Description of document:	United States Army Intelligence and Security Command (INSCOM) Annual Command History, Fiscal Year 2001, 2002, 2003
Request date:	18-August-2007
Released date:	13-May-2014, 23-June-2014, 24-June-2014
Posted date:	30-June-2014
Updated:	25-August-2014
Note:	FY 2002 records begin on PDF page 87 FY 2003 records begin on PDF page 132
Source of document:	Freedom Of Information Act Request Commander, INSCOM ATTN: IAMG-C-FOI 4552 Pike Road Fort Meade, MD 20755-5995 Fax: (301) 677-2956

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

REPLY TO
ATTENTION OF:

Freedom of Information/
Privacy Office

13 MAY 2014

This is in further response to your Freedom of Information Act (FOIA) request of August 18, 2007, for a copy of the INSCOM Annual History for FY2001 and supplements our letter of October 9, 2012.

Coordination has been completed with other elements of this command and other government agencies. The records have been returned to this office for our review and direct response to you.

We have completed a mandatory declassification review in accordance with Executive Order (EO) 13526. As a result of our review information has been sanitized and five pages are being withheld in their entirety as the information is currently and properly classified TOP SECRET, SECRET and CONFIDENTIAL according to Sections 1.2(a)(1), 1.2(a)(2), 1.2(a)(3) and 1.4(c) of EO 13526. This information is exempt from the public disclosure provisions of the PA as provided unter Title 5 U.S. Code 552 (k)(1) and of the FOIA pursuant to Title 5 U.S. Code 552 (b)(1). It is not possible to reasonably segregate meaningful portions of the withheld pages for release. A brief explanation of the applicable sections follows:

Section 1.2(a)(1) of EO 13526, provides that information shall be classified TOP SECRET if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

Section 1.2(a)(2) of EO 13526, provides that information shall be classified SECRET if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

Section 1.2(a)(3) of EO 13526, provides that information shall be classified CONFIDENTIAL if its unauthorized disclosure reasonably could be expected to cause damage to the national security.

Section 1.4(c) of EO 13526, provides that information pertaining to intelligence activities, intelligence sources or methods, and cryptologic information shall be considered for classification protection.

In addition, information has been withheld that would result in an unwarranted invasion of the privacy rights of the individuals concerned, this information is exempt from the public disclosure provisions of the FOIA per Title 5 U.S. Code 552 (b)(6).

Additionally, information has been sanitized from the records as the release of the information would reveal sensitive intelligence methods. This information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(7)(E) of the FOIA. The significant and legitimate governmental purpose to be served by withholding is that a viable and effective intelligence investigative capability is dependent upon protection of sensitive investigative methodologies.

The withholding of the information described above is a total denial of your request. This denial is made on behalf of Major General Stephen G. Fogarty, Commanding, U.S. Army Intelligence and Security Command, who is the Initial Denial Authority for Army intelligence investigative and security records under the Freedom of Information Act and may be appealed to the Secretary of the Army. If you decide to appeal at this time, your appeal must be post marked no later than 60 calendar days from the date of our letter. After the 60-day period, the case may be considered closed; however, such closure does not preclude you from filing litigation in the courts. You should state the basis for your disagreement with the response and you should provide justification for reconsideration of the denial. An appeal may not serve as a request for additional or new information. An appeal may only address information denied in this response. Your appeal is to be made to this office to the below listed address for forwarding, as appropriate, to the Secretary of the Army, Office of the General Counsel.

Commander
U.S. Army Intelligence and Security Command
Freedom of Information/Privacy Office (APPEAL)
4552 Pike Road
Fort George G. Meade, Maryland 20755-5995

Additionally, we have been informed by the Central Intelligence Agency (CIA) that their information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(1) and (b)(3) of the FOIA. Exemption (b)(3) pertains to information exempt from disclosure by statute. The relevant statute is Central Intelligence Agency Act of 1949, 50 U.S.C. §403, as amended, e.g., Section 6, which exempts from the disclosure requirement information pertaining to the organization, functions, including those related to the protection of intelligence sources and methods, names, official titles, salaries, and numbers of personnel employed by the Agency.

