receive counterintelligence support, DoD Instruction 5240.10, "DoD Counterintelligence Support to Unified and Specified Commands," May 14, 2004, assigns Executive Agent support roles to each of the Military Departments. The DoD assigned an Air Force Office of Special Investigations Special Agent to the <sup>FBI: (b)(7)(E)</sup> ~~\_\_\_\_\_~~ because the Air Force is the Executive Agent for counterintelligence matters in the Office of the Secretary of Defense. <sup>FBI: (b)(7)</sup> ~~\_\_\_\_\_~~

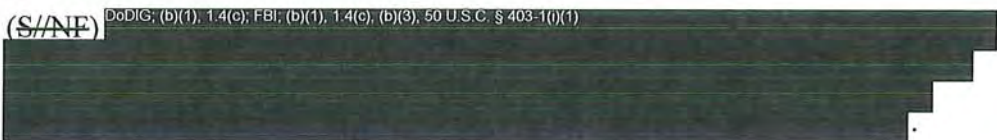
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)



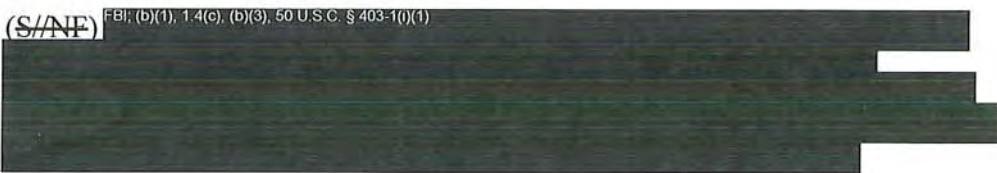
(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



(S//NF) DoD/G: (b)(1), 1.4(c), FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)




~~(U//FOUO)~~ Support for the Analyst's File Environment System

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424




<sup>20</sup> (S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c)






DIA: (b)(3), 10 U.S.C. § 424

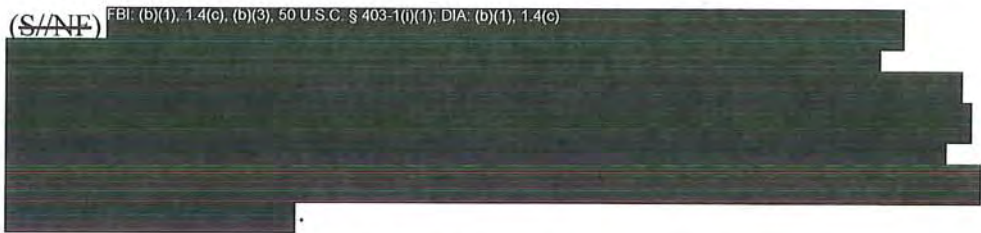


<sup>DoD IG: (b)(1), 1.4(c)</sup> <sup>DoD IG: (b)(1), 1.4(c)</sup> <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1), DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>



## (U) Prelude to Catching a Spy

<sup>(S//NF)</sup> <sup>DoD IG: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1), DIA: (b)(1), 1.4(c)</sup>



<sup>(TS)</sup> <sup>DoD IG: (b)(1), 1.4(c)</sup> <sup>DoD IG: (b)(1), 1.4(c), FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1), DIA: (b)(1), 1.4(c)</sup>



DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)

- FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E) ;
- DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E) ;
- FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E) ;
- FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)
- FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E) ;
- DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E) ;
- DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E) ;
- FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)
- FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)

~~TOP SECRET~~ <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup> ~~NOFORN//MR~~



## (U) Part V. A Prominent Life Unraveled

(S//NF)

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(6)



(S//NF) From 1998 to 2001, the U.S. Government continued its search for the Cuban penetration agent of the Intelligence Community. The period opens with the Intelligence Community using the profile information in its attempt to identify the Cuban penetration agent and closes with the arrest and imprisonment of Ana Montes as a Cuban spy.

(U//~~FOUO~~)

DIA: (b)(6)

### Concerns

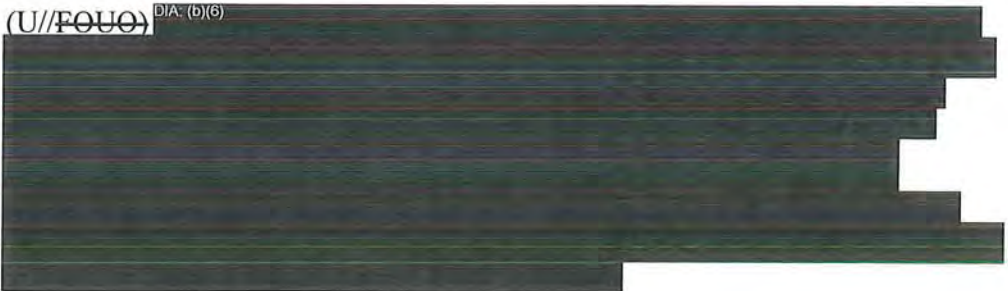
(U//~~FOUO~~)

DIA: (b)(6)



(U//~~FOUO~~)

DIA: (b)(6)



(U//~~FOUO~~)

DIA: (b)(6)



DIA: (b)(6)



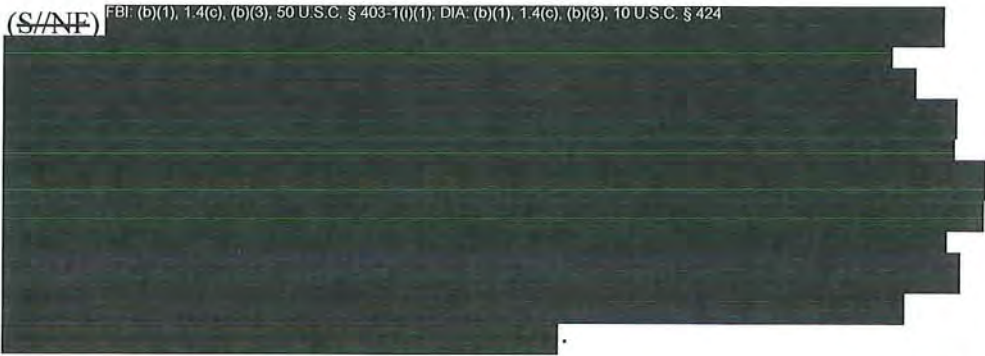
### (U) Significant Travel and Recognition

(U) This section focuses on significant events in Montes' official and clandestine travel from 1998 to 2001 and on the significant recognition she received during this period.

### (U) Travel for Official Government Business

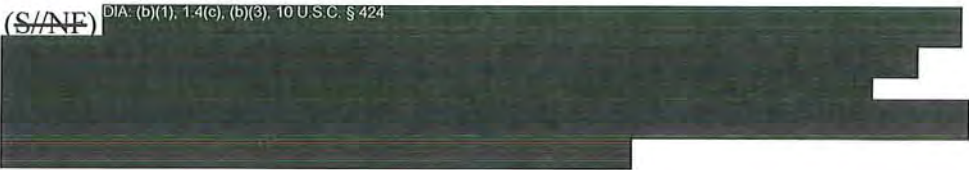
(S//NF)

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-10(1); DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424




(S//NF)

DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424



(S//NF)

DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424



(S//NF) In July 2001, Montes visited the <sup>DIA: (b)(3), 10 U.S.C. § 424</sup>  
<sup>DIA: (b)(3), 10 U.S.C. § 424</sup>, to attend briefings and discussions on improving HUMINT.



**(U) Travel for Personal and Clandestine Purposes**

(U//FOUO) <sup>DIA: (b)(6)</sup>

[REDACTED]

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(6)</sup>

[REDACTED]

(S//NF) <sup>DIA: (b)(6)</sup>

[REDACTED]

(S//NF) <sup>DIA: (b)(6)</sup>

[REDACTED]

(S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(6)</sup>

[REDACTED]

DIA: (b)(1), 1.4(c)

(U//~~FOUO~~) <sup>DIA: (b)(6)</sup>

## (U) Respect for Montes Deepens

(U//~~FOUO~~) During this period, Montes received many awards and recognition for her analytic skills. In July 1998, she received another <sup>DIA: (b)(6)</sup>

(U//~~FOUO~~) In April 1999, Montes received a <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(6)</sup>

December, she was awarded a Certificate in Recognition of Twenty Years of Service in the Government. <sup>DIA: (b)(6)</sup>

(U//~~FOUO~~) <sup>DIA: (b)(6)</sup>

(U//~~FOUO~~) <sup>DIA: (b)(6)</sup>



## (U) Additional Access

(S//NF) From early 1999 through 2001, Montes gained access to several sensitive SAPs.<sup>21</sup> In January 1999, she was briefed into the <sup>DIA (b)(1), 1.4(c)</sup> and was administratively debriefed from the program after her arrest. In February 2000, she was briefed into the <sup>DIA (b)(1), 1.4(c)</sup>, which was related to the <sup>DIA (b)(1), 1.4(c)</sup>. For a list of Montes' access to sensitive information, see Appendix D.

## (U//~~FOUO~~) A Potential Fellowship at the National Intelligence Council Clouded by an Inspector General Investigation

### (U//~~FOUO~~) The Fellowship

(S//NF) In 2000, the National Intelligence Council began a new program that offered Research Fellow positions to talented applicants. Since 1975, the National Intelligence Council had developed into an all-source center of strategic thinking. Drawing on the best available expertise inside and outside Government, it provides the DCI and Government policy makers with an authoritative voice on the complex international issues of today and those that lie ahead. In September 2000, Montes applied for one of the Research Fellow positions. In her application, she stated that the position would provide her with the time she did not have in her current position to investigate issues of high interest to policy makers. If approved, DIA management did not object to her beginning the program in January 2001. The National Intelligence Council approved her application in November and she planned to begin the fellowship on January 2, 2001. Montes was scheduled to become the first DIA employee to participate in the fellowship program.


(U//~~FOUO~~) The Research Fellow position required that candidates successfully complete a polygraph examination. Montes notified the National Intelligence Council that the start date of her fellowship might be delayed because <sup>DIA (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

### (U//~~FOUO~~) DIA Inspector General Investigation and its Aftermath


(S//NF) <sup>DIA (b)(3), 10 U.S.C. § 424, (b)(6)</sup>

<sup>21</sup>(U//~~FOUO~~) This section will not describe the substance of the SAPs to which Montes had access because in-depth knowledge of those programs is beyond the scope of this review.


DIA: (b)(3), 10 U.S.C. § 424, (b)(6)



(S//NF) DIA: (b)(3), 10 U.S.C. § 424, (b)(6)

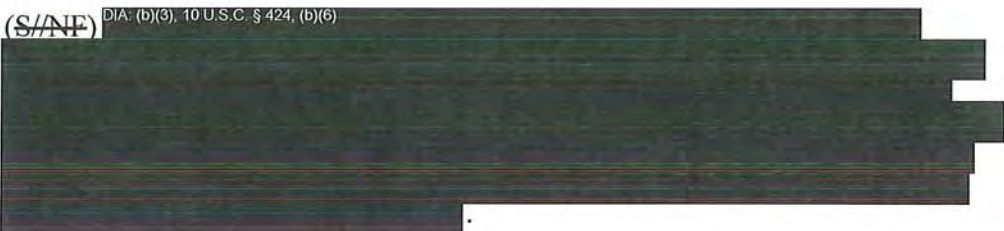


(S//NF) DIA: (b)(1), 1.4(c), (b)(7)(E)



. Montes was interviewed by an official in the  
DIA Office of the Inspector General on January 4, 2001.


(S//NF) DIA: (b)(3), 10 U.S.C. § 424, (b)(6)



(S//NF) On February 13, 2001, the Director, DIA froze all rotational assignments  
outside the DIA <sup>DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>



. The Director, DIA said his justification for  
making that all-encompassing decision was that the DIA had been overextended  
in terms of the number of employees detailed and the freeze would give the  
agency some relief. <sup>DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>





DIA: (b)(1), 1.4(c), (b)(7)(E)

(S//NF) In early March 2001, Montes learned of the freeze on external rotational assignments for all DIA employees. Her polygraph examination was postponed and she was told that it would be rescheduled when the freeze was lifted. Montes

DIA: (b)(3), 10 U.S.C. § 424, (b)(6)

## (U//~~FOUO~~) Counterespionage Efforts Against Cuba

(S//NF) <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

(TS//NF) <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

• <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

• <sup>DoD IG: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

• <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

• <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

• <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

• <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

• <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

• <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

(U//)

(TS) DoD/G:  
(b)(1),  
10/1/00

(S//NF)

Page 1 of 1

DoD[IG: (b)(1), 1.4(c)

officials

CIA officials declined the offer. CIA investigators contend that they were not aware of [REDACTED] offer. Had such an offer been made, CIA officials believe they would have been obliged to obtain FBI permission to share information collected [REDACTED]

(S//NF)

\_\_\_\_\_

~~(C)~~

(S/NF)

\_\_\_\_\_



the Air Mobility Command, Scott Air Force Base, Illinois, were routinely destroyed after 6 months. This effort did not develop any leads.<sup>22</sup>

(U//~~FOUO~~) Clues to an Elusive Profile

(TS) DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c); (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]

(TS) DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c); (b)(3), 50 U.S.C. § 403, Sec. 6; (b)(7)(E); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]

(TS) DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]

- DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]
- DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]
- CIA: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]
- DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]
- DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) [REDACTED]


(TS) DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c); (b)(3), 50 U.S.C. § 403, Sec. 6; (b)(7)(E) [REDACTED]

<sup>22</sup> (S//NF) DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6 [REDACTED]


(S//NF) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(7)(E); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>




(TS) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(7)(E); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> (NF)




(TS) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(7)(E)</sup> (NF) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(7)(E)</sup>



(TS) <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> (NF)



<sup>23</sup> (S//NF) <sup>DoD IG: (b)(1), 1.4(c)</sup>





(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

(S//NF) DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

(TS//NF) DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

(TS//NF) DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(7)(E)


(S//NF) DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

<sup>24</sup> (TS//NF) DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

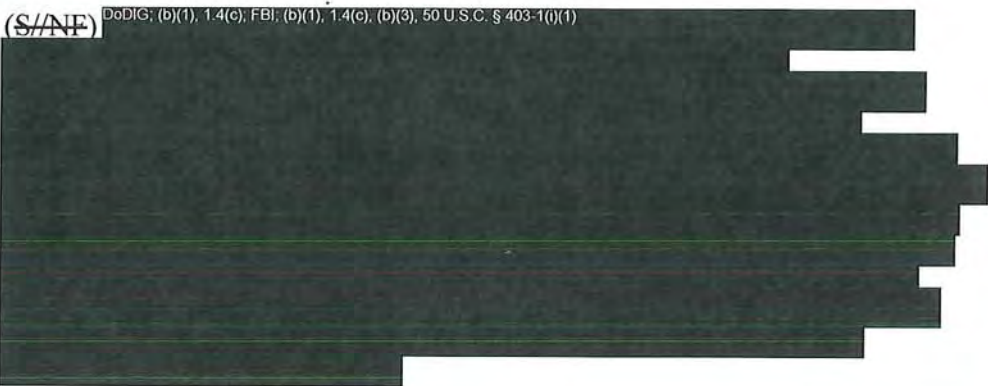
<sup>25</sup> (S//NF) An FBI Supervisory Special Agent told us that the agents were conducting the investigation in a very professional, thorough, and methodical manner. They developed analytic matrices to identify possible leads. As they eliminated a possible lead, they investigated the next lead. Both the DoS and the DoD were on their list; they simply had not yet reached the point of the investigation that included those agencies.

## (U) Serendipity


~~(TS)~~ <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~(NF)~~ <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c); (b)(3), 50 U.S.C. § 403-1(j)(1)</sup>



~~(S/NF)~~ <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c); (b)(3), 50 U.S.C. § 403-1(j)(1)</sup>




~~(S/NF)~~ <sup>DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c); (b)(3), 50 U.S.C. § 403-1(j)(1)</sup>






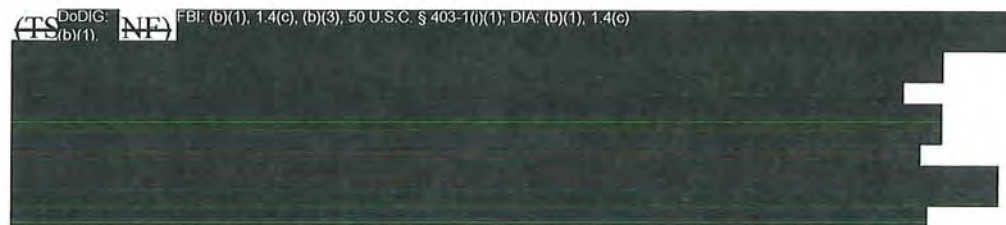
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)




~~(TS)~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~(NF)~~ ~~DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424~~




~~(TS)~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~(NF)~~ ~~FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c)~~



~~(TS)~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~(NF)~~ ~~DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(5), (b)(7)(E)~~




~~(TS)~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~(NF)~~ ~~FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c)~~



<sup>26</sup>(U//FOUO) All FBI officials we interviewed denied making this statement. The DIA counterintelligence Special Agent that followed up on this statement determined that it was made by an individual detailed from the DIA to the FBI who simply did not care for Montes, and that the FBI was not investigating Montes at the time the warning was issued.


DoD/G: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(j)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)



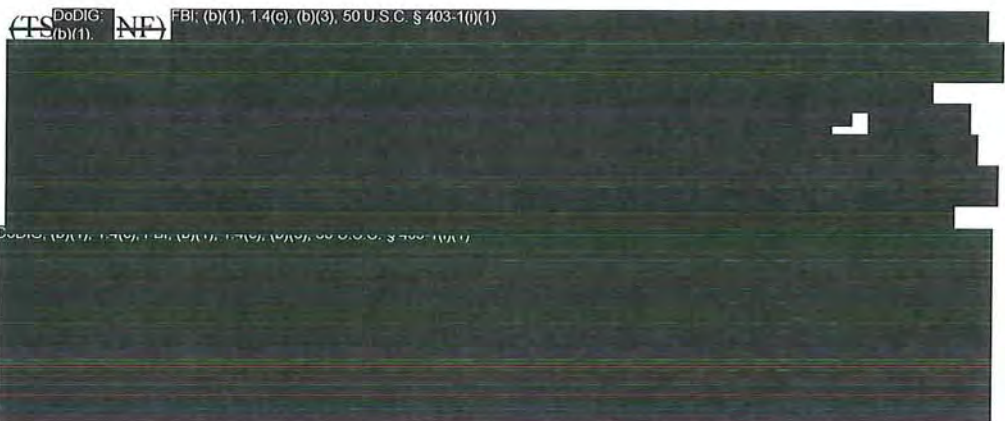
## (U) The End Game

### (U//~~FOUO~~) Building the Case against Montes

<sup>(TS)</sup> <sup>DoD/G: (b)(1), 1.4(c)</sup> <sup>(NF)</sup> <sup>FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(j)(1)</sup>



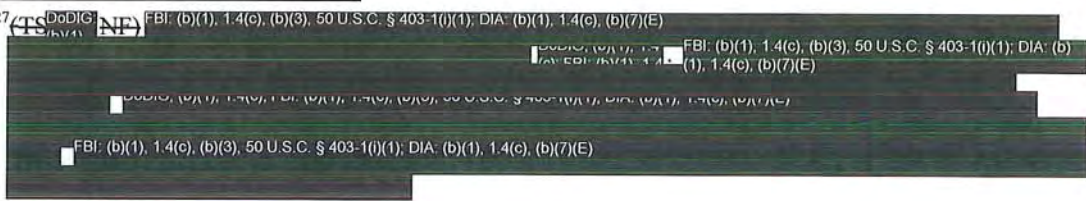
<sup>(TS)</sup> <sup>DoD/G: (b)(1), 1.4(c)</sup> <sup>(NF)</sup> <sup>FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(j)(1)</sup>



<sup>(TS)</sup> <sup>DoD/G: (b)(1), 1.4(c)</sup> <sup>(NF)</sup> <sup>DoD/G: (b)(1), 1.4(c); FBI: (b)(3); 50 U.S.C. § 403-1(j)(1)</sup>




27 <sup>(TS)</sup> <sup>DoD/G: (b)(1), 1.4(c)</sup> <sup>(NF)</sup> <sup>FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-1(j)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>

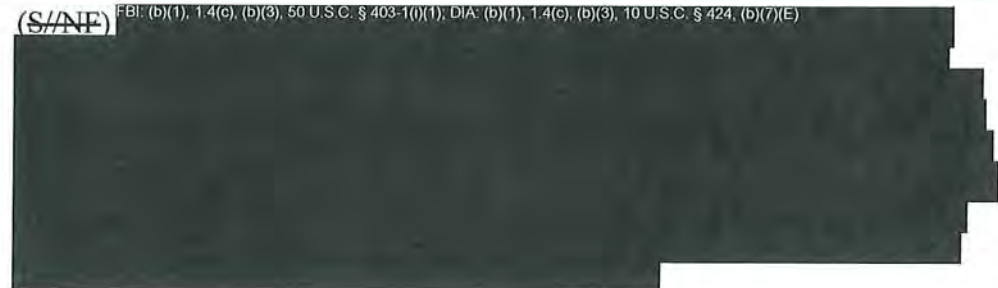




DoD/G: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)




(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>



### (U//~~FOUO~~) The Investigative Wheels Begin to Turn


(S//NF) <sup>DoD/G: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>



(S//NF) The DIA leadership consistently apprised DoD senior officials on the status of the Montes case. On November 27, the DIA informed the Joint Counterintelligence Evaluation Office (JCEO)<sup>28</sup> about the investigation and briefed the ASD(C<sup>3</sup>I), who then briefed the SECDEF and the Deputy Secretary of Defense. After the Office of the Secretary of Defense was briefed about the case, senior FBI Headquarters officials interacted with the JCEO, providing it<sup>29</sup> with periodic updates on the status of the case. The FBI briefed the Director, DIA every 2 weeks throughout the investigation because the Director wanted to make sure that DIA was doing everything possible to assist the FBI in pursuit of Montes.

<sup>28</sup> (U//~~FOUO~~) In September 1998, the Deputy Secretary of Defense established the JCEO to ensure an adequate flow of information relating to espionage investigations. The Deputy Secretary wanted a mechanism through which he and the SECDEF could be apprised of counterintelligence matters. The JCEO evolved into the CIFA, Investigations, within the CIFA in May 2002.

<sup>29</sup> (S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>



(U) <sup>FBI: (b)(7)(E)</sup> [REDACTED]

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> [REDACTED]

(TS) <sup>DoD IG: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> (NF) [REDACTED]

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> [REDACTED]

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> [REDACTED]

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> [REDACTED]

<sup>30</sup>(U) The Office of Intelligence Policy and Review is responsible for advising the Attorney General on all matters relating to the national security of the United States. The Office prepares and files all applications for electronic surveillance and physical search under the FISA of 1978.

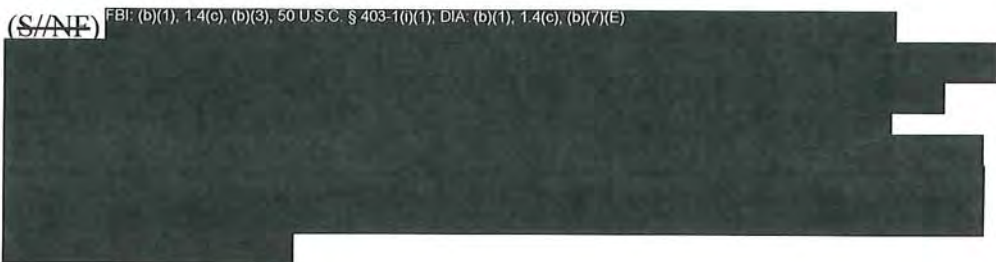


(U) Gathering Evidence and Briefing Senior Officials

(TS) <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NOFORN~~ FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)



(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)



(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



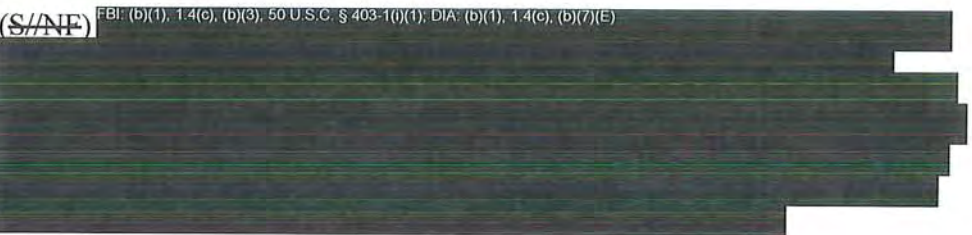
(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)



(S//NF) DIA: (b)(1), 1.4(c), (b)(7)(E)



(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)



(S//NF) In June, the Director, DIA; Director, NSA; the DoD General Counsel; the ASD(C<sup>3</sup>I); the Deputy Assistant Secretary of Defense (Security and Information Operations); the Director, National Reconnaissance Office; and the Chief of the JCEO met to discuss Montes' Intelligence Community accesses. <sup>DIA: (b)(1), 1.4(c); (b)(7)(E)</sup>

(S//NF) Also in June 2001, the FBI Headquarters senior leadership met with DoJ Internal Security Section officials to provide information about the Montes investigation so the Chief of the DoJ Internal Security Section could make an informed decision about assuming DoJ responsibility for case.

(S//NF) In July, the FBI senior leadership met with the Director, DIA to provide a status report on the Montes investigation, and the Director, DIA met with the DCI to discuss the case.

(S//NF) In August, the FBI senior leadership met once again with DoD leadership officials and then the Director, DIA to provide an update on the Montes investigation. Further, the Chief of the JCEO met with the Director, DIA to discuss the case. Specifically, the JCEO was concerned about Montes' continued access to sensitive DoD information; the JCEO wanted to minimize Montes' access to sensitive information in a non-alerting fashion;<sup>31</sup> place a time limit on the FBI investigation; and provide the basis for terminating Montes' employment should the FBI investigation fail to develop evidence to support a prosecution.

(S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(5)</sup>

<sup>DIA: (b)(3), 10 U.S.C. § 424</sup> Montes was scheduled to shift her daily focus from Cuba and assume responsibility for the Colombia account, a move that would enable her to access additional sensitive information. In the aftermath of September 11, the Director, DIA stated that his "plate was overflowing;" he not only had to deal with the intelligence activities of his agency in support of national security, but he had to offer comfort to the families of those DIA members who died at the Pentagon on that fateful day. Also, he believed that the time had come to arrest Montes. He called the <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> and told him: "This is it." Montes had just been assigned to the Bomb Damage Assessment Team that would perform those duties shortly after the commencement of hostilities in Afghanistan – Operation ENDURING FREEDOM. Team members were gearing up for their assignment, which included several days of training. The Director, DIA wanted resolution before bombing operations began in Afghanistan. He said that he would not wait any longer for a decision. The FBI Headquarters leadership believed that, in a perfect world, the FBI would have had more time to monitor Montes' activities with the prospect that she may have eventually led the FBI to others in the Cuban spy network. Instead, September 11, 2001, and its aftermath helped determine the timing of her arrest.

<sup>31</sup>(S//NF) Efforts to ensure that Montes did not learn of the investigation were successful. During our interview of her in September 2004, she said that she never heard from anyone at the DIA that there were suspicions about her being a spy. Montes did state, however, that the week before her arrest, she was aware that she was being followed but that she could not flee because she "couldn't have given up on the people [she] was helping."



## **(U//~~FOUO~~) The Finale to More Than Sixteen Years of Espionage**

(S//NF) Several days after September 11, 2001, FBI Washington Field Office and DIA counterintelligence officials met to begin preparations for Montes' arrest. Similarly, the JCEO and DIA carefully began to coordinate notification of the senior DoD leadership of Montes' impending arrest.

(U//~~FOUO~~) On September 21, 2001, when FBI Washington Field Office Special Agents interviewed Montes at the Defense Intelligence Analysis Center, they informed her that they had information from a senior official in the Cuban Intelligence Service concerning a Cuban penetration agent that implicated Montes. During the course of the interview, Montes refused to sign a Classified Information Nondisclosure Agreement, and she asked to speak with an attorney. The FBI Special Agents then read Montes her Advice of Rights; she signed it after it was amended to reflect that she refused to answer questions without counsel present. Montes was then arrested for conspiracy to commit espionage against the United States in violation of 18 U.S.C. section 794(a) and (c).

(U//~~FOUO~~) Several officials from DIA, FBI, and the JCEO stated that once the FBI launched its investigation of Montes, it became the best example of cooperative information sharing that they had experienced.

## **(U) Post Arrest**

(U) On March 19, 2002, Ana Belen Montes<sup>32</sup> pleaded guilty to conspiracy to commit espionage in violation of 18 U.S.C. section 794(a) and (c):

To communicate, deliver, and transmit to the government of Cuba and its representatives, officials 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 objects of this conspiracy in the District of Columbia and elsewhere, all in violation of 18 U.S.C. § 794(c),

(U) As part of her plea agreement, Montes waived her right to plead not guilty and her right to a jury trial. She also waived her rights under the Fifth Amendment to the Constitution of the United States that would have protected her from the use of self-incriminating statements in a criminal prosecution. Montes is required to be available for questioning by Federal, state and local law enforcement agencies and to be available for debriefings by law enforcement and intelligence officials. Montes is required to voluntarily submit to polygraph examinations to be conducted by a polygraph examiner of the U.S. Government's choice. The results of the polygraph examinations are admissible in proceedings to determine Montes' compliance with the plea agreement. Montes' obligation to cooperate pursuant to the plea agreement is a lifelong commitment.

<sup>32</sup>(U) Between her arrest and her plea, Montes was housed at the Orange County Detention Center in Orange, Virginia.

(S//NF)

FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

(U) On October 16, 2002, Montes was sentenced to 25 years in prison with 5 years of supervised probation upon her release. She currently is serving her sentence in the Carswell Federal Medical Center, Fort Worth, Texas.



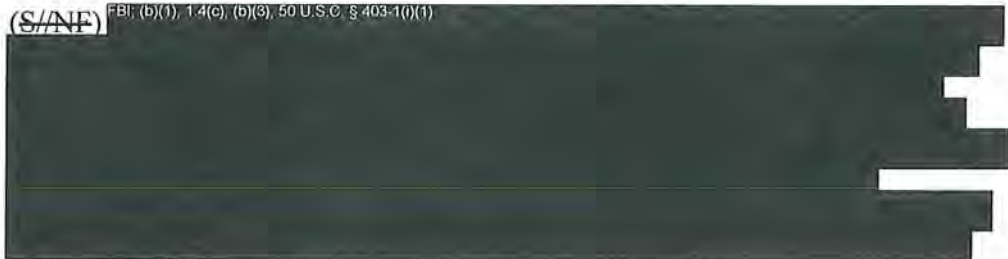
(U) Ana Montes arrested on September 21, 2001.



## (U) Part VI. Findings, Recommendations, and Observations

(S//NF) This section contains 11 findings and 5 observations. We found less-than-optimum sharing of counterespionage information between the Intelligence and Law Enforcement Communities. We discovered that the CIFA was not effective as the DoD focal point for counterespionage investigations, and that this shortcoming inhibited the identification of unknown espionage subjects within the DoD. We found significant DoD polygraph and SAP deficiencies. Further, we determined that the DIA does not have an adequate counterespionage infrastructure to meet its needs and has difficulty retaining highly skilled investigators. The DIA also does not have Standard Operating Procedures on counterintelligence inquiries, nor does it have a comprehensive program to determine the suitability of prospective employees.

(S//NF) <sup>FBI (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-10(1)</sup>



### (U) Finding 1

(C) In the years preceding the identification of Ana Montes as a penetration agent for the Cuban Intelligence Service, management indifference; interagency rivalry; personal rancor; and lack of appreciation for and understanding of counterespionage roles, structures, and responsibilities led to less than optimum sharing of counterespionage information between Intelligence and Law Enforcement Communities.

(C) One of the first actions in any espionage investigation is to direct investigative and analytic resources from a vast amount of information on unknown subjects toward identifying a suspect. The FBI and its Intelligence Community partners cannot effectively convert unknown subjects into espionage suspects without sharing information. In this finding, we will first explore authoritative counterintelligence and counterespionage guidance and then demonstrate how those imperatives were overlooked or ignored by organizations exposed to information that led to the arrest of Ana Montes.

## (U) Authoritative Guidance

(U) During the past 25 years, the U.S. Government Executive and Legislative Branches issued authoritative guidance that highlighted the criticality of sharing counterintelligence and counterespionage information.

(S)

FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

A large rectangular area of the document is completely redacted with black ink, covering approximately 10 lines of text.

(U)

DoD IG: (b)(1), 1.4(c)

A rectangular area of the document is redacted with black ink, covering approximately 2 lines of text.

(S)

FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

A large rectangular area of the document is completely redacted with black ink, covering approximately 15 lines of text.

(U) On May 3, 1994, Presidential Decision Directive 24 succeeded Presidential Review Directive/NSC-44. Directive 24 ordered the creation of a new national



counterintelligence policy structure under the auspices of the National Security Council to coordinate counterintelligence policy matters and to foster greater cooperation among the departments and agencies with counterintelligence responsibilities. Directive 44 further required an exchange of senior managers between the CIA and the FBI to ensure timely and close coordination between the Intelligence and Law Enforcement Communities. It also established the National Counterintelligence Policy Board, which consisted of one senior executive representative from the CIA; the FBI; the DoD, the DoS, and the DoJ; a Military Department counterintelligence component; and the National Security Council, Special Assistant to the President and Senior Director for Intelligence Programs. The National Counterintelligence Policy Board exercised oversight responsibilities for the National Counterintelligence Center and was responsible for the regular monitoring and review of the integration and coordination of U.S. counterintelligence programs.

(U) <sup>DoD IG (b)(1), 1.4(c)</sup> [REDACTED]

(C) Presidential Decision Directive/NSC-75, "U.S. Counterintelligence Effectiveness: Counterintelligence for the 21<sup>st</sup> Century," December 28, 2000, is another counterintelligence-related directive. Presidential Decision Directive/NSC-75 stressed that, while there had been dramatic improvement in the coordination of counterintelligence activities, there was a need to meet the challenge of "an expanded and diversified threat" to the national security of the United States. Presidential Decision Directive/NSC-75 pointed out that the importance and complexity of the issue required a commitment to "cooperation, coordination, and collaboration." Presidential Decision Directive/NSC-75 established the National Counterintelligence Board of Directors and the NCIX, who serves as the substantive leader of national-level counterintelligence and coordinates and supports the detection and neutralization of espionage against the United States.

(S) The FY 2004-2005 Congressional Budget Justification for the DoD portion of the National Foreign Intelligence Program asserts that effective counterintelligence support must be "unencumbered by traditional organizational and cultural bias that has traditionally been an impediment to change." The FY 2005 National Foreign Intelligence Program Congressional Budget Justification mentions that security processes and procedures should not become barriers to achieving the vision of open and efficient exchange of information across the Intelligence Community. The National Foreign Intelligence Program notes that an open and efficient exchange of information requires cooperation and a willingness to practice risk management.

## (U) Marginal Success

(U//~~FOUO~~) Two recent reports demonstrate that, although repeated guidance on information sharing has been well-intentioned, success has been marginal and remains elusive.

(U) In August 2003, the Inspector General, DoJ, issued "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." The report indicated that FBI penetration efforts in the late 1970s and 1980s suffered from a lack of cooperation with the CIA and from management inattention. Throughout the 1980s, the FBI did not work cooperatively with the CIA, but the early 1990s saw significant improvement, especially in the 1985-1986 cases involving the loss of assets operating against the Soviet Union. However, the DoJ report mentioned that the FBI failed to keep the CIA apprised of information on non-CIA espionage investigations, which "undermined the effort to identify Hanssen." As the Hanssen investigation unfolded, the FBI focused on a CIA suspect and "lost a measure of objectivity and failed to give adequate consideration to other possibilities." In sum, the DoJ report claimed that the CIA could not function as an effective counterbalance to the FBI in the Hanssen case because it was not an equal partner in the hunt for the espionage agent.

(U) The 2004 "Final Report of the National Commission on Terrorist Attacks Upon the United States," states that, "Agencies uphold a need-to-know culture of information protection rather than promoting a need to share culture of integration," and stresses that "information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge." While the National Commission report focuses on counterterrorism information sharing, it can also be applied to counterespionage.

## (U) Management Indifference

(S//~~NF~~) Our examination of the Montes espionage case found at least 11 examples of management indifference that impeded counterespionage information sharing. Management indifference to compliance with guidance on sharing counterintelligence information was reflected by the lack of cooperation, forthrightness, and management oversight and action.

1. (TS//<sup>DoD(G) (b) (1), 1.4(c)</sup> ~~NF~~) <sup>DoD(G) (b) (1), 1.4(c); CIA (b) (1), 1.4(c); (b) (3), 50 U.S.C. § 403, Sec. 6; FBI (b) (1), 1.4(c); (b) (3), 50 U.S.C. § 403-1(f)</sup>





(U//FOUO) <sup>DoD IG: (b)(1), 1.4(c)</sup>  
<sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

2. (S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

- <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

- <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

- <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

- <sup>CIA: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

- <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

- <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

33 (U) <sup>DoD IG: (b)(1), 1.4(c)</sup>  
<sup>DoD IG: (b)(1), 1.4(c)</sup>

3. (TS <sup>DoD IG: (b)(1)</sup> ~~NF~~) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

[REDACTED]

4. (TS <sup>DoD IG: (b)(1)</sup> ~~NF~~) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

[REDACTED]

5. (S/NF) <sup>DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(5); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

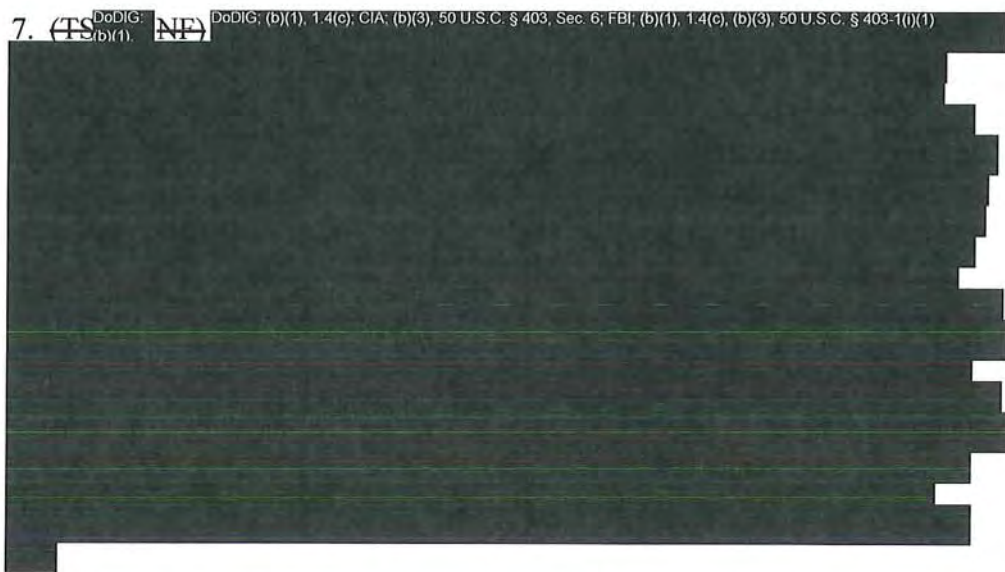
[REDACTED]



6. (TS <sup>DoD IG: (b)(1)</sup> <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NP~~)  
<sup>DoD IG: (b)(1)</sup> <sup>DoD IG: (b)(1), 1.4(c)</sup> <sup>CIA: (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(5)</sup>



7. (TS <sup>DoD IG: (b)(1)</sup> <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NP~~) <sup>CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>




8. (TS <sup>DoD IG: (b)(1)</sup> <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NP~~) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>



9. (TS <sup>DoD IG: (b)(1)</sup> <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NP~~) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>




DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)




(TS) <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NOFORN~~ DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



10. (TS) <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NOFORN~~ DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)




11. (TS) <sup>DoD IG: (b)(1), 1.4(c)</sup> ~~NOFORN~~ DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)


DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, (b)(5); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



(U//FOUO) <sup>DoD IG: (b)(1), 1.4(c)</sup>



34 (U//FOUO) <sup>DoD IG: (b)(1), 1.4(c)</sup>





DoD IG: (b)(1), 1.4(c)

[REDACTED]

(TS) DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

[REDACTED]

## (U) Interagency Rivalry and Personal Rancor

(S//NF) Notwithstanding abundant guidance to share counterespionage information, investigations are conducted by human beings with biases and insecurities. Personal character traits sometime interfere with efficient information flow among organizations. We found several instances where interagency rivalry and personal rancor led to less-than-optimum sharing of counterespionage information.

(TS) DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)

[REDACTED]


(TS) DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6

[REDACTED]

DoD IG: (b)(1), 1.4(c)




~~(S//NF)~~ <sup>DoD IG: (b)(1), 1.4(c), FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>  
~~DoD IG: (b)(1), 1.4(c), FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)~~



(S//NF) The intelligence cycle consists of identifying information gaps, collecting needed information, analyzing the information collected, disseminating the intelligence product to the customer, and receiving feedback on the usefulness of the intelligence provided. Customer feedback often generates additional collection requirements. Despite this time-honored process, the FBI was often not a good “customer.” Several DoD officials told us that the insular attitude of the FBI made it extremely difficult to get feedback from the Bureau. A senior DoD official said:

Getting the FBI to give information is difficult. The FBI gives enough information for us to brief up our chain of command, but not much more than that. I would go back to the FBI to get more information and the FBI would say ‘no.’ Over the course of the last 5 years, I have been telling the FBI that it is in everyone’s best interests to give up the information because we are working as a team not only to arrest and prosecute, but also to protect the loss of DoD information.

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



(b)(3), 50 U.S.C. § 403-1(i)(1)



~~DoD/G: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)~~

## **(S) Limited Appreciation for and Understanding of Counterespionage Roles and Responsibilities**

(S//NF) The DoD is the largest branch of the U.S. Government with more than 1 million civilian and military employees. The DoD has its own arcane language and organizational infrastructure. It is often a daunting task for DoD personnel to navigate the complex bureaucracy to accomplish their mission. For those outside the DoD, the task can be even more challenging. A DoD organization responsible for counterespionage must therefore be easily recognizable to non-DoD entities. In our review of the Montes breach, we found several instances where a limited appreciation for, and understanding of, counterespionage roles, structures, and responsibilities led to less-than-optimum sharing of counterespionage information.

(S//NF) <sup>DoD/G: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

(S//NF) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

(S//NF) <sup>DoD/G: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

~~DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-10(i)(1)~~

~~(S//NF)~~ <sup>DoD IG: (b)(1), 1.4(c)</sup>  
~~DoD IG: (b)(1), 1.4(c); DIA: (b)(3), 10 U.S.C. § 424~~

## **(U) A Final Thought on Information Sharing**

~~(S//NF)~~ Promulgation of DCI Directive 8/1 reinforces the maxim that "...the broadest possible sharing of intelligence information is fundamental to the mission of the Intelligence Community." Sharing intelligence information at the earliest possible point maximizes its potential value and, given sufficient safeguards, protects sensitive sources and methods. The Directive 8/1 recognizes that, "when multiple data sources, collection techniques, and analytical viewpoints are brought to bear on a problem...the whole can indeed be greater than the sum of its parts." Once Ana Montes was identified as a possible Cuban espionage agent, the investigative resources of the Law Enforcement and Intelligence Communities focused on that target in the most professional manner imaginable. Notwithstanding that professional investigation, reluctance to share vital information enabled Montes to continue her clandestine activity for a number of years with a certain degree of comfort. While the principle of need to know is a lofty aspiration, balancing need to know with a need to share optimizes mission success.

## **(U) Recommendation 1**

~~(U//FOUO)~~ We recommend that the Under Secretary of Defense for Intelligence request the Intelligence Community Inspectors General Forum to conduct a comprehensive joint evaluation of counterespionage information sharing. The Intelligence Community Inspectors General Forum could use the Inspector General of the Department of Defense Research Report, "Research on Information Sharing Between the Intelligence and Law Enforcement Communities," May 3, 2002, as the starting point for its counterespionage evaluation.