The withholding of the information by the CIA constitutes a denial of your request and you have the right to appeal this decision to the Agency Release Panel within 45 days from the date of this letter. If you decide to file an appeal, it should be forwarded to this office and we will coordinate with the CIA on your behalf. Please cite CIA #F-2010-00777/Army #681F-09 assigned to your request so that it may be easily identified.

In addition, we have been informed by the Defense Intelligence Agency (DIA) that their information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(3) of the Freedom of Information Act (FOIA) and 10 U.S.C. § 424.

The withholding of the information by the DIA constitutes a denial of your request and you have the right to appeal this decision directly to the DIA. If you decide to file an appeal, it should be forwarded to the Director, Defense Intelligence Agency, Attention: DAN-1A, FOIA, Washington, DC 20340-5100. Please cite DIA Case #CONF0026-2010 assigned to your request so that it may be easily identified.

Additionally, we have been informed by the National Security Agency (NSA) that portions of their information has been sanitized from the records pursuant to the exemptions listed below:

5 U.S. Code 552(b)(1) – The information is properly classified in accordance with the criteria for classification in Section 1.4 of Executive Order 13526.

5 U.S. Code 552 (b)(2)

5 U.S. Code 552(b)(3) – The specific statutes are listed below:

50 U.S. Code 402 note (Public Law 86-26 Section 6)
50 U.S. Code 403-1(i)
18 U.S. Code 798

The initial denial authority for NSA information is the Director Associate Director for Policy and Records. Any person denied access to information may file an appeal to the NSA/CSS FOIA/PA Appeal Authority. The appeal must be postmarked no later than 60 calendar days of the date of the initial denial. The appeal shall be in writing to the NSA/CSS FOIA/PA Appeal Authority (DJP4), National Security Agency, 9800 Savage Mill Road, STE 6248, Fort George G. Meade, Maryland 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS FOIA/PA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent unusual circumstances.

There are no assessable FOIA fees.

If you have any questions regarding this action, feel free to contact this office at 1-866-548-5651, or email the INSCOM FOIA office at: usarmy.meade.902-mi-grp-mbx.inscom-foia-service-center@mail.mil and refer to case #681F-09.

Sincerely,

Joanne Benear
Chief
Freedom of Information/Privacy Office

Enclosure

~~TOP SECRET~~ ~~NOFORN//X1~~

(FOUO) ANNUAL COMMAND HISTORY

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

FISCAL YEAR 2001

History Office
Office of the Chief of Staff
Headquarters, U.S. Army Intelligence and Security Command
Nolan Building
8825 Beulah Street
Fort Belvoir, Virginia 22060-5246

30 September 2002

DERIVED FROM: MULTIPLE ~~SOURCES~~
DECLASSIFY ON: ~~X1~~
DATE OF ~~SOURCE~~: 30 September 2001

TABLE OF CONTENTS

Captured War Criminal Declassification Effort

Army Attaché Management

Impact of AG Transformation on the Field Support Center Activities

(b)(1),(b)(3) Per CIA

Challenges to the Field Support Center

Deployment per Diem

Accident Statistics

Closure of the Army National Capital Region (ANCR) Civilian Personnel Operations Center (CPOC)

Civilian Personnel Changes

Drug Testing

Security Clearance Processing

INSCOM Investment Strategy

FY04-09 POM Strategy

Mail Protection

Wearing of the Beret

INFORMATION AND SYSTEMS Chpt 3 pp 22-26

Transfer of Billets

Overview of Information Arena

Foreign Language Technology Website

501st Network Operations Center Consolidation

Headquarters Networks

Information Dominance Center (IDC) Portal

Viruses

Technology Support Element

Mandatory Deployment of Systems Management Server (SMS)