~~(U//FOUO)~~ **Management Comments.** The Under Secretary of Defense for Intelligence concurred with our recommendation and indicated that in July 2005,



the Intelligence Community Inspectors General Forum will be requested to conduct a joint evaluation of counterespionage information sharing.

## (U) Finding 2

(U//~~FOUO~~) The CIFA has not been effective in its role as the DoD focal point for counterespionage investigations, in part because it has experienced difficulty marshalling resources to examine counterespionage activities, operations, case leads and investigations that might result in the identification of unknown subjects within the DoD.

(S//NF) Foreign intelligence and security services pose a significant espionage threat to the DoD. However, the DoD has not organized its counterespionage assets to effectively meet this threat. This finding discusses the organization of DoD counterespionage assets, the manner with which DoD has tried to address counterespionage weaknesses, and how the CIA is organized to confront the same threat.

(U//~~FOUO~~) The March 24, 1994, Presidential Review Directive, "U.S. Counterintelligence Effectiveness," asked the DoD, among other Intelligence Community members, whether there was a focal point for determining when foreign intelligence reporting becomes a counterintelligence concern that requires a law enforcement response, such as an espionage investigation. In 1996, the ASC(C<sup>3</sup>I) established the DoD Investigations Working Group to function as the focal point for national-level operational "anomalies," otherwise known as unknown subject cases. Also, in 1996, the ASD(C<sup>3</sup>I) created the Defense Unknown Subject Team to act as a specialized investigative team to focus on unknown subject espionage leads and investigations which appear to have no specific information indicating the potential subject's Military Department affiliation or unit of assignment. The DoD Investigations Working Group provided guidance, direction, and oversight to the Defense Unknown Subject Team, whose members included counterintelligence investigators from the Army, Navy, and Air Force.

(U//~~FOUO~~) On May 6, 1998, the ASD(C<sup>3</sup>I) approved the establishment of the JCEO to inform senior DoD officials of all significant DoD counterintelligence activities in a timely manner. To facilitate DoD access to all relevant information and to coordinate counterintelligence activities, JCEO positions were to be filled by liaison officers from the FBI, the CIA, and the military counterintelligence components.

(U) DoD Directive 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)," February 19, 2002, established the CIFA as a DoD Field Activity. Its mission is to develop and manage DoD counterintelligence programs and functions, including the detection and neutralization of espionage against the DoD. The CIFA assumed the mission and functions of the JCEO. Although investigative jurisdiction over espionage subjects resides with the military counterintelligence components and the FBI, the components are responsible for reporting all significant counterintelligence activities to the CIFA.

(U//~~FOUO~~) The DoD organizes counterespionage around the Military Departments. Under 10 U.S.C. 3013(c)(7), 5013(c)(7), 8013(c)(7), the Military Departments are the only DoD entities empowered to conduct counterespionage investigations. Some DoD agencies have limited authorization to conduct preliminary investigations to develop leads for the FBI and the Military



Departments. For DoD organizations that do not have this authority, the Military Departments provide Executive Agent support as detailed in DoD Instruction 5240.10, "Counterintelligence Support to the Combatant Commands and the Defense Agencies," May 14, 2004.

(S//NF) We found that the Executive Agent arrangement is not effective in meeting the espionage challenges facing the DoD. Foreign intelligence and security services target the DoD entities that handle classified material. While some specialized military units may handle a great deal of classified material, the majority of the DoD classified information resides in the defense agencies, field activities, and executive level offices. While Military Department counterintelligence agents are highly trained professionals, they rotate too frequently to operate as subject-matter experts for complex organizations such as the Office of the Secretary of Defense or the Joint Staff. This results in ad hoc counterespionage support for organizations that are at greatest risk.

(S//NF) In 1995, when the FBI needed a DoD point of contact for <sup>FBI (b)(7)(E)</sup> [REDACTED], the task fell to the Air Force Office of Special Investigations. The Office of Special Investigations detachment that provides support to the Office of the Secretary of Defense appointed a <sup>DoD(G) (b)(6)</sup> [REDACTED]. He did not have the authority to access any information outside the Air Force, so the DoD appointed representatives from the Army and the Navy to assist the FBI, as appropriate. However, the other representatives also did not have the authority to access DoD civilian employment records for organizations outside their parent Service. <sup>FBI (b)(7)(E)</sup> [REDACTED]. <sup>FBI (b)(7)(E)</sup> [REDACTED].

(U//FOUO) Establishing the DoD Investigations Working Group and the Defense Unknown Subject Team in 1996 were positive steps that the DoD took to address unknown subject espionage leads and investigations. However, the DoD Investigations Working Group did not include a cadre of vetted analysts and investigators working continuously to identify unknown espionage subjects across the entire DoD. The DoD Investigations Working Group continues to meet periodically. The Defense Unknown Subject Team was mainly staffed by detailees from the Military Departments; the arrangement created a significant problem. When faced with tasking directions from their parent organizations, detailees often tended to defer to their Military Department. As a result, support to the Defense Unknown Subject Team suffered. Further, the Defense Unknown Subject Team could only proceed with an investigation if other agencies willingly shared information. Many times the FBI, the Military Departments, and other DoD agencies did not share information with the Defense Unknown Subject Team. The Defense Unknown Subject Team was disbanded in late 2003 due in large measure to a lack of meaningful support from the Military Departments' counterintelligence organizations.

(U//FOUO) Positions in the JCEO were filled by liaison officers from the FBI, the CIA and the Military Department counterintelligence components. As was the case with the Defense Unknown Subject Team, JCEO detailees would often be tasked by their parent organization to accomplish actions that took them away from their DoD-wide counterespionage duties. Several JCEO liaison officers told us that they were underutilized and were not given all relevant DoD counterespionage information to conduct effective investigations. One FBI Special Agent said that he was misused by the JCEO. He believed that he was

detailed to provide expert guidance and advice on counterintelligence matters involving joint equities, but that did not happen. He said that certain JCEO officials created an undesirable work atmosphere for detailees, "running off" at least three agents from the Air Force Office of Special Investigations, and two from the Naval Criminal Investigative Service. Further, he said that the CIA recalled its representative from the JCEO because he was misused; to date the CIA has not refilled the position. The FBI eventually removed its liaison officer from the JCEO and does not intend to provide a replacement.

(U//~~FOUO~~) A number of factors, to include the reliance on detailees, the primacy of the Military Departments over counterespionage, and the reluctance to share relevant information, have contributed to CIFA difficulties in marshalling resources to examine counterespionage activities, operations, case leads and investigations that might result in the identification of unknown subjects within the DoD.

(S//NF) The CIA confronts the espionage threat through the <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

~~[REDACTED]~~

<sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

~~[REDACTED]~~

(S//NF) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

~~[REDACTED]~~



## (U) Recommendation 2

(S) We recommend that the Under Secretary of Defense for Intelligence formulate a plan to establish permanent Foreign Counterintelligence Program billets to build a DoD counterespionage organization similar to the <sup>CIA, (b)(3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED] Functions of the new organization should include, but not be limited to:

- acting as the central DoD point of contact for all counterespionage inquiries from outside DoD;
- identifying and resolving all unknown subject espionage cases within DoD;
- hosting a forum where vetted DoD counterintelligence analysts and special agents meet regularly to discuss openly all available counterespionage information;
- establishing investigative leads for the Military Departments' counterintelligence components and the Federal Bureau of Investigation; and,
- sharing all counterespionage information from the Military Departments and DoD agencies in accordance with Executive Orders, statutes, and DoD Directives.

(S) **Management Comments.** The Under Secretary of Defense for Intelligence concurred with our recommendation and stated that the DoD needs this capability and that CIFA is the appropriate organization wherein a <sup>CIA, (b) (3), 50</sup> [REDACTED]-like entity could be established, financed and managed. The Under Secretary also stated that a DoD <sup>CIA, (b) (3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED] would require the support of the FBI and the <sup>CIA, (b) (3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED].

(S) **Review Response.** Although the Under Secretary of Defense for Intelligence concurred, we request specific actions planned and milestones for completion of the recommended action.

### (U) Finding 3

(S) <sup>DIA: (b)(1), 1.4(c)</sup> [REDACTED]

(U//FOUO) <sup>DIA: (b)(7)(E)</sup> [REDACTED]

(S//NF) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c)</sup> [REDACTED]

(U//FOUO) <sup>DIA: (b)(7)(E)</sup> [REDACTED]

(U//FOUO) By the late 1990s, the Polygraph Institute began providing formal countermeasures instruction to Federal polygraph examiners. The current <sup>DIA: (b)(7)(E)</sup> [REDACTED] related to countermeasures. All examiners are encouraged to attend a more comprehensive continuing education course in polygraph countermeasures after completing the course. <sup>DIA: (b)(7)(E)</sup> [REDACTED]



DIA: (b)(7)(E)

Although the DoD Polygraph Institute provides instruction on polygraph countermeasures during introductory and recertification courses, dissemination of information on the subject is not widespread.

(S//NF) <sup>DIA: (b)(1), 1.4(c)</sup>

(U) The DoD Intelligence Production Program establishes policies, procedures, and production responsibilities to satisfy the foreign military and military-related intelligence requirements of the warfighter, policy maker, and force development and acquisition organizations. The goal of the DoD Intelligence Production Program is to provide complete, responsive, and functionally integrated military intelligence to consumers in the most efficient manner possible. The Director, DIA is charged by DoD Directive 5105.21, "Defense Intelligence Agency," February 18, 1997, as the DoD Intelligence Production Program Production Functional Manager. As the Production Functional Manager, the DIA performs strategic planning for centralized management of defense intelligence production and facilitates the assignment and transfer of production responsibilities in the DoD Intelligence Production Program.

(S//NF) <sup>DIA: (b)(1), 1.4(c)</sup>

### (U) Recommendation 3

a. (U//~~FOUO~~) We recommend that the Director, Defense Intelligence Agency assign a DoD Production Program Intelligence Functional Code to the Counterintelligence Field Activity for the purpose of <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>


(U//~~FOUO~~) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

DIA (b)(3), 10 U.S.C. § 424, (b)(7)(E)



(U//~~FOUO~~) The Under Secretary of Defense for Intelligence indicated that the DoD Polygraph Program Manager in CIFA will provide requests for scheduled as well as ad hoc production on countermeasures and foreign use issues via <sup>DIA (b)(3), 10 U.S.C. § 424</sup> to the DoD Counterintelligence Production Requirements Manager (J2CI).

(S) <sup>DIA (b)(1), 1.4(c)</sup>



**b. (U//~~FOUO~~) We recommend that the Director, Counterintelligence Field Activity:**

- (i) (U//~~FOUO~~) Research polygraph countermeasures and then collaborate with polygraph manufactures to develop, produce, and distribute new countermeasures detection devices for use by polygraph community consumers.**

**(U) Management Comments.** The Under Secretary of Defense for Intelligence concurred with our recommendation and stated that the DoD Polygraph Institute is conducting research on countermeasure detection. As a by-product of that research, it has identified specific criteria and training that polygraph examiners can use to identify efforts to employ polygraph countermeasures. The three major polygraph manufacturers are producing effective countermeasure detection devices as an option with their polygraph systems. Additionally, the DoD Polygraph Institute drafted a new chapter for the Federal Examiner's Handbook (FEH, Chapter 18) that will require examiners to employ these devices as an aid to countermeasure detection. That chapter is currently being staffed with all federal programs for formal incorporation. The Federal Examiner's Handbook standardizes specific procedures and requirements that are binding for all DoD polygraph programs.

- (ii) (U//~~FOUO~~) Develop comprehensive polygraph standards for the DoD polygraph community to increase the effectiveness of polygraph countermeasures.**

**(U//~~FOUO~~) Management Comments.** The Under Secretary of Defense for Intelligence concurred with our recommendation that will increase the DoD capability to detect and/or neutralize polygraph countermeasures applied against



the DoD. He stated that Chapter 18 of the Federal Examiner's Handbook will provide those standards for DoD polygraph examiners.

- (iii) (U//~~FOUO~~) Establish a comprehensive polygraph countermeasures course at the DoD Polygraph Institute that requires all DoD polygraph examiners to attend the course within 1 year of graduation from initial polygraph training and thereafter requires them to attend refresher training at least biennially.

(U//~~FOUO~~) **Management Comments.** The Under Secretary of Defense for Intelligence concurred with our recommendation and stated that the DoD Polygraph Institute has already significantly increased the number of polygraph examiners who receive specific countermeasure detection training. Since 2001, <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

<sup>(b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>. This is in large part attributed to the demand from field examiners and the effective marketing of DoD Polygraph Institute personnel who championed the importance of increasing polygraph examiner awareness and ability to neutralize polygraph countermeasure efforts. In addition, Chapter 18, Federal Examiner's Handbook requires 40 hours of comprehensive countermeasures detection training and follow-up training on a biennial basis. These standards will become accountable items for DoD polygraph programs under the Quality Assurance Program inspection schedule.

- (iv) (U//~~FOUO~~) Direct all DoD polygraph programs to report to the DoD Polygraph Institute all polygraph examinations in which countermeasures are confirmed.

<sup>(b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>  


## (U) Finding 4

(U//~~FOUO~~) The DoD polygraph directive is out of date.

(U//~~FOUO~~) Over the past 20 years, Governmentwide polygraph policies, procedures, and techniques have changed significantly. For example, DoD Directive 5210.48 states that, "The authority to expand use of the polygraph in DoD beyond that authorized. . . has been limited to a test program, involving not more than 3,500 persons to be conducted during Fiscal Year 1985." The 3,500 person ceiling was lifted in October 2004. Also, since Directive 5210.48 and its implementing regulation were promulgated in 1984 and 1985, respectively, the titles and responsibilities of several offices within DoD changed. The Under Secretary of Defense for Intelligence is now responsible for DoD polygraph policy and the CIFA is the Executive Agent charged with DoD polygraph responsibilities. Furthermore, the DoD Polygraph Institute is now responsible for U.S. Governmentwide polygraph education.

(U//~~FOUO~~) We realize that updating the Directive 5210.48 is predicated on a change to 10 U.S.C. section 1564a. The Deputy Under Secretary of Defense for Counterintelligence and Security 2005 Legislative Strategy cites the need to update the Directive. However, the Strategy indicates that Directive 5210.48 cannot be updated because wording in 10 U.S.C. section 1564a links the Directive to the DoD polygraph program. The DoD Legislative Strategy seeks to change 10 U.S.C. section 1564a by adding language that expands the categories of personnel for which DoD polygraph examinations may be administered. The language will state that CSPs are required for those who have access to other information "...whose unauthorized disclosure or manipulation would have significant potential impact upon national security, as determined under standards established by the Secretary of Defense."

## (U) Recommendation 4

(U//~~FOUO~~) We recommend that the Deputy Under Secretary of Defense for Counterintelligence and Security continue working with Congress to change DoD polygraph provisions in 10 U.S.C. section 1564a, and then update DoD Directive 5210.48 and DoD Regulation 5210.48-R, accordingly.

(U) **Management Comments.** The Under Secretary of Defense for Intelligence concurred with our recommendation. Due to an unusual situation regarding a 1987 Federal law, the DoD Directive cannot be updated until the law is changed. The Under Secretary of Defense for Intelligence has submitted a legislative proposal that would change the law in 2005.

(U) **Review Response.** We consider management comments to be responsive to our recommendation. We request that the Under Secretary of Defense for Intelligence keep us apprised of the status of the legislative proposal to change 10 U.S.C. section 1564a, and, once the law is changed, to advise us of the update to DoD Directive 5210.48 and DoD Regulation 5210.48-R.



## (U) Finding 5

(U//~~FOUO~~) The DIA does not use pre-employment polygraph examinations as part of the screening process for positions that require access to Top Secret material.

(U//~~FOUO~~) The DIA does not perform pre-employment polygraph examinations for positions that require access to Top Secret material in accordance with DoD Directive 5210.48. However, the NSA, a DoD entity, and all other non-DoD intelligence agencies require pre-employment polygraph examinations for civilian employees.

(U//~~FOUO~~) The requirement to administer a CSP to DIA employees originates from DoD Directive 5210.48, which prescribes polygraph examinations to assist in determining eligibility for employment with or assignment to the DIA in positions that have been designated by the Director, DIA as critical intelligence positions.

(U) Furthermore, the December 13, 1988, DIA Policy Statement #04-88, "Security Requirements for DIA Open Systems Architecture (OSA)," states that all authorized users of Open Systems Architecture, now termed the Joint Worldwide Intelligence Communications System, must possess Top Secret/SCI access as governed by DIA Manual 50-1, "Sensitive Compartmented Information (SCI) Security Management," December 10, 1984. DIA Manual 50-1 was superseded by DoD Manual 5105.21-M-1, "Sensitive Compartmented Information Administrative Security Manual," in August 1998. DIA personnel who possess Top Secret/SCI access and have access to a Joint Worldwide Intelligence Communications System computer terminal are candidates for CSP examinations.

(U//~~FOUO~~) <sup>CIA, (b)(3), 50 U.S.C. § 403, Sec. 6</sup>

[REDACTED] that the polygraph deters some, but not all, individuals from engaging in or expanding espionage activities. The review shows that in the Pollard, Souther, Hall, and Pelton espionage cases, none of them would have applied for positions where a CSP was a condition of employment. All four feared that a CSP examination would have uncovered their espionage activities. Ironically, in 1985 when Montes applied for a position at DIA, she knew that DIA did not require a pre-employment polygraph like the NSA or CIA.

(U) On February 28, 1994, the Joint Security Commission issued "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence." The report states that:

The polygraph is a significant espionage deterrent....The CIA and the NSA, two agencies that routinely use full-scope polygraphs to screen applicants, present a strong case that the polygraph serves as an efficient and effective cost-containment hiring tool. When admissions made by a subject during a polygraph test result in a disqualification, these agencies are saved the considerable cost and time of conducting a background investigation. In addition, the CIA's Office of Medical Services reported to the Commission that full-scope polygraphs enable

it to detect and screen out 50 percent to 75 percent of the most troubled applicants. While senior officials at the CIA and the NSA acknowledge the controversial nature of the polygraph process, they also strongly endorse it as the most effective information gathering technique available in their personnel security systems. They argue that without the polygraph, the quality of their work force would suffer immeasurably.


(U//~~FOUO~~) Every CIA, NSA and DIA polygraph examiner that we interviewed echoed those sentiments. The Acting Chief of the CIA Polygraph Office characterized the pre-employment screening polygraph as an effective means to gauge the conduct of background investigations. Additionally, CIA officials believe the screening exam is a cost- and time-effective segment of the hiring process; that is, temporary access can be granted to an employee pending completion of a full background investigation. Finally, the polygraph process is seen as a security deterrent because new CIA employees are made aware of behavior they should avoid during their career. The Chief of the CIA Personnel Security Group wrote that, "As a matter of business practice, the Agency does conduct polygraph testing as early as possible in the applicant process. This allows the Agency to use suitability information obtained during polygraph testing at the earliest point possible in applicant processing."

(U//~~FOUO~~) The Chief of the DIA Polygraph Branch told us that, with increased polygraph assets (20 polygraph examiners and 11 examination rooms), the DIA Polygraph Branch will be capable of conducting pre-employment CSPs. He contends that pre-employment polygraphs are more desirable for two reasons. First, it is far easier not to hire individuals with security issues than it is to fire them. Second, a pre-employment CSP assists background investigators in investigating security issues raised during an examination. The Chief concluded that pre-employment CSP examinations save time and money by greatly reducing the time it takes to conduct a background investigation.

## (U) Recommendation 5

(U//~~FOUO~~) We recommend that the Director, Defense Intelligence Agency use pre-employment Counterintelligence Scope Polygraph examinations for every Defense Intelligence Agency position that requires access to Top Secret material.

(U//~~FOUO~~) **Management Comments.** The Director, DIA concurred in principle with our recommendation and stated that all DIA employees are required to have a Top Secret SCI security clearance. <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>





(U//~~FOUO~~) The Under Secretary of Defense for Intelligence commented that, currently, the Director, DIA has the authority to designate positions as critical intelligence positions that would be subject to CSP testing to assist in determining their eligibility for employment. However, any additional increase in personnel awaiting CSP examinations before entering on duty could create a backlog that may effectively delay employment start dates and cause a possible shift in internal priorities within the broader DIA polygraph missions. The Under Secretary stated that the legislative proposal that DoD submitted to update its polygraph directive would authorize all Components to implement CSP examinations as they deem necessary in determining initial eligibility for personnel for assignment to critical or sensitive positions based upon certain risk assessment criteria.

## (U) Finding 6

(U//~~FOUO~~) The DIA does not retain in perpetuity the charts of CSP examinations.

(U) The DIA administers an effective CSP program. Evidence that DIA complies with DoD policy and procedures and meets the standards of a Federal Government polygraph program is found in the results of numerous DoD Polygraph Institute annual inspections. <sup>DIA (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

(U) All DIA personnel in positions designated by the Director, DIA as critical intelligence positions are, as a condition of employment, periodically subjected to CSP examinations. The authority to administer a CSP is contained in DoD Directive 5210.48. The Directive states that the scope of the polygraph examination must be limited to counterintelligence topics. Questions permitted pursuant to the Directive are:

- Have you ever engaged in espionage or sabotage against the United States?
- Do you have knowledge of anyone who is engaged in espionage or sabotage against the United States?
- Have you ever been approached to give or sell any classified materials to unauthorized persons?
- Have you ever given or sold any classified materials to unauthorized persons?
- Do you have knowledge of anyone who has given or sold classified materials to unauthorized persons?
- Have you had any unauthorized contact with representatives of a foreign government?

(U//~~FOUO~~) <sup>DIA (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

(U//~~FOUO~~) DoD Regulation 5210.48-R stipulates that polygraph examination results should be destroyed within 3 months from completion of the investigation in which the polygraph was authorized; however, the policy is flawed and outdated. <sup>DIA (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>



DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)

(U//~~FOUO~~) ~~DoD IG: (b)(1), 1.4(c)~~ may not have been of much assistance to investigators as they sought to identify an unknown subject believed to be conducting espionage on behalf of Cuba, but they may have provided valuable insight in terms of comparative analysis for the post-arrest period when Montes had to submit to polygraph examinations as a condition of her plea agreement with the U.S. Government. Those examinations are expected to continue indefinitely to test Montes' cooperation with the U.S. Government.

(U//~~FOUO~~) As a result of management comments, we revised Recommendation 6 to indicate that all DoD entities with polygraph programs should digitize and retain all CSP examination charts for a minimum of 35 years.

## (U) Recommendation 6

(U//~~FOUO~~) We recommend that the Under Secretary of Defense for Intelligence direct all DoD entities with polygraph programs to digitize and retain for a minimum of 35 years all Counterintelligence Scope Polygraph examination charts.

(U//~~FOUO~~) **Management Comments.** The Under Secretary of Defense for Intelligence concurred with our recommendation and stated that a requirement will be incorporated in the revision of DoD Regulation 5210.48-R to digitize and retain the charts for 35 years.

## (U) Finding 7

(U//~~FOUO~~) The DIA does not use a coordinated approach to determine prospective employee suitability.

(U//~~FOUO~~) The CIA and the NSA use a multidisciplinary coordinated approach to determine prospective employee suitability. They coordinate the work of personnel specialists, security officials, polygraph examiners, and psychologists in a logical and systematic way to make hiring decisions. The DIA, an organization with far fewer employees than the CIA or the NSA, does not employ those techniques.

(U//~~FOUO~~) The CIA and the NSA use a holistic approach to vetting prospective employees through the security clearance process. When a CIA applicant has "clean" polygraph charts, that individual can be granted temporary access to classified information pending completion of a full background investigation. The CIA uses a panel of medical, psychological, security and personnel professionals to scrutinize those applicants with security or unresolved polygraph difficulties. Should a prospective NSA employee have security or unresolved polygraph difficulties, the application goes before an NSA Application Panel which is similar to the CIA panel. The NSA panel addresses suitability and security issues that might have surfaced during an applicant's background investigation.

(U//~~FOUO~~) When Ana Montes applied for a position in 1985, DIA security clearance adjudication standards were codified in DIA Regulation 50-8, "Personnel Security Program," October 2, 1975, which stipulated that granting a security clearance must be based on common sense using all available information. The basic criteria for granting security clearances were: excellent character, discretion, and unquestioned loyalty to the United States; and the applicant and members of the immediate family had to be citizens of the United States. Regulation 50-8 also listed 21 supplemental criteria for not granting a security clearance, including espionage, the forceful overthrow of the U.S. Government, criminal acts, and other nefarious activity.

(U//~~FOUO~~) In August 1985, the DIA Security Office ordered an initial Personnel Security Review of Montes, and a DIA investigator conducted a pre-employment interview of her. On August 23, 1985, the DIA Security Office notified the Personnel Office that it did not object to tendering a formal job offer to Montes and, if she accepted the position, she would be eligible for an interim Top Secret clearance upon entering duty with DIA. Montes began her career with DIA on September 30, 1985. She was granted an interim Top Secret clearance pending completion of a background investigation, which was initiated by the Personnel Security Division on October 2, 1985. Unlike the CIA or NSA, the DIA did not, and still does not, use polygraph screening or psychological testing as a precursor to employment. In 1985, prospective DIA employees, including military members, were only subjected to comprehensive background investigations. As a result, the background investigation and a cursory DIA security investigation formed the basis for evaluating Montes' eligibility for access to classified information.



(U//~~FOUO~~) In June 1986, DIA completed the background investigation initiated shortly after Montes began her employment with the agency. Several security concerns were raised, including falsification of her Master of Arts degree from Johns Hopkins and her trustworthiness. <sup>DIA (b)(3), 10 U.S.C. § 424</sup>

<sup>DIA (b)(3), 10 U.S.C. § 424</sup> determined that because Montes was a probationary employee, her <sup>DIA (b)(6)</sup> should be reviewed by the Personnel Office for possible dismissal action. A series of discussions and informal notes to the Personnel Office and the DIA Office of the General Counsel followed, but no formal action was ever taken. As a result, Montes was certified eligible for SCI. Montes' <sup>DIA (b)(6)</sup> posed numerous difficulties for DIA; officials could not agree whether the claim was a security or a personnel issue.

(U//~~FOUO~~) The Director, DIA declared all positions to be categorized as critical intelligence positions. The June 1995 DIA Manual, "DIA Personnel Security Program, DIA Manual 50-8," indicates that all DIA positions are "special sensitive," thus personnel in those positions require access to SCI. The 1997 National Counterintelligence Center report, "A Review of Security and Counterintelligence Findings from Community Damage Assessments," suggests that candidates for particularly sensitive positions may warrant coordinated examinations by personnel specialists, psychologists, polygraph examiners, and security officials. The CIA and the NSA have heeded this advice; the DIA has not.

## (U) Recommendation 7

**(C) We recommend that the Director, Defense Intelligence Agency institute a coordinated employee vetting program that uses personnel specialists, security officials, polygraph examiners, and psychologists to determine the suitability of prospective employees.**

**(C) Management Comments.** The Director, DIA concurred in principle with our recommendation and stated that senior DIA personnel and security officers will coordinate with CIA and NSA officials to assess their applicant and employee suitability review programs and make appropriate recommendations to the Director, DIA in August 2005. When the DIA determines the resource and funding implications, the Director will decide what can be done within existing resources, and will seek additional resources, if required. The Under Secretary of Defense for Intelligence supports this recommendation.

**(C) Review Response.** We consider management comments to be responsive to our recommendation. We request that the DIA provide us with the results of its assessment of the CIA and NSA applicant and employee suitability review program, and DIA actions contemplated within 6 months of the date of this report.



## (U) Finding 8

(U//~~FOUO~~) The current counterespionage force structure at DIA is inadequate to meet the needs of the agency. Several attempts to resolve this shortcoming have not survived the Foreign Counterintelligence Program budget process. The DIA <sup>DIA (b)(3), 10 U.S.C. § 424</sup> identifies Foreign Counterintelligence Program shortfalls through the program build process. Once a year DIA reaffirms its base budget and identifies shortfalls in funding for current and future missions (2 years out). DIA ranks these shortfalls and submits them as either unfunded requirements or overguidance to the DIA Financial Executive Staff. The Financial Executive Staff consolidates all DIA Foreign Counterintelligence Program submissions and ranks them as an agency priority before submitting the package to the Program Manager for the Foreign Counterintelligence Program, CIFA.

(U//~~FOUO~~) Furthermore, DIA has difficulty retaining highly skilled counterintelligence investigators because the agency cannot offer the 25 percent Law Enforcement Availability Pay differential that investigators at other agencies receive as an added incentive.

(U//~~FOUO~~) In an agency with approximately <sup>DIA (b)(3), 10 U.S.C. § 424</sup>, the DIA currently has <sup>DIA (b)(3), 10 U.S.C. § 424</sup> Special Agents responsible for countering espionage. During the lengthy period leading to the identification of Ana Montes as a penetration agent for the Cuban Intelligence Service and <sup>FBI (b)(7)(E)</sup> that followed, when <sup>DIA (b)(3), 10 U.S.C. § 424</sup> Special Agents were assigned to DIA, <sup>DIA (b)(3), 10 U.S.C. § 424</sup> devoted more than 90 percent of their time focusing on Montes. Other matters, ranging from mundane to crucial, were given little or no attention.

(U//~~FOUO~~) Recognizing the retention problem, DIA has submitted a Foreign Counterintelligence Program initiative labeled "Counterintelligence (CI) Investigations Support Growth," every year since 2002. The initiative would add <sup>DIA (b)(3)</sup> investigators to upgrade the "extremely limited" DIA counterintelligence investigative capability, the reason being that additional personnel would allow greater coverage of counterintelligence and security interviews of all newly assigned or hired civilian and military personnel, counterintelligence debriefings of all personnel departing DIA, an upgraded counterintelligence review of all foreign contacts by DIA personnel, and an upgraded counterintelligence review and assessment of all unofficial travel by DIA personnel. Finally, the initiative pointed out that without increased force structure, "The ability to deter DIA personnel from taking steps to engage in espionage on behalf of a foreign power and the ability to detect DIA personnel already potentially serving as foreign spies will remain hindered."

(U//~~FOUO~~) To date, the initiative has not received sufficient priority among other DoD Foreign Counterintelligence Program priorities to warrant funding approval. The Senior Program Manager recognized that since September 11, 2001, counterintelligence programs supporting the Global War on Terrorism have received the highest Foreign Counterintelligence Program ranking. Counterespionage enhancements have not fared nearly as well.

(U//~~FOUO~~) <sup>DIA (b)(3), 10 U.S.C. § 424</sup> indicated that additional security investigator positions authorized under the General Defense



Intelligence Program budget have improved the capability of his organization. However, the number of counterintelligence and counterespionage positions governed by the Foreign Counterintelligence Program has remained static. The <sup>DIA (b)(3), 10 U.S.C. § 424</sup> mentioned that the investigations office has difficulty attracting qualified applicants because DIA does not offer pay incentives and cannot compete with other agencies or private contractors for the talent required to accomplish its mission. Proposals for incentive pay have been rejected by the DIA Human Resources Directorate. Comments made by the <sup>DIA (b)(3), 10 U.S.C. § 424</sup> illustrate the point. He said that although he received authority to hire several security investigators, he could not attract qualified applicants because he could not offer salary incentives. He lamented that he had difficulty retaining investigators because, once trained, they look for opportunities with other agencies that offer incentive pay. Finally, he said that the <sup>DIA (b)(3), 10 U.S.C. § 424</sup> caseload has <sup>DIA (b)(3), 10 U.S.C. § 424</sup> since 2000 and, as a result, the organization has become reactive rather than proactive because of personnel constraints.

(U//~~FOUO~~) As a result of management comments, we revised Recommendation 8 to clarify that DIA counterintelligence personnel cannot receive Law Enforcement Availability Pay.

## (U) Recommendation 8

(U//~~FOUO~~) We recommend that the Director, Counterintelligence Field Activity address and give high priority to the Defense Intelligence Agency Foreign Counterintelligence Program initiative to upgrade the Defense Intelligence Agency counterintelligence investigative capability.

(U//~~FOUO~~) **Management Comments.** The Under Secretary of Defense for Intelligence partially concurred with our recommendation. The Under Secretary stated that DoD policy does not authorize DIA personnel to conduct counterintelligence investigations. Counterintelligence personnel in DIA are not classified as 1811 Criminal Investigators and thus no link exists to Law Enforcement Availability Pay. They may conduct initial inquiries until a determination is made that an investigation is warranted. At that point, the matter is referred to the FBI or to the Military Department counterintelligence investigative agency that has Title X responsibility for conducting the investigation. All organizations with organic counterintelligence personnel should use existing policies and programs to attract and retain the necessary counterintelligence expertise.

(U//~~FOUO~~) **Review Response.** We consider management comments to be responsive to our recommendation. We recognize that DIA counterintelligence investigators are not classified as 1811 Criminal Investigators and, as such, do not qualify for Law Enforcement Availability Pay. Nonetheless, DIA is woefully short of qualified, highly skilled counterintelligence investigators. Timely and positive action is warranted in response to DIA Foreign Counterintelligence Program requests for an upgraded capability.

## (U) Finding 9

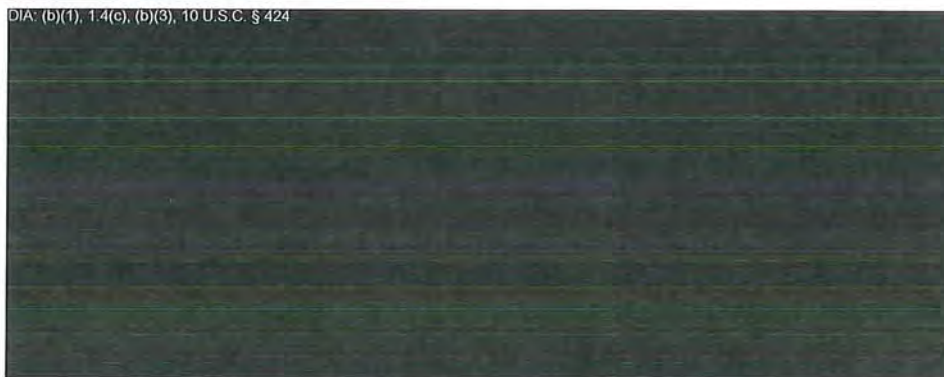
(S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>




(S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>



<sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>



(S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>



(U//FOUO) In an August 24, 1999, memorandum, "Changes to Special Access Program Oversight Committee Procedures and Organization," the Deputy Secretary of Defense ordered the Director of the Special Access Program Oversight Committee to develop a plan to consolidate all program access clearances into an integrated database. The Chief of Security for the Under Secretary of Defense (Acquisition, Technology, and Logistics/Special Programs),



who is responsible for implementing a DoD-wide SAP database, told us that the Military Departments had to standardize security forms and procedures and resolve reciprocity issues before the integrated access database could become a reality. However, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics continued its pursuit of a centralized SAP registry. The 2002 Defense Planning Guidance included language that directed the Under Secretary of Defense for Acquisition, Technology and Logistics, the ASD(C<sup>3</sup>I), and the Under Secretary of Defense for Policy to formulate a Program Objective Memorandum funding request to support the development of an integrated SAP information management system. The information management system will include databases to manage budget, personnel access, security information, and archiving requirements, among others issues. Consideration will also be given to integrating Military Department and defense agency SAP databases into the architecture of the information management systems.

(U//~~FOUO~~) On June 6, 2003, the Defense Advanced Research Project Agency was given Executive Agent responsibilities for the SAP information management system and was directed to field the system by 2007. Once fielded, system operations and resource responsibilities will shift to the SAP Coordination Office, which will retain oversight responsibility. On May 28, 2004, the Under Secretary of Defense for Acquisition, Technology, and Logistics promulgated specific requirements for the system and implemented the August 1999 Deputy Secretary of Defense order to develop a single DoD personnel access database that "creates a single common authoritative information reference for personnel security information and SAP access." The Chief of Security for the Under Secretary of Defense (Acquisition, Technology, and Logistics/Special Programs) said that the DoD SAP information management system would be tested in March 2005 and is expected to become fully operational in early 2007. Computer "hubs" are scheduled to be placed at all combatant commands and Defense agencies, as appropriate, before the system becomes operational.

## (U) Recommendation 9

a. (C) We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics continue the process of establishing a DoD central registry for personnel with access to Special Access Programs.

b. (C)

<sup>DoD(G) (b) (1), 1.4(c), (b) (3), 10 U.S.C. § 424</sup>

(C)

<sup>DoD(G) (b) (1), 1.4(c), (b) (3), 10 U.S.C. § 424</sup>



## (U) Finding 10

(U//~~FOUO~~) The DIA does not have Standard Operating Procedures for counterintelligence inquiries that lead to support of counterespionage investigations conducted by the FBI or the Military Departments.

(~~C~~) DIA counterintelligence Special Agents were aggressive and proactive in identifying Ana Montes as a suspected espionage agent and provided outstanding support to the FBI during the nearly year-long investigation leading to her arrest. However, DIA does not have Standard Operating Procedures for undertaking inquiries that may result in FBI or Military Department counterespionage investigations. The lack of specific procedures caused some confusion in coordinating actions within the DoD and with the FBI, and may have delayed the identification of Montes as the individual who fit the profile of the sought after Cuban spy.

(~~C~~) The <sup>DIA (b) (3)</sup> long-tenured counterintelligence Special Agents in the <sup>DIA (b) (3), 10</sup> never possessed Standard Operating Procedures. The Special Agents always used an informal ad hoc approach to problem solving. As evidence mounted that pointed toward Montes, the Special Agents did not appreciate the procedures to effect liaison and coordination with the FBI and the Office of the Secretary of Defense. When the Special Agents began to seriously focus on Montes in September 2000, they tried to convince the FBI of their judgment through personal contacts with the Washington Field Office. This informal approach eventually resulted in the FBI decision <sup>FBI (b) (7)(E)</sup> ~~\_\_\_\_\_~~. <sup>FBI (b) (7)(E)</sup> ~~\_\_\_\_\_~~.

(~~C~~) Had DIA possessed Standard Operating Procedures, the Special Agents would have known that counterespionage concerns must be formally presented in writing to FBI Headquarters using an 811 referral as outlined in the June 1996 supplement to the 1979 FBI/DoD Memorandum of Understanding, and Section 811(c) of the Intelligence Authorization Act of 1995. Section 811 of the Intelligence Authorization Act of 1995, 50 U.S.C. section 402a, governs the coordination of counterespionage investigations between Executive Branch agencies and the Military Departments and the FBI. Section 811 referrals advise the FBI of any information, regardless of its origin, which may indicate that classified information is being or may have been disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. The Special Agents also would have known that the Under Secretary of Defense for Intelligence must be promptly advised of any significant counterintelligence referrals to the FBI in accordance with DoD Instruction 5240.6, "Counterintelligence Awareness Briefing Program," July 16, 1996. Had DIA forwarded the 811 referral, the FBI may have been formally alerted to the critical nature of the undertaking and may have acted more swiftly to label Montes the suspect. Alerting the Under Secretary of Defense for Intelligence might have sensitized the issue within the DoD sooner than it did.

(U//~~FOUO~~) As a result of management comments, we revised Recommendation 10 to clarify that DIA does not have Standard Operating Procedures for counterintelligence inquiries that lead to support of counterespionage investigations conducted by the FBI or the Military Departments.



## (U) Recommendation 10


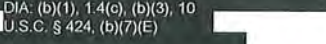
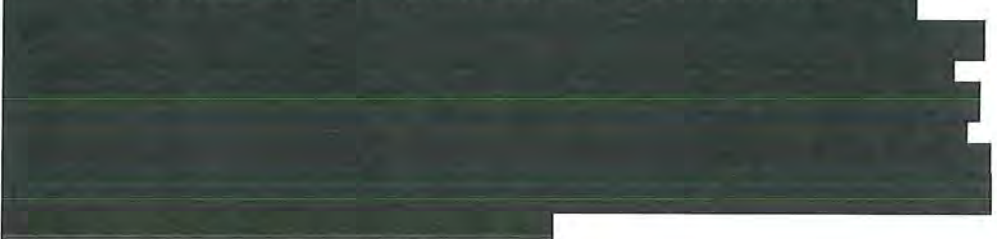
~~(C)~~ We recommend that the Director, Defense Intelligence Agency develop and issue Standard Operating Procedures for counterintelligence inquiries that lead to counterespionage investigations in support of the Federal Bureau of Investigation or the Military Departments.



~~(C)~~ **Management Comments.** The Director, DIA concurred with our recommendation and stated that a revision of the DIA manual on security investigations will contain a section dedicated to the conduct of espionage inquiries. The revision will be completed in August 2005.

## (U) Finding 11

(S//NF) During the latter stages of the Montes investigation, the DIA could have jeopardized the outcome by not strictly following Operations Security procedures.

(S//NF) During the latter stages of the Montes investigation, DIA officials did not strictly follow Operations Security e-mail procedures on the Joint Worldwide Intelligence Communications System. The mission of the Joint Worldwide Intelligence Communications System is to deliver secure information to intelligence consumers around the world. This Operations Security deficiency could have jeopardized the outcome of the investigation. Operations Security is the process of identifying critical information and analyzing friendly actions to identify actions that can be observed by adversary intelligence systems, determine indicators that hostile intelligence systems might obtain that could be pieced together to derive critical information useful to adversaries, and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.


(S//NF) <sup>FBI: (b)(7)(E)</sup>  <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup> The next day, in support of the investigation,   


(S//NF) On October 30, 2000, <sup>DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>   



(S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(7)(E)</sup>   





DIA: (b)(1), 1.4(c), (b)(7)(E)




(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c), (b)(7)(E)




(S//NF) FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



(S//NF) DoD IG: (b)(1), 1.4(c); FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1); DIA: (b)(1), 1.4(c)



(S//NF) All of the e-mail messages cited above were sent during the period when DIA was conducting <sup>DIA: (b)(1), 1.4(c)</sup> 

DIA: (b)(1), 1.4.(c)

[REDACTED] In this case, prudent Operations Security procedures were not evident.

(S//NF) While examining DIA Operations Security practices during the Montes investigation, we conducted a forensic analysis of more than 3,000 e-mails. We found that at least 85 DoD employees had knowledge of the FBI Montes investigation. Those individuals included officials in the Office of the Secretary of Defense, the DIA, <sup>DoD IG: (b)(1), 1.4.(c)</sup> [REDACTED] and the National Reconnaissance Office. The list did not include FBI and CIA officials who may have been aware of the investigation. Although the number seems excessive, certain officials such as those in the offices of the General Counsel, the CIFA, the Under Secretary of Defense for Intelligence, and many others had a rightful need to know. Although it is recognized that the DIA SAFE System and the Joint Worldwide Intelligence Communications System e-mail application are separate systems maintained by different technicians with unique internal authorities and capabilities, sensitive counterespionage investigations require cautious action; the fear of compromise cannot be overstated.

## (U) Recommendation 11

(C) We recommend that the Director, Defense Intelligence Agency reevaluate the Operations Security risks associated with using the Joint Worldwide Intelligence Communications System to disseminate close-hold information during counterespionage investigations.

(C) Management Comments. <sup>DIA: (b)(1), 1.4.(c)</sup> [REDACTED]

(C) The Under Secretary of Defense for Intelligence indicated that the Deputy Under Secretary of Defense for Counterintelligence and Security already directed through a memorandum to the field that all counterintelligence investigative reporting will be submitted via Portico, a secure communications network for the counterintelligence community. The upcoming revision of DoD Instruction 5240.4, "DoD Counterintelligence Investigations and Significant CI Activity Reporting," will codify the requirement for investigations to be reported through Portico.



## (U) Observation 1

(U//~~FOUO~~) After Ana Montes was identified as a suspect, the investigation leading to her arrest and conviction was a model of efficiency and effectiveness.