OPERATIONS Chpt 4 pp 27-52

Unified Cryptologic System

CIA Commendation

Aerial Exploitation

Information Warfare in the Field

Greater Computer Access

Conviction of George Trofimoff

Offensive CI Operations

Army's Relationship to the NRO

Status of SAEDA in Europe

September 11 Legal Policy Changes

Intelligence Oversight Issues

MASINT in Europe

(b)(1)(b)(3) Per NSA

Pre 9/11 Support to Counter Terrorism

MDITDS/Blackbird Database

Army CI Center

NGIC's Reach to the Field

SPO Activities

TAREX Activities

Polygraph Program

TROJAN

EAC IO Requirements

501st Special Operations Concepts

9/11 Search Support

Operation END GAME

Combat Development Target

Deployment of IOWA

Smugglers

MASINT Breakthrough

USN EP-3 Crisis

MRSOC Role

Significant IIR

CI Support to Force Protection

Second Generation Computer

(b)(1)(b)(3) Per NSA

PALMETTO SHIELD/GHOST

NGIC Team Visit

(b)(1)(b)(3) Per NSA

Bad Aibling Coverage

Asian Studies Detachment

(b)(1)(b)(3) Per NSA

500th CI Detachment

902d MI Group

704th MI Brigade

116th MI Group

115th MI Group

LIWA

500th MI Group

501st MI Brigade

INTRODUCTION

(U) *The following are excerpts from a statement delivered by Major General Keith Alexander, CG INSCOM, to the House Permanent Select Committee on Intelligence (November 14, 2001):*

****

(U//~~FOUO~~) INSCOM's transformation to meet the growing challenges of an asymmetric, transnational threat began in earnest prior to 11 September. The attack on the *USS Cole* highlighted the need for greater focus on actionable counterterrorism intelligence. USCINCCENT asked the Chairman, Joint Chiefs of Staff, to support development of a program to "get out in front" of the CT threat using the Information Dominance Center, at INSCOM. In December, 2000, the Chief of Staff of the Army agreed with this tasking and directed INSCOM to take on these operations. INSCOM intensified that focus during a February 2001, Commanders' Conference, which assembled the Brigade Commanders of the previously mentioned units. The conference was devoted to envisioning a revised concept of INSCOM's mission and capabilities. In the end, the conferees recognized the need for a new methodology to transform the entire Command as it confronted the asymmetric threats, while, at the same time, meeting the challenges of providing operational intelligence in the Army's Transformation.

(U//~~FOUO~~) n the past, INSCOM units generally conducted their respective missions as discrete entities. The INSCOM Headquarters performed personnel administration, logistics, resourcing, planning, and programming functions, but did little in the way of Command-wide mission management, synchronization, on focusing these disparate units against a specific intelligence problem. The new challenge was to optimize the efforts and effects of a worldwide, multi-discipline intelligence organization.

(U) ~~(S//NF)~~ The significant change INSCOM made is both physical and mental-transforming the MACOM headquarters into an organization focused on unifying the intelligence operations of our subordinate units, and ensuring a common view in the battle against terrorism. The intellectual and technical capabilities of the NGIC and the SIGINT Brigades link with the operational expertise of the Theater Brigades, the 902d MI Group, LIWA, and our Special Missions Units. Thus CI/HUMINT, SIGINT, Science and Technology, and operations are woven together, along with the Information Operations efforts, into a synergy that ensures the best minds and intelligence tools are harnessed, via the INSCOM Information Dominance Center (IDC) to support commanders. The goal is to prosecute the Army's and Nation's toughest challenges of Counterterrorism (CT), Counternarcotics (CN), Counterintelligence (CI), and Computer Network Operations (CNO) in a comprehensive, integrated, collaborative manner. All in one Command, each in an agile and optimized fashion.

(U//~~FOUO~~) From February to June 2001, INSCOM commanders and staff completed much of the preliminary work for instituting a transformed organization. We identified the requisite enablers: people,

resources, policy changes, databases, and communications improvements necessary to ensure command-wide collaboration and synchronization.

~~(S/~~ ~~/NF)~~ In June, INSCOM entered into a formal agreement with the National Security Agency, which allowed us to access to specific classified databases and to receive live communication feeds from (b)(1)(b)(3) Per NSA This was an unprecedented step by the DIRNSA, for which he and NSA should receive full credit! The summer was spent exploiting data bases and live "metadata" to identify terrorist networks, wile simultaneously developing the tactics, techniques, and procedures of running an Information Dominance Center (IDC). Concurrently, we established the operational procedures for ensuring the full engagement of the entire command.