(S//NF) On October 13, 2000, DIA counterintelligence Special Agents and FBI Special Agents met to discuss the profile of a Cuban unknown subject. The DIA officials presented compelling evidence that Montes fit the profile. The FBI believed that the DIA officials had presented sufficient evidence to <sup>FBI (b)(7)(E)</sup> ~~\_\_\_\_\_~~ <sup>FBI (b)(7)(E)</sup> From that day forward, through the arrest of Ana Montes on September 21, 2001, the FBI, the DoD, and the DIA collaborated and cooperated with such profound professionalism that the FBI-led investigation could easily be used as a model for the future. Hallmarks of the investigation included collegial sharing of information in a timely fashion; continuous and continual feedback of actions planned or taken; and senior leadership involvement. Without exception, every FBI, DoD, and DIA official we encountered during our review told us that the Montes investigative process unfolded seamlessly and prompted them to conclude that it was the very best counterespionage investigation they had ever experienced.

(S//NF) DIA counterintelligence Special Agents and FBI Special Agents provided weekly updates on the Montes case to the JCEO who, in turn, provided numerous timely briefings and information papers on the case to the SECDEF and Deputy Secretary of Defense, the ASD(C<sup>3</sup>I), and other senior DoD officials. FBI and DIA Special Agents frequently briefed the Director and Deputy Director, DIA on the progress of the case. The Director, DIA stated that when he learned that the agency may have had "a spy in our midst," he knew that it was extremely important to coordinate everything related to the case with the FBI. Particularly noteworthy was the FBI desire to consult with the Director, DIA to receive advice on matters uniquely related to the agency. The Director, DIA also met regularly with the DCI and senior FBI officials to discuss the ongoing investigation and to outline a contingency plan that would eventually lead to the arrest of Montes. He also regularly conferred with the Senior Military Assistant to the Secretary of Defense and was apprised of the FBI presentations to the congressional intelligence oversight committees on the status of the investigation. Although the Director, DIA was somewhat frustrated by the slow pace of the investigation, particularly given the magnitude of the case and its potential impact on national security, he understood that the FISA Court would deliberate and eventually provide the necessary authority to proceed. In sum, the Director, DIA said that he "was comfortable with what was being done and was well informed."

(S//NF) A senior JCEO official stated that once the SECDEF knew about the case, the Montes investigation became the best example of information sharing with the FBI that the JCEO had ever seen. That sentiment was echoed many times over in our discussions with senior officials who were involved directly or functioned on the periphery of the Montes investigation. An FBI Special Agent's comments regarding the cooperation between agencies, typifies the latter stages of the investigation: "I briefed a multitude of officials within the Office of the Secretary of Defense, to include the Office of the General Counsel and provided periodic updates on the status of the case." He also briefed the Director, DIA every 2 weeks and said that the Director was very interested and wanted to make sure that DIA was doing everything possible to make the investigation successful.

Finally, he said that, "Our interaction with DIA was the best that I have experienced on any espionage case with any agency during my career."



## (U) Observation 2

(U//~~FOUO~~) Severely limited dissemination of damage assessments and other reports on espionage cases prevents opportunities to share lessons learned.

(U//~~FOUO~~) Damage assessments and reports detailing espionage cases perpetrated against the United States are valuable tools for decision makers and others engaged in countering that inimical threat to national security. We recognize that responsible distribution of those reports is both prudent and wise and that the need-to-know principle must be strictly enforced. However, our experience in attempting to gain access to reports on recent espionage cases warrants repeating so that future reviews and evaluations can prevent delay and obfuscation. More importantly, sound lessons learned cannot be applied without an awareness of shortcomings, failings, and successful actions aggregated from past espionage activities.

(S//~~NF~~) The House Permanent Select Committee on Intelligence charged the Department of Defense Inspector General to use the basic framework of the Robert Hanssen and Aldrich Ames reports, authored by the Inspectors General of the DoJ and the CIA, respectively, as guides to accomplish the Montes evaluation. We learned that the DoJ had issued three separate reports on the Hanssen case--one highly classified with restricted access; one classified Secret//No Foreign Dissemination; and one 31-page unclassified Executive Summary -- "A Review of the FBI's Performance in Detering, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen." The House Permanent Select Committee on Intelligence provided us a copy of the 31-page unclassified Executive Summary. In our attempt to comply with congressional direction, we asked the DoJ and then the FBI for a copy of the Secret//No Foreign Dissemination report on Hanssen; we were denied access. We sought guidance and support from the House Permanent Select Committee on Intelligence and were advised that we could only obtain the document from the originator. Out of options, we discontinued our effort to obtain a document that would have significantly assisted us in formulating the framework for this report. We experienced no such difficulty in obtaining access to the CIA report on Ames.

(S//~~NF~~) Reluctance to share information of this sort is not unique or particularly surprising. The 1997 National Counterintelligence Center, "Review of Security and Counterintelligence Findings from Community Damage Assessments," complained about the narrow distribution of reports on the Ames case. The review indicated that the Ames Damage Assessment Team, under the direction of the Community Management Staff, completed its report in 1995. That review and earlier reports issued by the CIA Inspector General, the House Permanent Select Committee on Intelligence, and the Senate Select Committee on Intelligence did not contain separate sections on counterintelligence and security. And, except for the congressional reports, which were unclassified, none of the reports or assessments listed in the National Counterintelligence Center's 1997 review received wide distribution in the Intelligence Community or in the DoD. The Center concluded that the damage assessments "were so highly classified and tightly controlled. . . that the reports went to just a handful of U.S. Government offices."

### (U) Observation 3

(U//FOUO) <sup>FBI, (b)(7)(E)</sup> [REDACTED]

(U//FOUO) <sup>FBI, (b)(7)(E)</sup> [REDACTED]

. The National Commission on Terrorist Attacks Against the United States, Staff Statement Number 9, "Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11," suggests a similar view.

The poor state of the FBI's information systems meant that analysts' access to information depended in large part on their personal relationships with individuals in the operational units or squads where the information resided. In short, analysts didn't know what they didn't know ... The FBI's primary information management system, designed using 1980s technology already obsolete when installed in 1995, limited the Bureau's ability to share its information internally and externally. The FBI did not have an effective system for storing, searching, or retrieving information of intelligence value in its investigative files.


(S//NF) <sup>FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> [REDACTED]

(S//NF) <sup>FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> [REDACTED]


(S//NF) <sup>FBI, (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup> [REDACTED]



(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>




(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>




## (U) Observation 4

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>



(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>

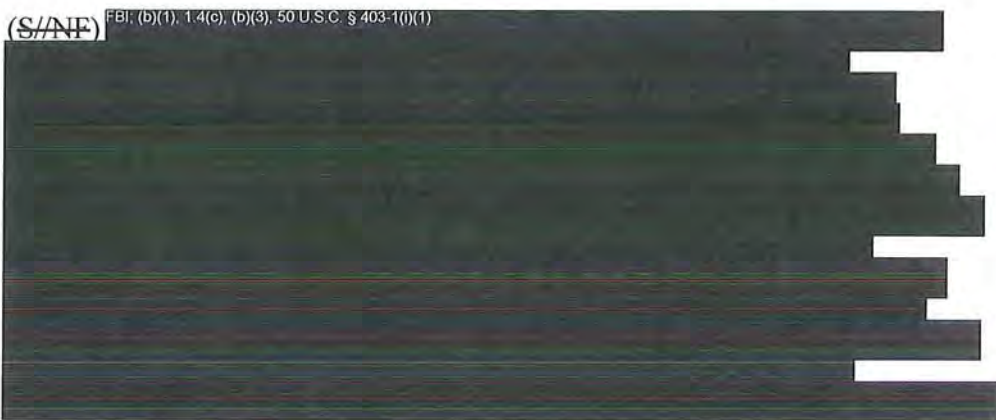


(U//~~FOUO~~) The National Commission on Terrorist Attacks Against the United States, Staff Statement Number 9, outlines FBI strategic analysis difficulties with respect to terrorism. The Staff Statement said:

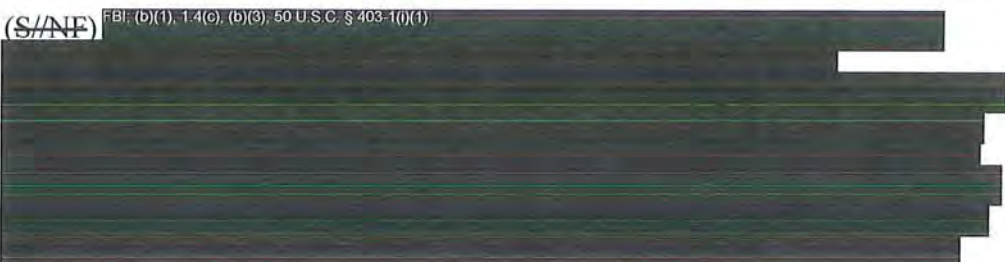
It is the role of the strategic analyst to look across individual operations and cases to identify trends in...activity and develop broad assessments of the...threat to U.S. interests. The goal is not abstract. Such analysis drives collection efforts. It is the only way to evaluate what the institution does not know. The FBI had little understanding of, or appreciation for, the role of strategic analysis in driving investigations or allocating resources. FBI agents failed to see the value of strategic analysis, finding it too academic and therefore irrelevant, and...analysts did not know what they didn't know.

We observed similar circumstances regarding counterespionage.

(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>




(S//NF) <sup>FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)</sup>






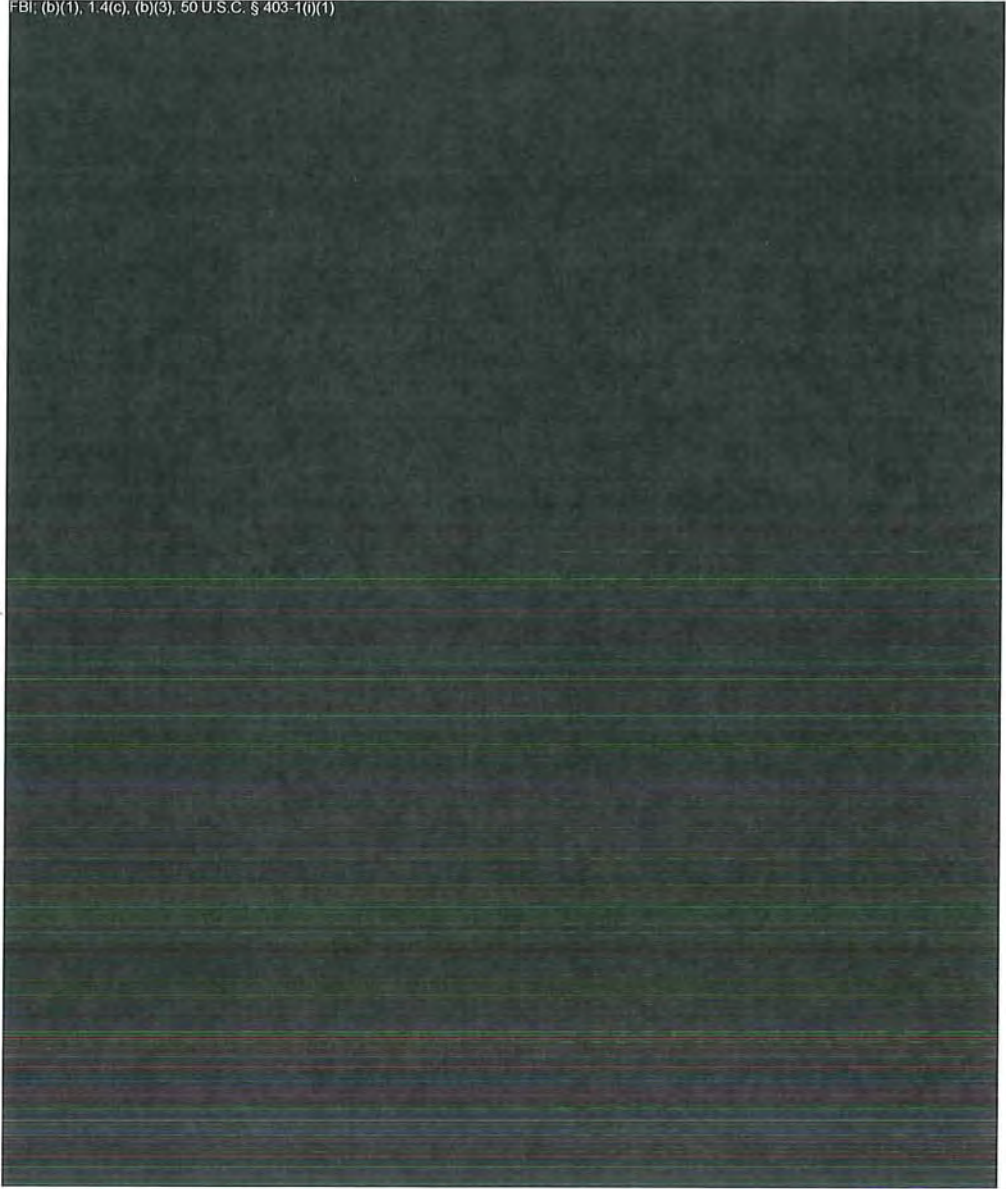
FBI; (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



(S//NF) FBI; (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



FBI; (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)



## (U) Observation 5

(U//~~FOUO~~) The DIA's adoption of risk management as the operating information technology philosophy successfully postulates that it is possible to balance the risk of disclosure against the cost of protection.

(U//~~FOUO~~) The DIA <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED] has adopted a risk management perspective. According to its <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED] to be cost-effective and efficient in a risk management environment, DIA categorizes its employees as trustworthy.

(U//~~FOUO~~) The vast majority of DIA civilian and military employees require access to highly classified and extremely sensitive information. Those employees must, out of necessity, be screened and vetted prior to assignment to the agency. A DIA employee gains access to DIA information systems when, depending on the level of access required, the employee's supervisor requests that access through the <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED] reviews a database showing all employee clearances and then grants the employee the required access. Should an employee require access to a different system, for example a CIA database, the employee must obtain that access through the CIA. <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED] is notified when an employee departs DIA and it then terminates that individual's computer accesses.

(S//NF) The DIA information technology policy of risk management is an effective way to provide employees with broad access to classified information while limiting the risks to national security. The DIA provides employees with access to information technology platforms based on need to know. Ana Montes indicated that she did not download classified information from her system, neither did she stray outside her area of expertise because she feared that the DIA monitored her computer at all times. Having received DIA information technology security awareness training, Montes was mindful that her computer was always prone to being monitored. The DIA proactively informed its employees that their systems were susceptible to monitoring at any time. That warning, coupled with security awareness training, may have deterred Montes from downloading classified information from her work station to supply hard copy information to the Cubans. We found no evidence to suggest that Montes ever secreted classified information on her person and carried it out of her work place for delivery to the Cubans.

(S//NF) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED] that security rules and regulations cannot guarantee that individuals will adhere to those standards. Nevertheless, <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6</sup> [REDACTED], clear articulation of the standards, bolstered by strict enforcement of security procedures, can create an atmosphere that promotes security awareness and may help deter or prevent espionage.

(U//~~FOUO~~) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED] protects DIA information systems, develops and promulgates policies related to those systems, and protects information systems in a way that is comparable to other Intelligence Community agencies. DIA Regulation 50-23, "DIA Information Systems Security



(INFOSEC) Management,” March 1, 2002, is the primary operating document for DIA information systems.

(U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup> [REDACTED]

(U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED] is also responsible for the Joint Worldwide Intelligence Communications System used by the DoD. The <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup> [REDACTED]

(U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup> [REDACTED]

THIS PAGE INTENTIONALLY LEFT BLANK (U)



## (U) Part VII. Appendixes

THIS PAGE INTENTIONALLY LEFT BLANK (U)



## (U) Appendix A. Montes' Official and Unofficial Travel

### (U) 1987

- (C) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

### (U) 1988

- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

### (U) 1989

- (S//NF) <sup>DIA: (b)(1), 1.4(c)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

### (U) 1990

- (S//NF) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

### (U) 1991

- (U) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1992

- (U) None.

(U) 1993

- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> <sup>NSA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 402 note; DIA: (b)(3), 10 U.S.C. § 424</sup> <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

(U) 1994

- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> <sup>NSA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 402 note; DIA: (b)(3), 10 U.S.C. § 424</sup> <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]



(U) 1995

- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> <sup>NSA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 402 note; CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

(U) 1996

- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> <sup>NSA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 402 note; CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> <sup>NSA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 402 note; CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6; DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

(U) 1997

- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1998

- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, FBI; (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-10(1); DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]



(U) 1999

- (S//NF) <sup>DIA: (b)(1), 1.4(c)</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

(U) 2000

- (S//NF) <sup>DIA: (b)(1), 1.4(c)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c)</sup> [REDACTED]
- (S//NF) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]
- (U) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 2001

- (U) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> [REDACTED]

THIS PAGE INTENTIONALLY LEFT BLANK (U)



## (U) Appendix B. Montes' Awards, Recognition, and Training

### (U) 1985

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

### (U) 1986

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].

### (U) 1987

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].

### (U) 1988

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED].

(U) 1989

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1990

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1991

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1992

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]



(U) 1993

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1994

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1995

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1996

- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//~~FOUO~~) <sup>DIA: (b)(6)</sup> [REDACTED]

- (S//NF) <sup>DIA: (b)(6)</sup> [REDACTED] <sup>CIA: (b)(1), 1.4 (c), (b)(3), 50 U.S.C. § 403, Sec. 6, DIA: (b)</sup>

(U) 1997

- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1998

- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 1999

- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED] a.
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 2000

- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]

(U) 2001



- (FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]
- (U//FOUO) <sup>DIA: (b)(6)</sup> [REDACTED]

THIS PAGE INTENTIONALLY LEFT BLANK (U)




## (U) Appendix C. Background on the Brothers to the Rescue Incident

(U) The Brothers to the Rescue is one of several Cuban exile groups based in Florida.<sup>35</sup> A group of Cuban exiles formed the organization in 1991 as an air search and rescue force to provide humanitarian assistance to refugees fleeing Cuba in small boats and rafts. When the "rafter" exodus slowed in 1994, the focus of the group's activities shifted. In July 1995, while a flotilla of small boats organized by another Cuban exile group conducted a political demonstration off the Cuban coast, the president of the Brothers to the Rescue, Mr. Jose Basulto, flew his Cessna 337 aircraft over Havana, dispersing propaganda leaflets and religious objects. A television reporter accompanied Mr. Basulto and videotaped the streets of Havana from the Brothers to the Rescue aircraft. A Miami television station later aired the videotape. A Cuban Air Force fighter did escort Mr. Basulto's aircraft in Cuban territorial airspace, but took no action against it.

(U) On two nights in January 1996, Brothers to the Rescue aircraft again dropped propaganda leaflets on Havana. The Cuban government charged that the aircraft violated Cuban territorial airspace. Mr. Basulto acknowledged that the Brothers to the Rescue dropped the leaflets. He stated, however, that Brothers to the Rescue aircraft released the leaflets outside of Cuban territorial airspace and the wind carried them over Havana. Apparently, the Cuban military did not detect the aircraft on either night.

(S) <sup>DoD IG: (b) (1), 1.4(c)</sup>



(U) On February 24, 1996, a group of three Brothers to the Rescue aircraft, led by Mr. Basulto, departed Opa Locka Airport in Miami. Mr. Basulto filed a flight plan for a search and rescue mission for Cuban "rafter" refugees. The area of the mission was approximately 25 nautical miles north of Havana. At approximately 3:00 p.m. Eastern Standard Time, just before the aircraft crossed the twenty-fourth parallel, marking the boundary between U.S. and Cuban Air Defense Identification Zones, two Cuban Air Force fighters launched from San Antonio de los Baños Airfield, which is southwest of Havana. At 3:21 p.m. and 3:28 p.m., respectively, the Cuban fighters intercepted and shot down the two trailing Brothers to the Rescue Aircraft. The lead Brothers to the Rescue aircraft entered and left Cuban airspace without incident. At 3:35 p.m., the Cuban Air Force launched a second pair of fighters. The second pair of fighters intercepted the

<sup>35</sup>(U) The description of the Brothers to the Rescue incident is extracted from the Office of the Inspector General of the Department of Defense, Policy and Oversight Report Number 97-011, "The DoD Response to the Brothers to the Rescue Incident, Phase I," March 28, 1997.

remaining Brothers to the Rescue aircraft, piloted by Mr. Basulto, approximately 25 nautical miles east of the shoot down area. They took no action against the aircraft. At 5:08 p.m., Mr. Basulto landed safely at Opa Locka Airport.



## (C) Appendix D. Montes' Accesses to Sensitive Programs and Information

(U//FOUO) This compilation of Montes' accesses is based upon data received from a variety of sources; it may not reflect the totality of Montes' access to sensitive programs. The list does not describe the substance of the sensitive programs and information to which Montes had access because in-depth knowledge of those programs and information is beyond the scope of this review.

(U//FOUO) DoD/G: (b)(1), 1.4(c);  
DIA: (b)(3), 10 U.S.C. §

(U//FOUO) DoD/G: (b)(1), 1.4  
(c); DIA: (b)(3), 10

(U//FOUO) DIA: (b)(3), 10 U.S.  
C. § 424

(S//NF) CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424

(S//NF) CIA: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403, Sec. 6, DIA: (b)(1),  
1.4(c), (b)(3), 10 U.S.C. § 424

(U//FOUO) CIA: (b)(1), 1.4  
(c), (b)(3), 50 U.

(U//FOUO) DIA: (b)(3), 10 U.S.C. §  
424

(S//NF) DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424

(U//FOUO) DoD/G: (b)(1), 1.4(c);  
DIA: (b)(3), 10 U.S.C. §

(U//FOUO) DoD/G: (b)(1), 1.4(c); DIA:  
(b)(3), 10 U.S.C. § 424

(U//FOUO) DoD/G: (b)(1),  
1.4(c), DIA: (b)

(U//FOUO) DIA: (b)(3), 10 U.S.C. §  
424

(U//FOUO) DIA: (b)(3), 10 U.S.  
C. § 424

(U//FOUO) DIA: (b)  
(3), 10

(U//FOUO) DIA: (b)(3), 10 U.S.  
C. § 424

(U//FOUO) DoD/G: (b)(1),  
1.4(c), DIA: (b)

(U//FOUO) DIA: (b)(3), 10 U.S.C. § 424

(U//FOUO) DoD/G: (b)(1), 1.4(c);  
DIA: (b)(3), 10 U.S.C. §

(U//FOUO) DIA: (b)  
(3), 10 U

(U//FOUO) DIA: (b)(3), 10  
U.S.C. § 424

(S//NF) [REDACTED] DIA: (b)(3), 10 U.S.C. § 424 [REDACTED]



(U//~~FOUO~~) Appendix E.

<sup>FBI: (b)(7)(E)</sup> [REDACTED]

(U//~~FOUO~~) <sup>FBI: (b)(7)(E)</sup> [REDACTED]

(U//~~FOUO~~) <sup>FBI: (b)(7)(E)</sup> [REDACTED]

THIS PAGE INTENTIONALLY LEFT BLANK (U)



## **(U) Appendix F. Report Distribution**

### **Office of the Secretary of Defense**

Deputy Secretary of Defense  
Under Secretary of Defense for Acquisition, Technology, and Logistics  
Under Secretary of Defense for Policy  
Under Secretary of Defense for Intelligence  
    Deputy Under Secretary of Defense for Counterintelligence and Security  
    Director, Counterintelligence Field Activity  
Assistant Secretary of Defense for Legislative Affairs  
Assistant Secretary of Defense for Public Affairs  
General Counsel of the Department of Defense  
Special Assistant to the Secretary of Defense  
Special Assistant to the Deputy Secretary of Defense  
Assistant to the Secretary of Defense for Intelligence Oversight

### **Joint Staff**

Director, Joint Staff  
    Director for Intelligence  
    Inspector General

### **Department of the Army**

Deputy Chief of Staff for Intelligence  
Inspector General

### **Department of the Navy**

Director, Naval Intelligence  
Inspector General  
Director, Marine Corps Intelligence

### **Department of the Air Force**

Director, Intelligence, Surveillance, and Reconnaissance  
Inspector General

## **Other Defense Organizations**

Director, Defense Intelligence Agency  
Inspector General  
Director, National Geospatial-Intelligence Agency  
Inspector General  
Director, National Reconnaissance Office  
Inspector General  
Director, National Security Agency  
Inspector General

## **Central Intelligence Agency**

Director of Central Intelligence  
Deputy Director of Central Intelligence  
Deputy Director of Central Intelligence for Community Management  
Associate Director of Central Intelligence for Military Support  
Inspector General

## **National Counterintelligence Executive**

## **Department of State**

Inspector General

## **Department of Justice**

Director, Federal Bureau of Investigation  
Inspector General

## **Congressional Committees and Subcommittees**

Chairman and ranking minority member of each of the following committees:

Senate Committee on Appropriations  
Senate Select Committee on Intelligence  
Senate Committee on Armed Services  
House Committee on Appropriations  
House Permanent Select Committee on Intelligence  
House Committee on Armed Services



## (U) Part VIII. Management Comments

# (U) Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

Final Report  
Reference

~~CONFIDENTIAL~~



## OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3000

22 April 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE,  
DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Response to Finding 9 of the "Review of Actions taken to Detour, Detect, and Investigate the Espionage of Ana Belen Montes" (U)

References: Draft report page 94 and 95, Finding 9, subject same as above. (U)

Revised

(FOUO) In the above reference you state in paragraph five pages 94 and 95, "(FOUO) DoD also attempted to develop a plan to consolidate all Special Access Programs into a central Registry. In an August 24, 1999 memorandum, "Changes to Special Access Program Oversight Committee Procedures and Organization," the Deputy Secretary of Defense ordered the Director of the Special Access Program Oversight Committee to develop the Plan." This is an incorrect statement. The August 24, 1999 memo states, "The Director of the SAPOC will develop a plan for approval by the SAPOC in October for the consolidation of all program access clearances into an integrated database." The difference being "access database" versus "all Special Access Programs into a Central Registry". There is a major difference in creating a Special Access Program registry and an access database. Therefore I recommend the draft report be changed to reflect the actual wording in the August 24, 1999 memo.

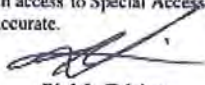
Revised

(FOUO) In addition, I take exception to the quote "died on the vine" because the Military Departments did not want to include their data and then be held responsible for providing updates to the database." I recommend that this quote be removed and replaced to more accurately state my intent, which was "there were many policy issues that had to be addressed prior to implementing changes toward an integrated access database. Each Military Department had to work through the standardization of security forms and procedures. Also identifying and resolving reciprocity issues with the other agencies and between Special Access Program and Sensitive Compartment Information security procedures. Therefore the actual movement toward implementing the integration of the Military Departments' access databases was delayed for a couple of years." To state that I said, "that the concept "died on the Vine" is incorrect. The "concept" has always been active; the policy at that time (1999) had to be changed.

Revised

(FOUO) An additional correction to your draft report is on page 95, second paragraph, where you reference that SAP IMS be fielded by 2008 needs to change to 2007. The 6 June 2004 memo specifically states "DARPA will complete the fielding of the SAP IMS within four years (FY2007)..."

(S) I concur with your recommendation 9 (a) that the USD(AT&L) continue the process of establishing a DoD central registry for personnel with access to Special Access Programs. I also recommend the above changes be made to be more accurate.

  
Rick L. Fulgum  
Chief of Security  
USD(AT&L)/DSP



~~CONFIDENTIAL~~



## (U) Under Secretary of Defense for Intelligence Comments

Final Report  
Reference



INTELLIGENCE

~~CONFIDENTIAL~~  
UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

MAY 2 2005

### MEMORANDUM FOR THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Response to DOD IG Report (Project No: D2004-DINTEL-0012)

Thank you for the opportunity to comment on the review of circumstances surrounding the espionage conducted by Defense Intelligence Agency employee, Ana Montes. This is a very comprehensive review of a complex matter, and your staff should be commended.

The attachment represents a consolidated input from my office and the Counterintelligence Field Activity (CIFA). We intend to take proactive, aggressive action consistent with our comments to the recommendations to enhance the security of the Department of Defense and the nation. In some instances your recommendations will be reflected in Department-wide policy that will enhance our efforts to identify those who would abuse the trust placed in them and betray our country.

Please contact <sup>DoD IG (b)(6)</sup> of my staff if you have any questions.

  
Stephen A. Cambone

Attachment:  
As stated

~~WHEN SEPARATED FROM ATTACHMENTS, THIS DOCUMENT IS  
UNCLASSIFIED.~~

~~CONFIDENTIAL~~



Final Report  
Reference

~~CONFIDENTIAL~~

**Response to the Findings and Recommendations of the Draft DODIG Review  
of Actions Taken to Deter, Detect and Investigate the Espionage Activities  
of  
Ana Belen Montes (U)**

(U) The following comments are provided concerning the eleven recommendations presented in the report:

- (FOUO) Recommendation 1: We recommend that the Under Secretary of Defense for Intelligence request the Intelligence Community Inspectors General Forum to conduct a comprehensive joint evaluation of counterespionage information sharing. The Intelligence Community Inspectors General Forum could use the Inspector General of the Department of Defense Research Report "Research on Information Sharing Between the Intelligence and Law Enforcement Communities," May 3, 2002, as the starting point for its counterespionage evaluation.

- (U) Concur. The Under Secretary of Defense for Intelligence will submit such a request within 30 days of this response.

- (C) Recommendation 2: We recommend that the Under Secretary of Defense for Intelligence formulate a plan to establish permanent Foreign Counterintelligence Program billets to build a DoD counterespionage organization similar to the <sup>CIA, (b)(3), 50 U.S.C. § 403, Sec. 6</sup> ~~functions of the new organization should include, but not be limited to:~~

acting as the central DoD point of contact for all counterespionage inquiries from outside DoD;

identifying and resolving all unknown subject espionage cases within DoD;

hosting a forum where vetted DoD counterintelligence analysts and special agents meet regularly to discuss openly all available counterespionage information;

Classified by: Multiple Sources  
Declassify on: 25X1

~~CONFIDENTIAL~~



~~CONFIDENTIAL~~

establishing counterespionage leads for the Military Departments  
counterintelligence components and the Federal Bureau of  
Investigations; and,

sharing all counterespionage information from the Military  
Departments and DoD Agencies in accordance with Executive Orders,  
statutes, and DoD Directives.

- o (C) Concur. The Department needs this capability, and CIFA is the appropriate organization wherein a <sup>CIA: (b)(3), 50 U.S.C. § 403, Sec. 5002</sup> like entity could be established, financed, and managed. CIFA has an organizational structure that would support such an element. Importantly, a DoD <sup>CIA: (b)(3), 50 U.S.C. § 403, Sec. 5002</sup> will require the support of the FBI and <sup>CIA: (b)(3), 50 U.S.C. § 403, Sec. 5002</sup>

• (FOUO) Recommendation 3:

a. (U//~~FOUO~~) We recommend that Director, Defense Intelligence Agency (DIA) assigns a DoD Production Intelligence Functional Code to the Counterintelligence Field Activity for the purpose of <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

<sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

- o (FOUO) Comment: <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

<sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

<sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

Instead, the DoD Polygraph Program Manager in CIFA, will provide requests for scheduled/ad hoc production on countermeasures and foreign use issues via <sup>DIA: (b)(3), 10 U.S.C. § 424</sup> to the DoD CI Production Requirements Manager (J2CI).

b. (U) Director, Counterintelligence Field Activity:

(i.) (FOUO) Research polygraph countermeasures and then collaborate with polygraph manufacturers to develop, produce, and distribute new countermeasure detection devices for use by polygraph community consumers.

~~CONFIDENTIAL~~

Final Report  
Reference

~~CONFIDENTIAL~~

- o (U) Concur. The Department of Defense Polygraph Institute (DoDPI) is conducting research on countermeasure detection. As a byproduct of that research, they have identified specific criteria and training that polygraph examiners can use to identify efforts to employ polygraph countermeasures. The three major polygraph manufacturers are producing effective countermeasure detection devices as an option with their polygraph systems. Additionally, the Quality Assurance Program (QAP), DoDPI has drafted a new chapter for the Federal Examiner's Handbook (FEH, Chapter 18.) that will require examiners to employ these devices as an aid to countermeasure detection. That chapter is currently being staffed with all federal programs for formal incorporation. The FEH standardizes specific procedures and requirements that are binding for all DoD polygraph programs.

(ii.) ~~(FOUO)~~ Develop comprehensive polygraph standards for the DoD polygraph community to increase the effectiveness of polygraph countermeasures.

- o ~~(FOUO)~~ Concur. Presumably, the intent is to increase the DoD capability to detect and/or neutralize polygraph countermeasures applied against DoD. In this matter, Chapter 18, of the FEH will provide those standards for DoD polygraph examiners. It includes guidance for polygraph examiners to incorporate anti-countermeasures procedures as routine measures to prevent countermeasures efforts, and counter-countermeasures to be applied when countermeasures are suspected or encountered during an examination.

(iii.) ~~(FOUO)~~ Establish a comprehensive polygraph countermeasure course at DoD Polygraph Institute that requires all DoD polygraph examiners to attend the course within one year of graduation from initial training and thereafter requires them to attend refresher training at least biennially.

- o ~~(FOUO)~~ Concur. DoDPI has already significantly increased the number of polygraph examiners who received specific countermeasure detection training. <sup>DoD IG: (b) (1), 1.4(c)</sup> <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

<sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup> the effective marketing of DoDPI personnel who championed the

~~CONFIDENTIAL~~




~~CONFIDENTIAL~~

importance of increasing polygraph examiner awareness and ability to neutralize polygraph countermeasure efforts. This will be further expanded by the mandate in Chapter 18, FEH to require 40 hours of comprehensive countermeasure detection training and the additional mandate for follow-up training on a biennially basis. These standards will become accountable items for DoD polygraph programs under the QAP inspection schedule.

(iv.) ~~(FOUO)~~ Direct all DoD polygraph programs to report to the DoD Polygraph Institute all polygraph examinations in which countermeasures are confirmed.

o ~~(e)~~ DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(7)(E)  
DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424, (b)(7)(E)



- \* (U) Recommendation 4: We recommend that the Deputy Under Secretary of Defense for Counterintelligence and Security continue working with Congress to change DoD polygraph provisions in 10 U.S.C. section 1564a, and then update DoD Directive 5210.48 and DoD Regulation 5210.48-R, accordingly.

- o (U) Concur. Due to an unusual situation regarding a 1987 federal law, the DoD Directive cannot be updated until the law is changed. USD(I) has submitted a legislative proposal to change the law, hopefully this year.

~~CONFIDENTIAL~~

Final Report  
Reference

~~CONFIDENTIAL~~

- ~~(FOUO)~~ Recommendation 5: We recommend that the Director, Defense Intelligence Agency use pre-employment Counterintelligence Scope Polygraph examinations for every DIA position that requires access to Top Secret materiel.

~~(FOUO)~~ Comment: Currently, the Director, DIA, has the authority to designate positions as critical intelligence positions that would be subject to counterintelligence scope polygraph testing to assist in determining their eligibility for employment. However, any additional increase in personnel awaiting Counterintelligence Scope Polygraph (CSP) examinations before entering on duty could create a backlog that may effectively delay employment start dates and cause a possible shift in internal priorities within the broader DIA polygraph missions. The legislative proposal that the Department has submitted to update its polygraph directive would authorize all components to implement CSP examinations as they deem necessary in determining initial eligibility for personnel for assignment to critical or sensitive positions based upon certain risk assessment criteria.

- ~~(FOUO)~~ Recommendation 6: We recommend that the Under Secretary of Defense for Intelligence direct all DoD entities with polygraph programs to digitize and retain in perpetuity all CSP examination charts.
  - ~~(FOUO)~~ Concur, with comment. A requirement will be incorporated in the revision of DoD Regulation 5210.48-R to digitize and retain the charts. The concept of "perpetuity" is probably too long. We will recommend retention for 35 years, as this is a reasonable estimate for the length of a government service career.
- ~~(C)~~ Recommendation 7: We recommend that the Director, Defense Intelligence Agency institute a coordinated security vetting program that uses personnel specialists, security officials, polygraph examiners, and psychologists to determine the suitability of prospective employees.
  - (U) Comment: USD(I) supports this recommendation.
- ~~(FOUO)~~ Recommendation 8: We recommend that the Director, Counterintelligence Field Activity establish FCIP funding for DIA Law

~~CONFIDENTIAL~~



~~CONFIDENTIAL~~

**Enforcement Incentive Pay to recruit sufficient staff and retain highly skilled counterintelligence investigators.**

- o (FOUO) Non-concur, in part. DIA personnel are not authorized by DoD policy to conduct counterintelligence investigations. Counterintelligence personnel in DIA are not classified as 1811 Criminal Investigators and thus no link exists to Law Enforcement Availability Pay. They may conduct initial inquiries until such time that a determination is made that an investigation is warranted. At that point the matter is referred to the FBI or to the Military Department counterintelligence investigative agency that has Title X responsibility for conducting the investigation. All organizations with organic CI personnel should use existing policies and programs to attract and retain the necessary CI expertise.

Revised

• (U) Recommendation 9:

a. (C) We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics continue the process of establishing a DoD central registry for personnel with access to Special Access Programs.

b. (C) <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>  
<sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>

- o (U) Comment: USD(I) supports this recommendation.

• (FOUO) Recommendation 10: We recommend that the Director, Defense Intelligence Agency DIA develop and issue Standard Operating Procedures for counterespionage investigations.

- o (FOUO) Comment: DIA is not authorized to conduct counterintelligence investigations. That does not limit DIA CI Special Agents from other proactive measures including conducting preliminary counterintelligence inquiries and making investigative referrals. To avoid confusion, an internal Standard Operating Procedure (SOP) should establish authoritative guidelines for referral

~~CONFIDENTIAL~~

Final Report  
Reference

~~CONFIDENTIAL~~

procedures and coordination requirements for counterespionage investigations.

- ~~(C)~~ **Recommendation 11: We recommend that the Director, Defense Intelligence Agency reevaluate the Operations Security risks associated with using the JWICS to disseminate close-hold information during counterespionage investigations.**

- (U) Comment: This is an excellent recommendation. The Deputy Under Secretary of Defense for Counterintelligence and Security has already directed through a memorandum to the field that all counterintelligence investigative reporting will be submitted via Portico, a secure communications network for the counterintelligence community. The upcoming revision of DoD Instruction 5240.4, DoD Counterintelligence Investigations and Significant CI Activity Reporting, will codify the requirement for investigations to be reported through Portico.

~~CONFIDENTIAL~~



## (U) Director, Defense Intelligence Agency Comments

Final Report  
Reference



~~SECRET~~ <sup>DoD IG: (b)(1)</sup> ~~NOFORN//20300421~~  
DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340

2 May 2005



S-0286/DR

To: Deputy Assistant Inspector General for Intelligence Evaluations  
Department of Defense  
400 Army Navy Drive  
Arlington, VA 22202-4704

Subject: (U) Review and Development of Action Plans - Ana Belen Montes Investigation

Reference: DoD IG Draft Proposed Report, 22 Mar 05, Review of the Actions Taken to Deter, Detect and Investigate the Espionage Activities of Ana Belen Montes (Project Number D2004-DINTL-0012)

1. (U) The Defense Intelligence Agency (DIA) has reviewed the referenced report and concurs with some of the Department of Defense (DoD) Inspector General (IG) recommendations directed specifically to this agency. In other cases, we agree in principle, but need to seek additional resources in order to fully implement the recommendations. There are some inaccuracies or misinterpretations in the report that should be changed.

2. (U) Finding 10, as written, contains factual errors and unsupportable conclusions. For example, DIA Counterintelligence (CI) and Security personnel are not authorized by a DoD directive to conduct counterespionage investigations, as stated in the finding. Also, the statement, "lack of specific procedures caused some confusion...and may have delayed the identification of Montes," is not supported by the events. DIA CI investigative officers were commended for their prompt action in identifying Montes as a possible Cuban agent in the ongoing FBI investigation. They exercised appropriate judgment in contacting FBI counterparts with whom they had excellent working relationships. These actions materially expedited, not delayed, the identification and subsequent apprehension of Montes.

3. (U) I have directed the following actions be taken to satisfy the DoD IG recommendations directed at DIA:

a. (FOUO) Recommendation 3a: The Director, DIA, assign a DoD Production Program Intelligence Functional Code to the Counterintelligence Field Activity for the purpose of  
DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)

(FOUO) DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)  
DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)

Derived from: Multiple Sources  
Declassify on: 20300421

UPON REMOVAL OF THE ENCLOSURE THIS  
DOCUMENT IS CLASSIFIED CONFIDENTIAL

~~SECRET~~ <sup>DoD IG: (b)(1)</sup> ~~NOFORN//20300421~~

Revised

Final Report  
Reference

~~SECRET~~ <sup>DoD IG: (b)(1)</sup> ~~NOFORN//20300421~~

b. ~~(FOUO)~~ Recommendation 5: The Director, DIA, use pre-employment Counter-intelligence Scope Polygraph (CSP) examinations for every DIA position that requires access to TOP SECRET material.

~~(FOUO)~~ Response: Concur in principle. All DIA employees are required to have a TOP SECRET Special Compartmented Information security clearance. <sup>DIA: (b)(3), 10 U.S.C. § 424, (b)(7)(E)</sup>

c. ~~(S)~~ Recommendation 7: The Director, DIA, institute a coordinated employee vetting program that uses personnel specialists, security officials, polygraph examiners and psychologists to determine the suitability of prospective employees.

~~(S)~~ Response: Concur in principle. Senior DIA personnel and security officers will coordinate with the Central Intelligence Agency and National Security Agency officials to assess their applicant/employee suitability review programs, and make appropriate recommendations to me within 90 days of this letter. Once we understand the resource/funding implications we will decide what can and cannot be done within existing resources. If required, we will seek additional resources.

d. ~~(S)~~ Recommendation 9b: <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>

~~(S)~~ Response: Concur. <sup>DIA: (b)(1), 1.4(c), (b)(3), 10 U.S.C. § 424</sup>

e. ~~(S)~~ DoD IG Recommendation 10: The Director, DIA, develop and issue standard operating procedures for counterespionage investigations.

~~(S)~~ Response: Concur. Current revision of the DIA manual on security investigations will contain a section dedicated to the conduct of espionage inquiries. The revision will be completed within 90 days of this letter.

f. ~~(S)~~ DoD IG Recommendation 11: The Director, DIA, reevaluate the operations security risks associated with using the Joint Worldwide Intelligence Communications System (JWICS) to disseminate close-hold information during counterespionage investigations.

~~SECRET~~ <sup>DoD IG: (b)(1)</sup> ~~NOFORN//20300421~~



~~TOP SECRET~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~NOFORN//MR~~

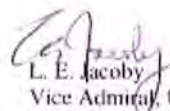
Final Report  
Reference

~~SECRET~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~NOFORN//20300421~~

~~(S)~~ ~~DIA: (b)(1), 1.4(c)~~  
~~DIA: (b)(1), 1.4(c)~~

4. (U) The point of contact for this issue is ~~DIA: (b)(3), 10 U.S.C. § 424, (b)(6)~~

1 enclosure a/s

  
L. E. Jacoby  
Vice Admiral, U.S. Navy  
Director

~~SECRET~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~NOFORN//20300421~~

147  
~~TOP SECRET~~ ~~DoD IG: (b)(1), 1.4(c)~~ ~~NOFORN//MR~~  
DoD OIG 000159

Final Report  
Reference

~~SECRET~~ <sup>DoD IG (b)(1)</sup> ~~NOFORN//20300421~~

**(U) Administrative Comments on the DoD IG Draft Proposed Report, "Review of the Actions Taken to Deter, Detect and Investigate the Espionage Activities of Ana Belen Montes"**

Revised

**1 (U) Page 1, paragraph 1, line 17**

- Recommend: Delete word "loyalty", substitute "pro-Cuba proclivity".
- Rationale: The Defense Intelligence Agency (DIA) source did not question Montes' loyalty, rather her naïve personal views toward Cuba.
- Source: DIA Investigative Report dated 1996.

**2. (S//NF) Page 36-37, paragraph 3, lines 3-7**

- Recommend: Delete sentence beginning "According to" and ending "notification in person"
- Rationale: The 1979 memorandum of understanding between the FBI and the Department of Defense (DoD) sets formal requirements for reporting *initial* suspected disclosure of classified material to a foreign power. When DIA investigators contacted the FBI in October 2000 regarding Montes, they were not acting within the context of an initial referral, but rather to alert the FBI of a possible suspect in an *ongoing* FBI Unknown Subject investigation.
- Source: DIA CI Investigations Staff.