(U) Accelerated Transformation: Post-11 September

~~(S/~~ ~~NF)~~ The next phase of INSCOM's transformation incorporated the most significant enhancements. On 14 September, INSCOM deployed 10 analysts to NSA to form the IDC-Meade element to assist the CT Office of Primary Interest. Additionally, 2 linguists were attached directly to the CTOPI. The intent was to augment NSA's on-going analytic efforts by leveraging the IDC's processing capabilities. With the continued support from NSA and analytic engagement with DIA, CIA, and the FBI, the INSCOM Information Dominance Center (IDC) captured the elements of data storage, data feeds, data acceleration, and robust analytic tools in dramatic ways. This resulted in

(b)(1)(b)(3) Per NSA

(U) ~~(S//NF)~~ In order to get real-time information to the warfighter and ensure Command-wide collaboration, we established a web-based technology portal on which we post our counterterrorism analytic exchanges. The portal enables an interactive link from INSCOM to our Brigades, the Army Operations Center at the Pentagon, the Army Service Component Commands, Defense Intelligence Agency's Joint Terrorism Analysis Center, Joint Commands - most notably CENTCOM, and National Agencies. The intellectual energy of the entire Command is harnessed and focused every day through the use of this portal and worldwide, classified, video tele-conference, during which we synchronize the intelligence operations of each of our units in the fight against terrorism.

****

CHAPTER ONE

MISSION AND ORGANIZATION

Headquarters Reorganization. (U/~~FOUO~~) At the January 2000 offsite, the leadership from the INSCOM staff met for the purpose of taking the command's strategic plan one step further and looking at what would allow the organization to reach its 5-year objectives. What came out of the meeting was the FY 00/01 INSCOM Performance Plan. One of the plan's objectives that was raised and approved by MG Noonan, CG INSCOM, was to establish an executive working group to review the headquarters structure and functions. Unlike recent studies such as the one performed by Mystech Associates in 1997, this was to be done in house and at little cost to the command. General Noonan wanted to know what was needed organizationally to accomplish the command's long-term goals. He went on to emphasize that he was not wedded to the past. More specifically, the Commanding General asked the working group to address the following questions: Is the current G-structure adequate? Are there functions being performed that are no longer needed? Can other functions and organizations be streamlined for the sake of efficiency? The working group was also to look at possible savings that the Command Group could redirect to areas of emerging priorities (LIWA, IOC, etc.). Finally, the working group was to be mindful that the command had a man-power survey coming up. If there were areas of vulnerability, then realignment of spaces could be made up front.

(U/~~FOUO~~) The 12-person working group, chaired by a representative from DCSRM, set out to conduct a functional analysis of the headquarters. Besides input from the various staff elements, the members of the working group conducted interviews with key members of the staff. In June 2000, the working group issued a report with the following conclusions: Consolidate major compliance and oversight processes to achieve greater focus and coordination. Consolidate System Integration and G-6 into one information management/technology organization. Reduce the complexity of the G3 organization. Force management and system acquisition should be realigned into a single element. The Deputy Commander and Chief of Staff positions should be realigned to function similar to an Army Division. INSCOM should establish a MACOM CPAC. Finally,

consolidate a number of functions such as safety and training.

(U//~~FOUO~~) The working group presented General Noonan with four options for restructuring the headquarters: The first was basically the same G-staff structure already in place. Options 2 and 3 created subordinate deputies under the Commanding General. These would be called Deputy for Support (including Personnel, Contracting, Resource Management, and Logistics) and Deputy for Intelligence Operations and Technology. Option 2 would further divide the Deputy for Intelligence Operations and Technology into two directorates: one for operations and systems acquisition and the other for information management and telecommunications. The only difference for Option 3 was that the Deputy for Intelligence Operations and Technology was further broken down into three directorates: operations and security; futures (systems acquisition); and information management/technology. Option 4 would be the most far-reaching of the proposals. The staff would be divided between a Deputy for Support, a Deputy for Operations, Security & Systems Acquisition, and a Deputy for Information Management/Technology. (Ironically, following a high-level, high cost study of its own, NSA would emerge with an organizational restructuring much like that shown in Option 4.)

(U//~~FOUO~~) However, unexpected events would interfere with the planning process. Anticipating his appointment as the new DCSINT, General Noonan hesitated to make a decision that his predecessor would have to live with. Consequently, the reorganization process was placed on hold. Because naming of a new commander was delayed until early 2001, the whole issue lay dormant. In the interim, (b)(6) COL [redacted] the Chief of Staff, coordinated the original recommendations among the staff and amended where appropriate.

(U//~~FOUO~~) In March 2001, BG Alexander, the new INSCOM CG, was briefed on the various restructuring options and chose to maintain the G-staff. He did not want to become so dissimilar from the rest of the Army that INSCOM was not recognized as an Army command. The more that INSCOM looked like the warfighters, the more they could identify with the command. General Alexander proceeded to appoint COL [redacted] (b)(6) to meet with the staff and pare down the recommendations. What emerged in July 2001 was a three phase implementation

process. All three phases would run simultaneously and were scheduled to be completed in 4 months, 8 months, and 12 months. Tiger Teams would be used to complete the process. By 1 October, the following major changes were to be completed: establishment of a Command Information Cell, development of a Compliance Process, analyze the establishment of an INSCOM CPAC, transfer the commercial process from G4 to G3, transfer of COMSEC oversight from G2 to G6, transfer of CCP (Consolidated Cryptologic Program) from G3 Army Cryptologic Office to DCSRM, and define the G3 Counterintelligence Office. Again, unforeseen events disrupted the planning process. After September 11, the Chief of Staff decided to proceed with only phase one. It was felt that to do more would be too disruptive for a staff focused on a war against terrorism.

Coming of Multi-Component Contingency Support Brigade (MCSB). (U) The following is an excerpt from an article by (b)(6) LTC [redacted] (Utah National Guard): The Intel XXI Study (also known as "The Hall Study") identified a number of unique, one-of-a-kind military intelligence assets that have the potential of spanning all echelons of the Army. The idea of a Multicomponent Contingency Support Brigade (MCSB) developed from this study. The mission of the MCSB is to provide increased full-spectrum capabilities at both echelons above corps (EAC) and echelons corps and below (ECB). The concept is to "pool" these unique capabilities to support the Total Force and to provide tailored packages of specific skills from this pool of broader resources. These tailored packages would be modular and flexible in order to meet the specific needs of the Total Force.

(U) The vision for the MCSB was further enhanced and refined in January 2000 during the MI Functional Area Assessment (FAA) when the Vice Chief of Staff for the Army (VCSA) approved the recommendation to develop a Force Design Update (FDU) for the MCSB. That decision included establishing an MCSB to 'support Army contingency operations with unique, one-of-a-kind capabilities.' The approved recommendation also assigned the MCSB to US Army Intelligence and Security Command (INSCOM) with operational control to US Forces Command (FORSCOM). The reason for this arrangement was to maintain the existing training relationships between INSCOM units and the current elements designated for the MCSB, while giving FORSCOM the ability to "plug and play" the pieces of the MCSB when and where they were most needed.

(U//~~FOUO~~) The initial force design included the following: the 300th MI Brigade (Linguist) as the headquarters element with representatives from the Active Component, Army National Guard, and Army Reserve. An electronic warfare unit formed from two Army Reserve units– the 323d MI Battalion and the 368th MI Battalion. An Active Component linguist unit designated to provide "first-in" deployment assets. Nine MI linguist companies pulled from

the Reserves along with six National Guard linguist battalions. The 203d MI Battalion, an existing multi-component unit in support of the National Ground Intelligence Center, was included. Finally, the 96Hs (Common Ground Station Operators) from the Joint Surveillance Target Attack Radar System were also made a part of the brigade.