Revised

**3. (S//NF) Page 57, paragraph 2, lines 6-7**

- Recommend: Delete part of sentence "... <sup>DoD IG (b)(1), 1.4(c)</sup> that item to the attention of the FBI" and replace with "the FBI personnel had no reason to equate the case term 'safe' with the DIA SAFE message system".
- Rationale: <sup>DoD IG (b)(1), 1.4(c)</sup> the FBI with information regarding an unspecified reference to "safe." FBI investigative personnel, however, had no logical basis for connecting the vague case term to the DIA classified message system.
- Source: DIA CI Investigations Staff.

Revised

**4. (S//NF) Page 57, paragraph 3, line 2**

- Recommend: Delete part of sentence "worked at" and replace with "had access to the DIA SAFE system".
- Rationale: Factual correction. DIA's <sup>DIA (b)(3), 10 U.S.C. § 424</sup> officials initially suspected that the Cuban Unknown Subject under investigation by the FBI had access to the DIA SAFE system, but did not focus on a suspect within DIA until additional case details became available.
- Source: DIA CI analyst and investigator staffs.

Derived from: Multiple Sources  
Declassify on: 20300421

~~SECRET~~ <sup>DoD IG (b)(1)</sup> ~~NOFORN//20300421~~



~~SECRET~~ <sup>DoD IG (b)(1)</sup> ~~NOFORN//20300421~~

5. (S//NF) Page 57, paragraph 3, lines 11-12

- Recommend: Delete "leave history" and "found" and replace with "travel vouchers" and "confirmed", respectively.
- Rationale: Factual correction. DIA CI investigators confirmed that Montes had traveled to <sup>DIA (b)(3), 10 U.S.C. § 424</sup> via a review of her travel vouchers, not her leave records.
- Source: DIA CI Investigations staff

Revised

6. (S//NF) Page 58, paragraph 1, lines 2-3

- Recommend: Delete "...had access to the unknown subject investigation" and replace with "...were aware that the FBI was attempting to identify a Cuban agent with possible access to the DIA SAFE system."
- Rationale: Factual correction. DIA CI investigators were concerned that a large number of DIA and Office of the Secretary of Defense (OSD) personnel were aware that the FBI was conducting a counterespionage investigation involving a DIA information system, but these individuals did not have access to specific investigative information.
- Source: DIA CI Investigations staff

Revised

7. (S//NF) Page 58, paragraph 2, end of paragraph

- Recommend: Add the following sentence to end of the paragraph: "The DIA investigators subsequently built a convincing picture of effective Cuban intelligence service deception support to their agent operations."
- Rationale: The DoD IG report fails to depict the important denial and deception aspects of the Montes and other Cuban intelligence operations.
- Source: DIA CI Investigations staff

8. (U) Page 94, paragraph 2, line 3

- Recommend: Delete "...by the head of an agency, with original Top Secret classification authority..." and replace with "...by the Deputy Secretary of Defense/Secretary of Defense..."
- Rationale: Factual correction.
- Source: DoD Regulation 5200.1-R.

9. (C) Pages 96-97, finding 10 in its entirety

- a. (C) Summary statement of error: DIA does not have standard operating procedures (SOPs) that function as a roadmap for counterespionage investigations.

Revised

2  
~~SECRET~~ <sup>DoD IG (b)(1), 1.4(c)</sup> ~~NOFORN//20300421~~

Final Report  
Reference

~~SECRET~~ ~~NOFORN//20300421~~

(G) Clarification of fact: DIA is not authorized to conduct counterespionage investigations. DIA conducts limited CI inquiries and provides investigative support to counterespionage investigations of the FBI and military services. DIAM 50-14, "Security Investigations," is the DIA guidance on investigative matters.

b. (G) Summary statement of error: Most DIA activities were conducted without benefit of authoritative guidelines.

(G) Clarification of fact: DIA investigative personnel in the Montes case used DoD directives and Office of the General Counsel guidance as authoritative guidelines.

c. (G) Summary statement of error: DIA special agents did not understand the procedures to effect liaison and coordination with the FBI and OSD, and did not know to make a formal written 811 referral to FBI headquarters.

(G) Clarification of fact: The DIA special agents, one a retired Air Force Office of Special Investigations special agent and the other a former Naval Criminal Investigative Service special agent had worked numerous CI actions and referral procedures. The Montes case was not an 811 referral, which is used for reporting initial suspected disclosure of classified material to a foreign power. When DIA investigators contacted the FBI, they were not making an initial referral, but were alerting the FBI to a possible suspect in an ongoing unknown subject espionage investigation. DIA investigators had no information to suggest any specific classified material had been disclosed to Cuba. The DIA investigators' experience with the FBI suggested that face-to-face discussions would be faster and more productive than a written referral.

d. (S//NF) Summary statement of error: Finding 10 states the absence of an SOP caused confusion, particularly with respect to DoD senior official notification, and cites the following quote from a DIA special agent: "We have no procedure in place to notify seniors.... Do we have a requirement to do so?"

(S//NF) Clarification of fact: This quote was taken out of context. The quote was not about notification to senior DoD officials, additionally, and occurred after OSD had been advised and the FBI had initiated an investigation. It addressed what should happen if Montes was observed during surveillance removing a classified document from the Defense Intelligence Analysis Center. If she was observed leaving with a classified document, the issue raised was whether we had a requirement and procedure to notify DIA leadership for a real-time decision on whether to confront Ms. Montes before she left the facility.

3  
~~SECRET~~ ~~NOFORN//20300421~~



Final Report  
Reference:

SECRET <sup>DoD IG: (b)(1)</sup> NOFORN//20300421

e. ~~(C)~~ Summary of unsupportable conclusions: Lack of specific procedures ... may have delayed the identification of Montes as ... Cuban spy.

~~(C)~~ Clarification of fact: The same day that DIA special agents learned the basic information the FBI was using to search for the unknown Cuban spy, DIA special agents identified Montes and contacted the FBI squad handling the case. The FBI summarily rejected Montes as a suspect and had to be convinced otherwise.

f. ~~(C)~~ Summary of unsupportable conclusions: A formal written 811 referral may have alerted the FBI to the critical nature of the undertaking and the FBI may have acted more swiftly to label Montes a suspect.

~~(C)~~ Clarification of fact: DIA experience has been that it takes the FBI 8 to 9 months, on average, to respond to an 811 referral. The FBI summarily rejected that Montes was the unknown espionage case subject. The FBI had to be convinced, over the course of several face-to-face contentious meetings, to consider her as a suspect.

10. (U) Pages 98-100, Finding 11 in its entirety

- Recommend: Revise Finding 11 to document that DIA SAFE and the Joint Worldwide Intelligence Communications System/Microsoft Outlook are separate systems, maintained by separate systems technicians, who have separate internal authorities and capabilities.
- Rationale: While DIA concurs with recommendation 11 regarding the need for improved operations security procedures, the accompanying finding errs in the description of information technology access vulnerabilities. A technician working SAFE message archives cannot access a CI investigator's Outlook email.  
Source: DIA CI Investigations staff and systems assurance staff.

Revised

4  
SECRET <sup>DoD IG: (b)(1), 1.4(c)</sup> NOFORN//20300421

DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6; FBI: (b)(6), (b)(7)(C)

Final Report  
Reference

Revised

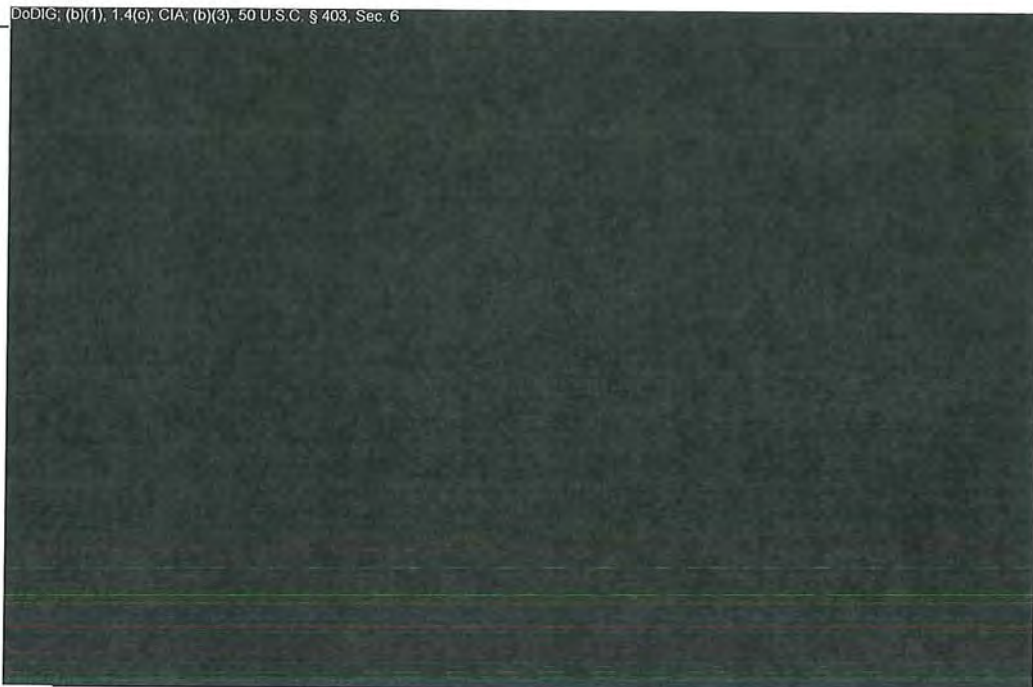
Revised

Revised



Final Report  
Reference

DoD IG: (b)(1), 1.4(c); CIA: (b)(3), 50 U.S.C. § 403, Sec. 6

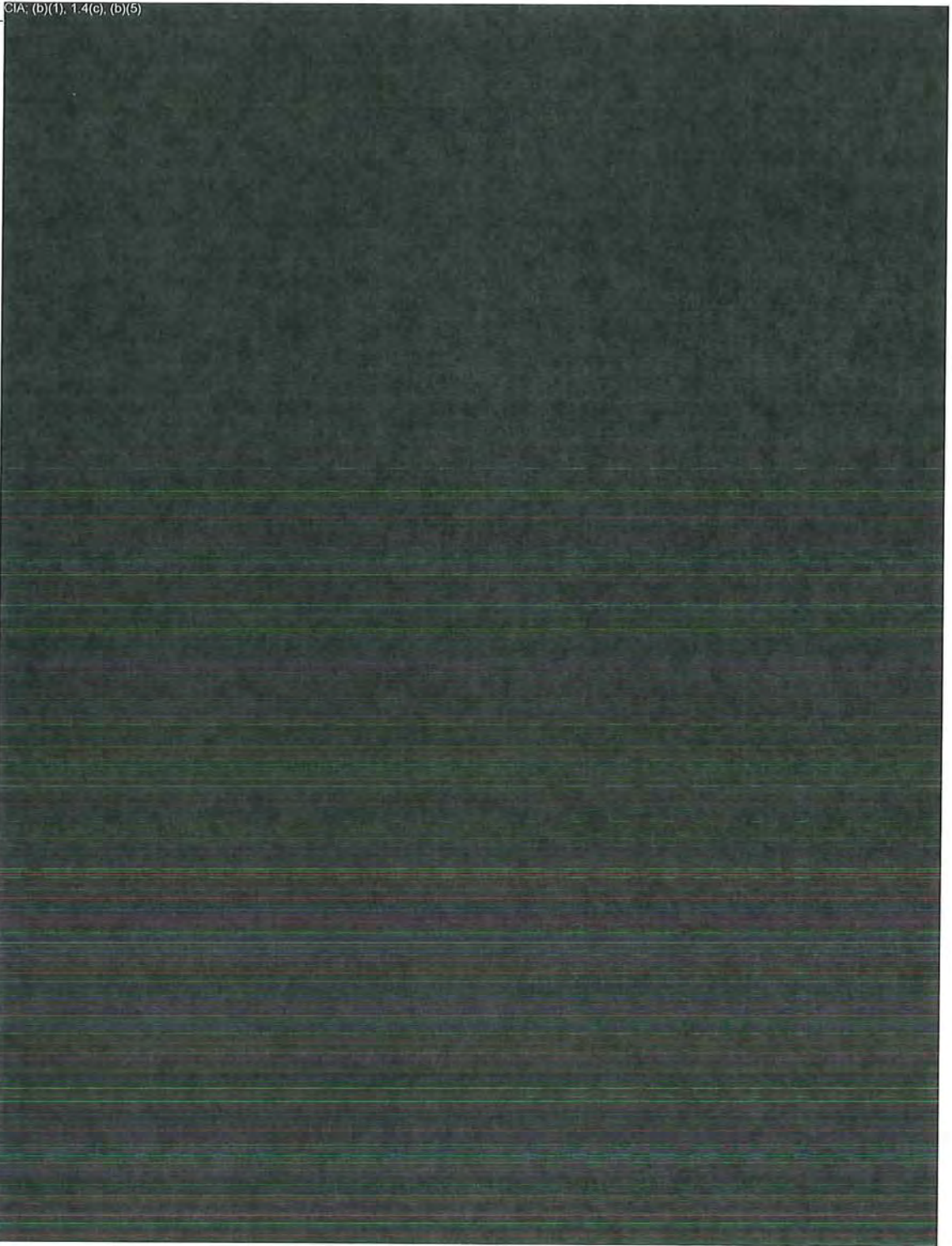


Revised

## (U) Central Intelligence Agency Comments

Final Report  
Reference

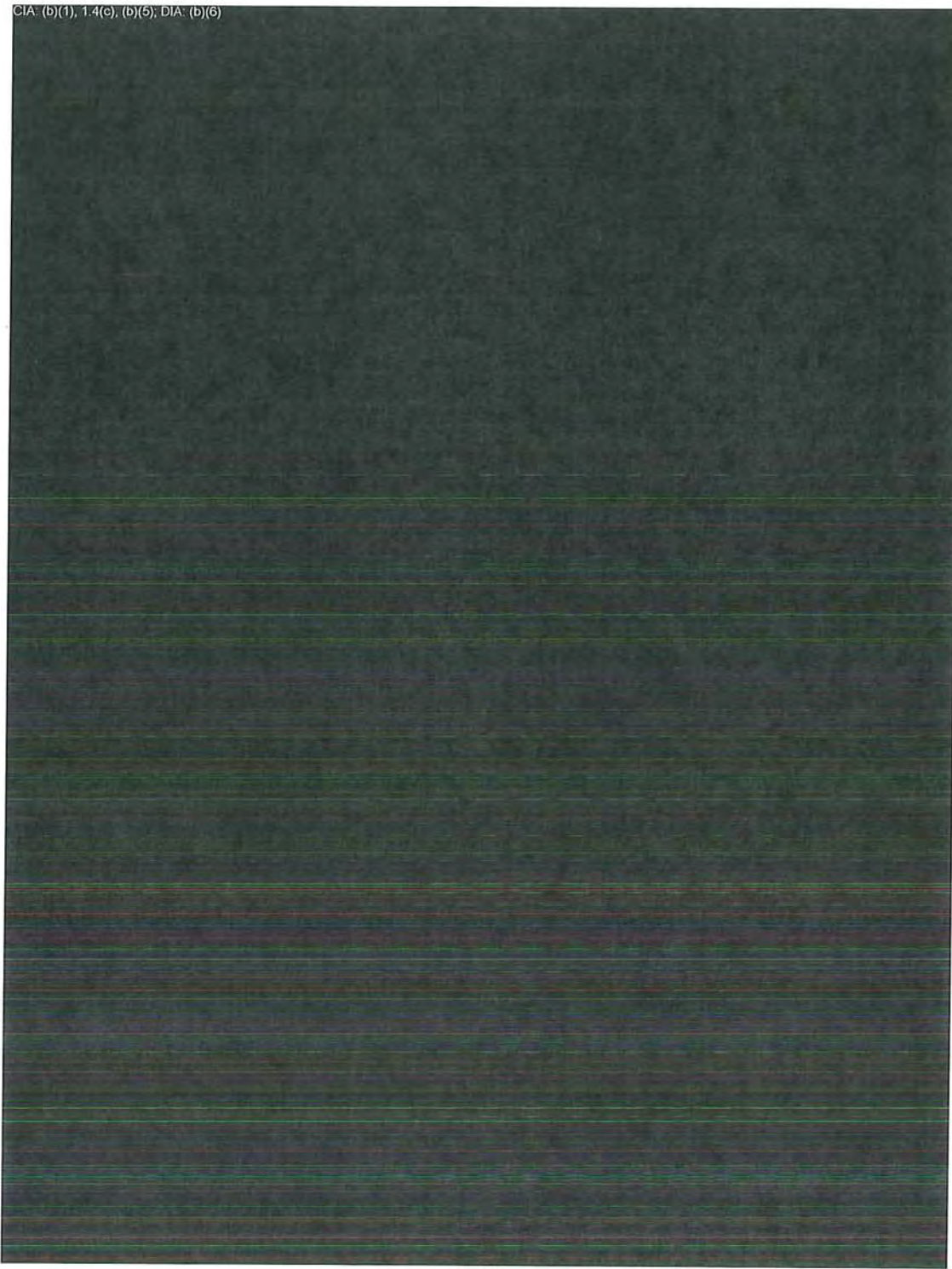
CIA: (b)(1), 1.4(c), (b)(5)



Revised



CIA: (b)(1), 1.4(c), (b)(5); DIA: (b)(6)



Final Report  
Reference

Revised

Revised

Information  
Provided

Final Report  
Reference

CIA; (b)(1), 1.4(c), (b)(5), FBI; (b)(7)(E)

Revised

Revised

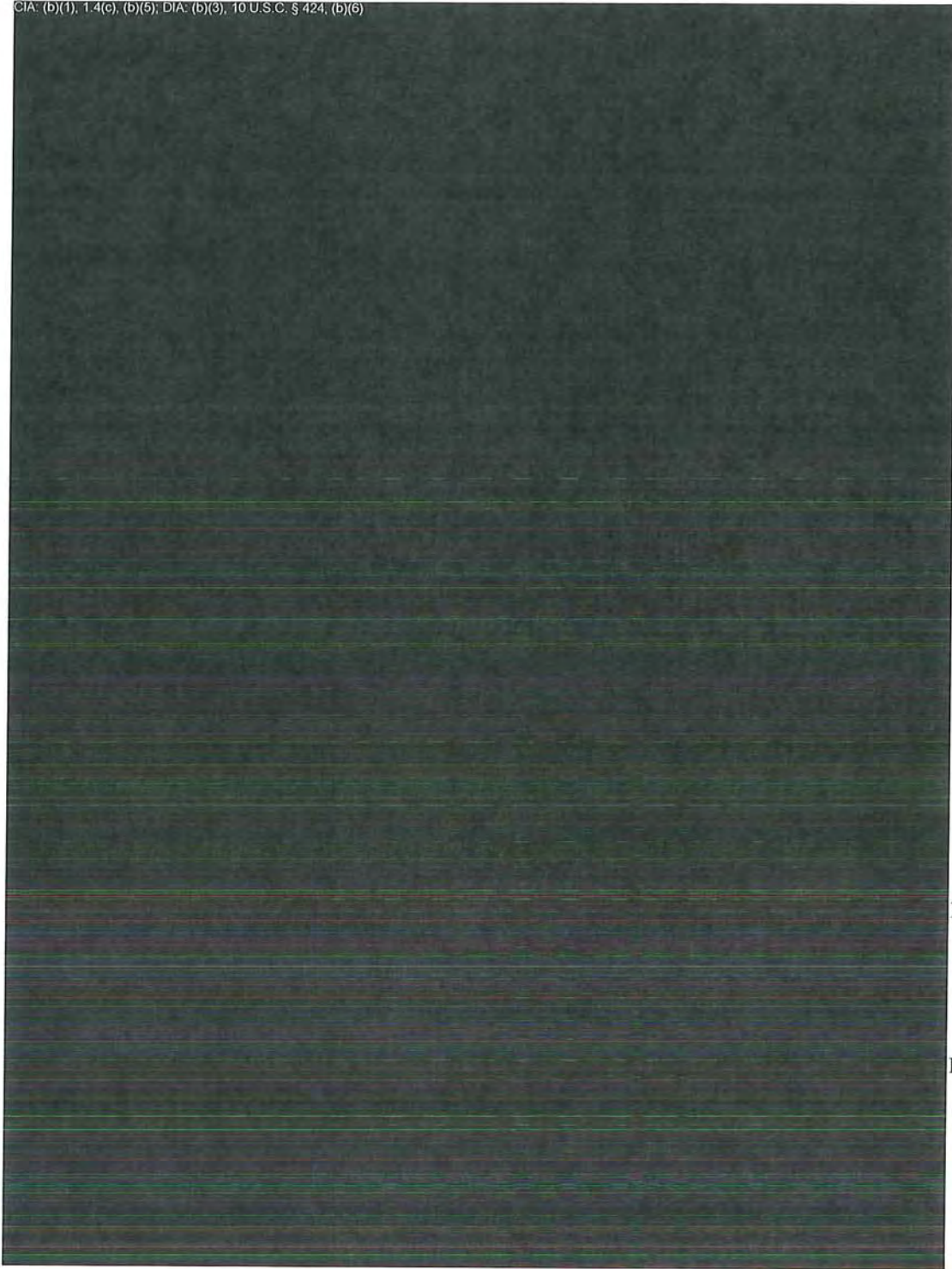
Revised

Revised



Final Report  
Reference

CIA: (b)(1), 1.4(c), (b)(6); DIA: (b)(3), 10 U.S.C. § 424, (b)(6)



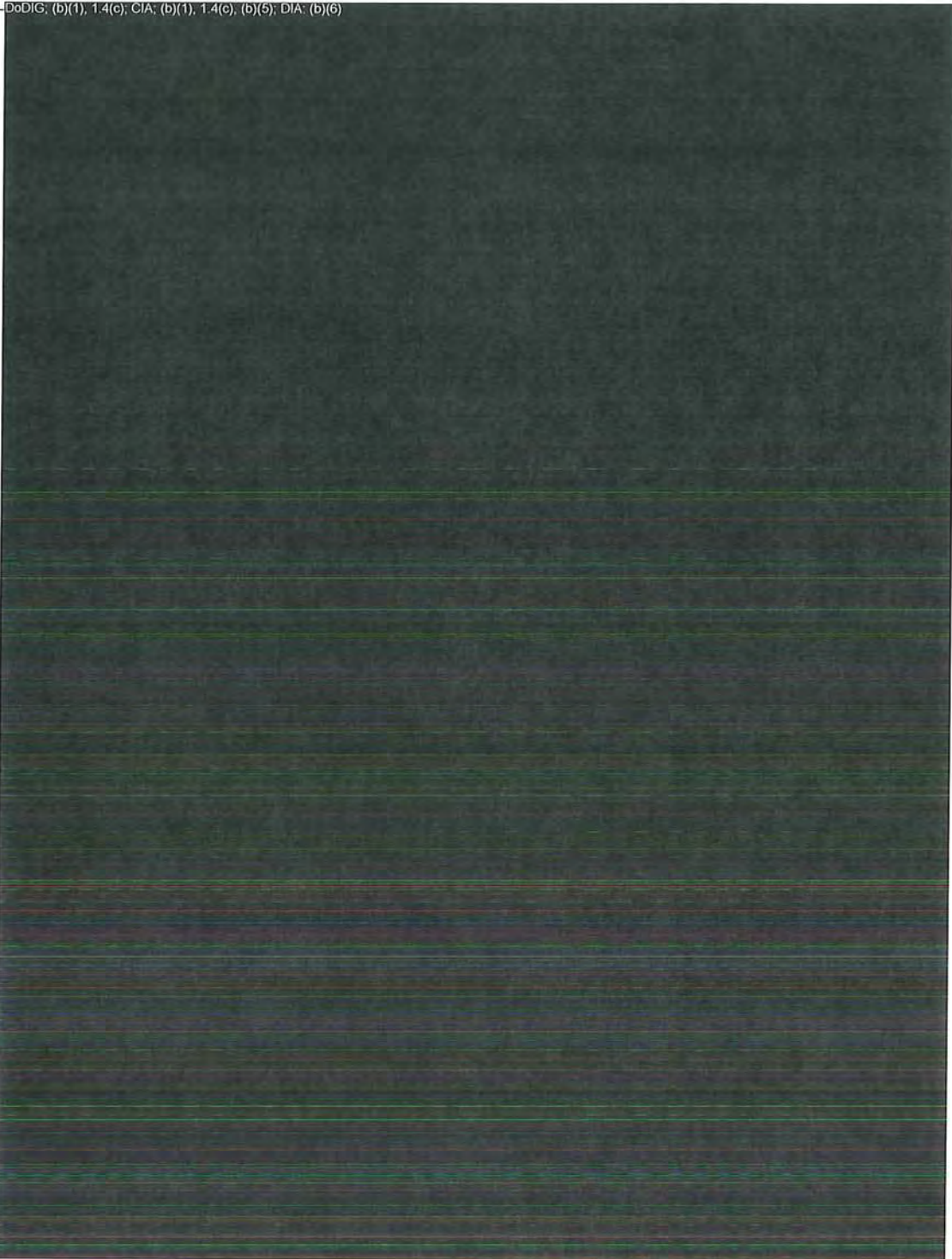
Revised

Revised

Revised

Final Report  
Reference

DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(5); DIA: (b)(6)



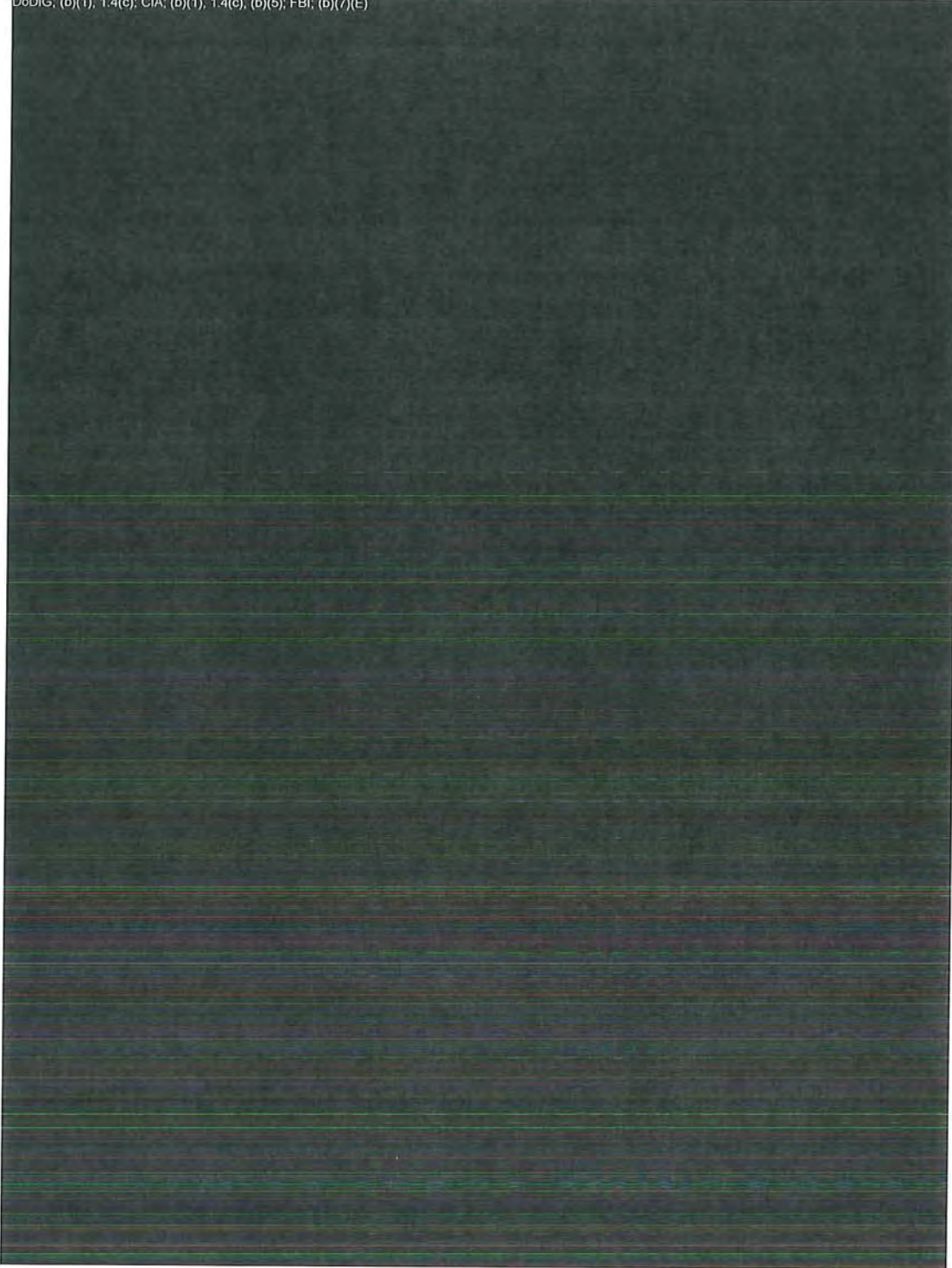
Revised

Revised

Revised



DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(5); FBI: (b)(7)(E)



Final Report  
Reference

Revised

Revised

Revised

Revised

Revised

Final Report  
Reference

DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(5)



Revised

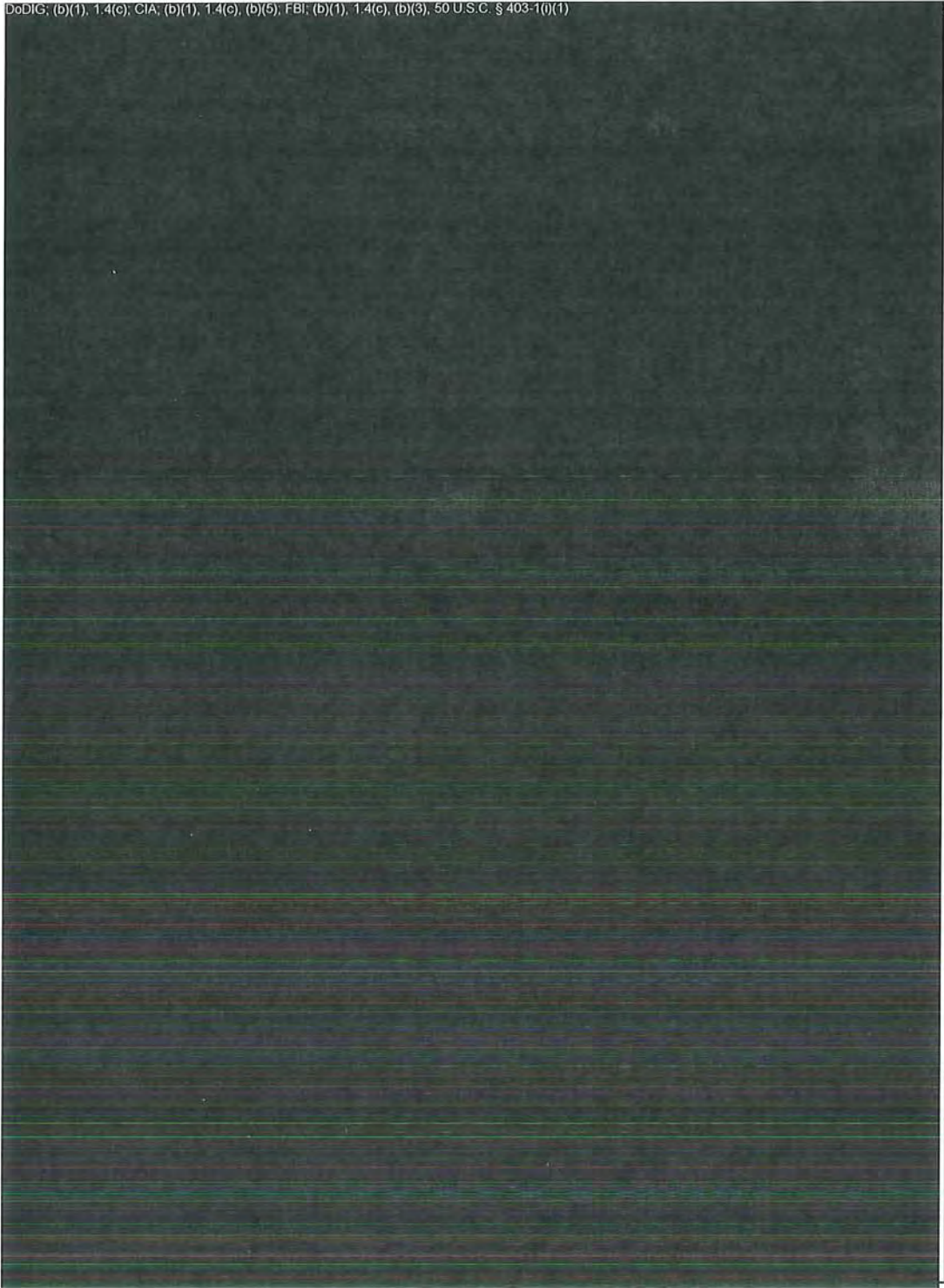
Revised

Revised



Final Report  
Reference

DoD IG: (b)(1), 1.4(c); CIA: (b)(1), 1.4(c), (b)(5); FBI: (b)(1), 1.4(c), (b)(3); 50 U.S.C. § 403-10(1)

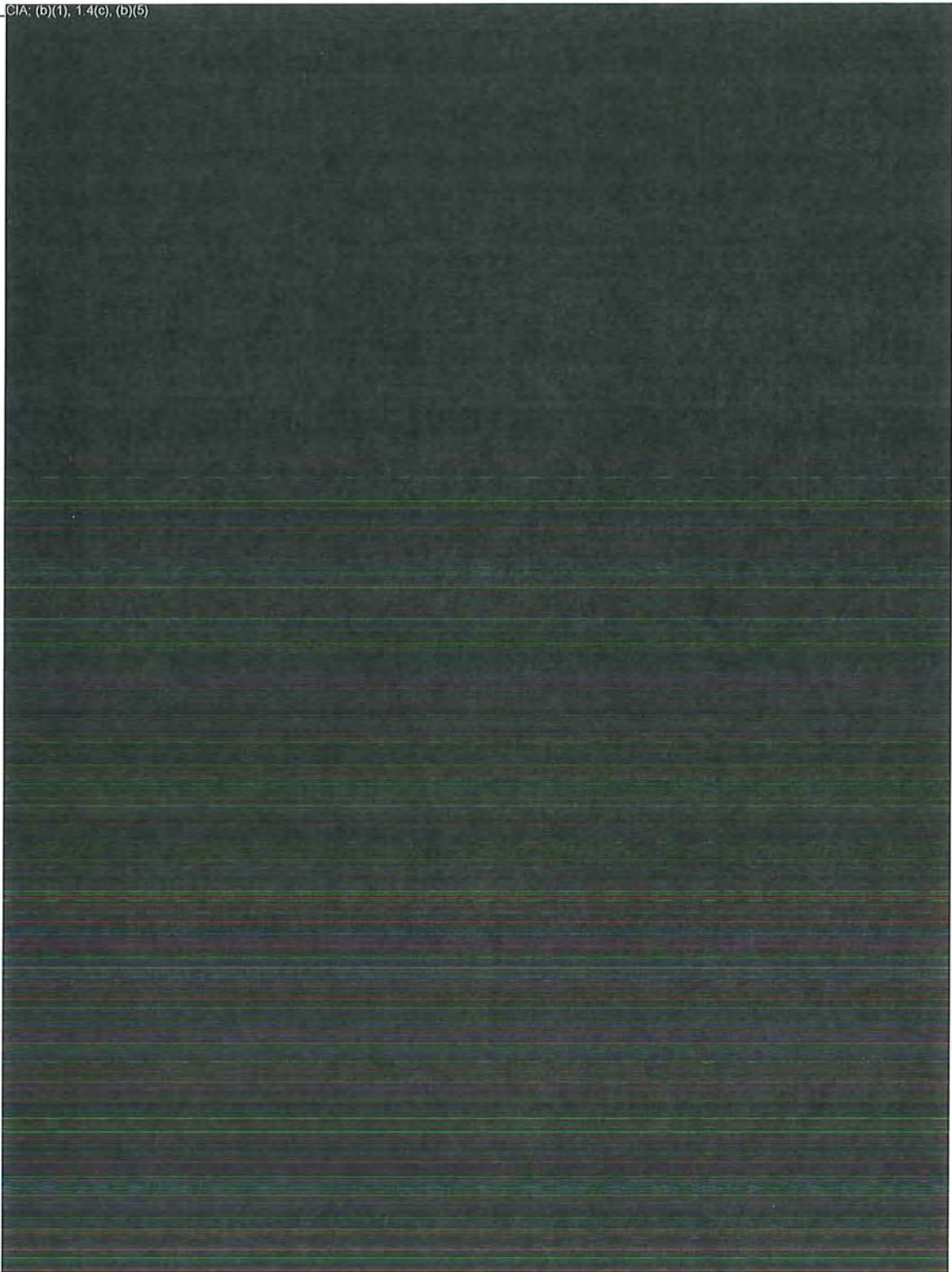


Revised

Revised

Final Report  
Reference

CIA: (b)(1), 1.4(c), (b)(5)

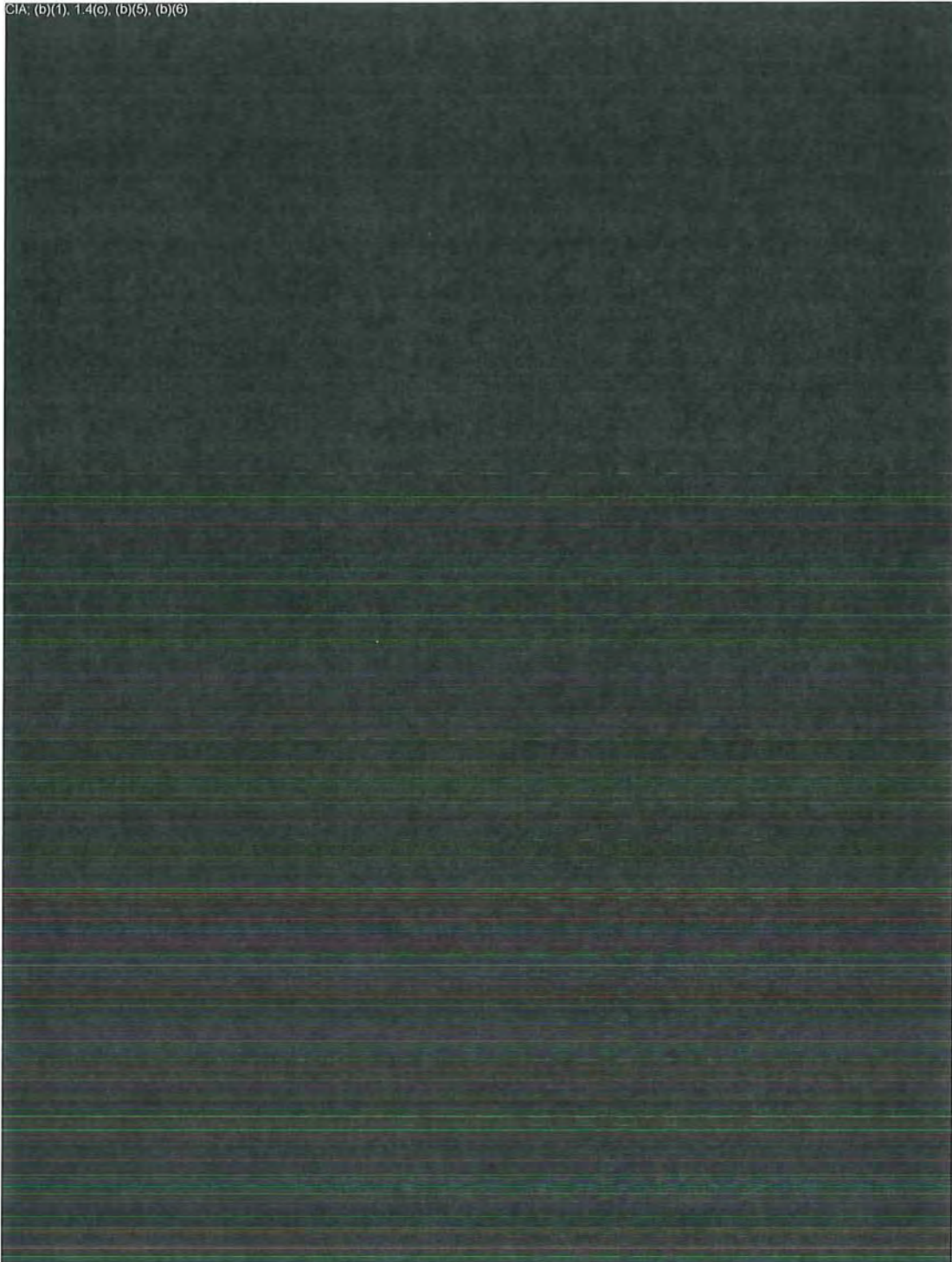


Revised



Final Report  
Reference

CIA: (b)(1), 1.4(c), (b)(5), (b)(6)



## (U) Inspector General, Department of Justice Comments

Final Report  
Reference



U.S. Department of Justice

Federal Bureau of Investigation

~~TOP SECRET~~

Washington, D.C. 20535

BY LIAISON

April 19, 2005

Ms. L. Susan Woodside  
Associate Director  
Office of Oversight and Review  
United States Department of Justice

From: *DWS/B* David W. Szady  
Assistant Director  
Counterintelligence Division

Subject: UNITED STATES DEPARTMENT OF DEFENSE  
OFFICE OF THE INSPECTOR GENERAL  
DRAFT REPORT ON ANA MONTES

Reference is made to a March 30, 2005 memorandum, with enclosure,  
from the United States Department of Justice (USDJ) Office of Oversight and Review,  
regarding the captioned matter. (TS)

As you are aware, the Federal Bureau of Investigation (FBI) was requested  
to review a draft report entitled "REVIEW OF ACTIONS TAKEN TO DETER,  
DETECT AND INVESTIGATE THE ESPIONAGE ACTIVITIES OF ANA BELEN  
MONTES," which was written by the United States Department of Defense (USDOD),  
Office of the Inspector General (OIG). (TS)

Classified by: G-3  
Declassify on: 25X1

~~TOP SECRET~~

*Copy 1 of 2*  
*OS-IG-060*

FBI/DOJ



Final Report  
Reference

~~TOP SECRET~~

Ms. L. Susan Woodside  
Associate Director

FBI Headquarters has reviewed the aforementioned report and has the following observations to provide which will assist in clarifying certain statements made within the document. In order to assist in any revision, the section and the page numbers of the information to be corrected are provided: (TS)

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) (TS)

Revised

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3) (TS)

Revised

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1), CIA: (b)(3), 50 U.S.C. § 403, Sec. 6  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) (TS)

FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1)  
FBI: (b)(1), 1.4(c), (b)(3), 50 U.S.C. § 403-1(i)(1) (TS)

Revised

USDOJ is advised that FBI Headquarters has no concerns with respect to the classification of the USDOD OIG report. (TS)

Should USDOJ have any questions regarding the contents of this communication, please contact FBI Headquarters. (U)

~~TOP SECRET~~

Copy 1 of 2  
04-16-060

Final Report  
Reference

~~TOP SECRET~~

Ms. L. Susan Woodside  
Associate Director

Your contact point at FBI Headquarters with reference to the captioned

<sup>matter is</sup>  
~~FBI (b)(6), (b)(7)(C)~~  
~~FBI (b)(6), (b)(7)(C)~~

(U)

Copy of 2  
OS-IG 060



## (U) Team Members

(U) This report was prepared by the Office of the Deputy Inspector General for Intelligence, Department of Defense Office of Inspector General.

DoD IG: (b)(6)



DIA (b)(3), 10 U.S.C. § 424

(Defense Intelligence Agency)

~~TOP SECRET~~

DoD IG: (b)(1), 1.4  
(c)

~~NOFORN//MR~~

~~TOP SECRET~~

DoD IG: (b)(1), 1.4  
(c)

~~NOFORN//MR~~