First Multi-Component MI Unit. (U//~~FOUO~~) On 16 June 2001, the first military intelligence multi-component unit was activated–the 203d MI Battalion at Aberdeen Proving Ground, Maryland. The multi-component concept began in 1997 when INSCOM was directed to make personnel cuts while still maintaining its mission. LTC [redacted] then commander of the 203d, and his staff came up with the multi-component plan. (The battalion already had a working relationship with two Reserve companies.) The process towards the activation was not an easy one and required drawdown and inactivation of the 203d by the Active Army as well as several companies in the Reserves. This restructuring allowed for the residual elements to fit into the new multi-component battalion activated on 16 June 2001. The battalion consisted of one integrated active/reserve company and two reserve companies (authorized strength was 253). The 203d had the unique mission of providing warfighter commanders with technical intelligence on foreign equipment and weapons systems. The 203d trained on foreign weapons, equipment, and both wheeled and tracked vehicles and participated in opposing forces operations at the National Training Center, Fort Irwin, California.

(b)(6)

INSCOM Performance Plan. (~~U//FOUO~~) At the January 2001 leadership offsite [redacted] the Command Group and staff leadership tackled the creation of a FY 00/01 Performance Plan. Using INSCOM's 1999 Strategic Plan, which covered goals for the next 5-6 years, the group created an annual plan to accomplish the long-term goals (some 36 initiatives). It also satisfied the demands of a newer requirement, the Government Performance and Results Act that encouraged an on-going planning process.

(b)(1),(b)(3) Per CIA

Strategic Goals. (U//~~FOUO~~)

1. Provide Actionable Intelligence to the Army Operations Center and the Army Service Component Commanders.

Strategic Objectives

1.1 Evolve the IDC CONOPs and architecture in concert with Army Leadership.
1.2 Develop doctrine and TTP for identifying, processing and disseminating actionable intelligence.
1.3 Demonstrate INSCOM capabilities to the Army leadership and the Intelligence Community.

2. Ensure INSCOM's Vision, Mission, and EAC Concept of Intelligence and Information Operations are Embedded into Army and Joint Doctrine.

Strategic Objectives

2.1 Secure acceptance by Senior Leaders of Army, DOD and the Intelligence Community.
2.2 Implement transformation concept into CONOP concurrently with Senior Leadership acceptance.
2.3 Identify relevant policies and propose changes/additions within 6 months of implementation.
2.4 Develop and implement plans to advance INSCOM's mission, vision, and capabilities NLT FY02.
2.5 Continuously revalidate, refine, and review intelligence and Information Operations requirements.

3. Identify and Establish Relationships and Agreements with DOD, the Intelligence Community, and Inter-Agencies to Advance INSCOM and Army Vision and Mission.

Strategic Objectives

3.1 Identify strategic partners by MSC, staff element, and discipline.
3.2 Define roles, responsibilities, and relationships and review annually.
3.3 De-conflict and synchronize INSCOM operations with Joint, Combined, and National level Intelligence Agencies/Organizations.
3.4 Formalize agreements as appropriate and review biennially.
3.5 Implement a strategy to advance INSCOM's vision and mission NLT FY02.

4. Identify, Exploit, and Sustain Leading Edge Technology.

Strategic Objectives

4.1 Establish and empower a coordinating office/technology board as the focal point for all future technological support requirements.

4.2 Actively participate in the Combat Development process.
4.3 Interface with industry, academia, and science and technology centers to leverage emerging technology.
4.4 Develop tactics, techniques, and procedures for identifying, exploiting, and sustaining leading edge technology.

5. Recruit, Train, and Retain a High Performance, Empowered Workforce.

Strategic Objectives

5.1 Attract and retain high performance personnel.
5.2 Establish developmental programs to sustain a quality workforce, and promote quality of life and wellness of the command.
5.3 Meet personnel retention quotas.
5.4 Ensure equity and fairness in the recognition and promotion of excellence.
5.5 Identify and reduce roadblocks and impediments to recruiting and retaining required personnel.

6. Resource and Organize the Command to Provide Real Time Intelligence, Security, and Information Operations Support to the Army Operations Center and the Army Service Component Commander.

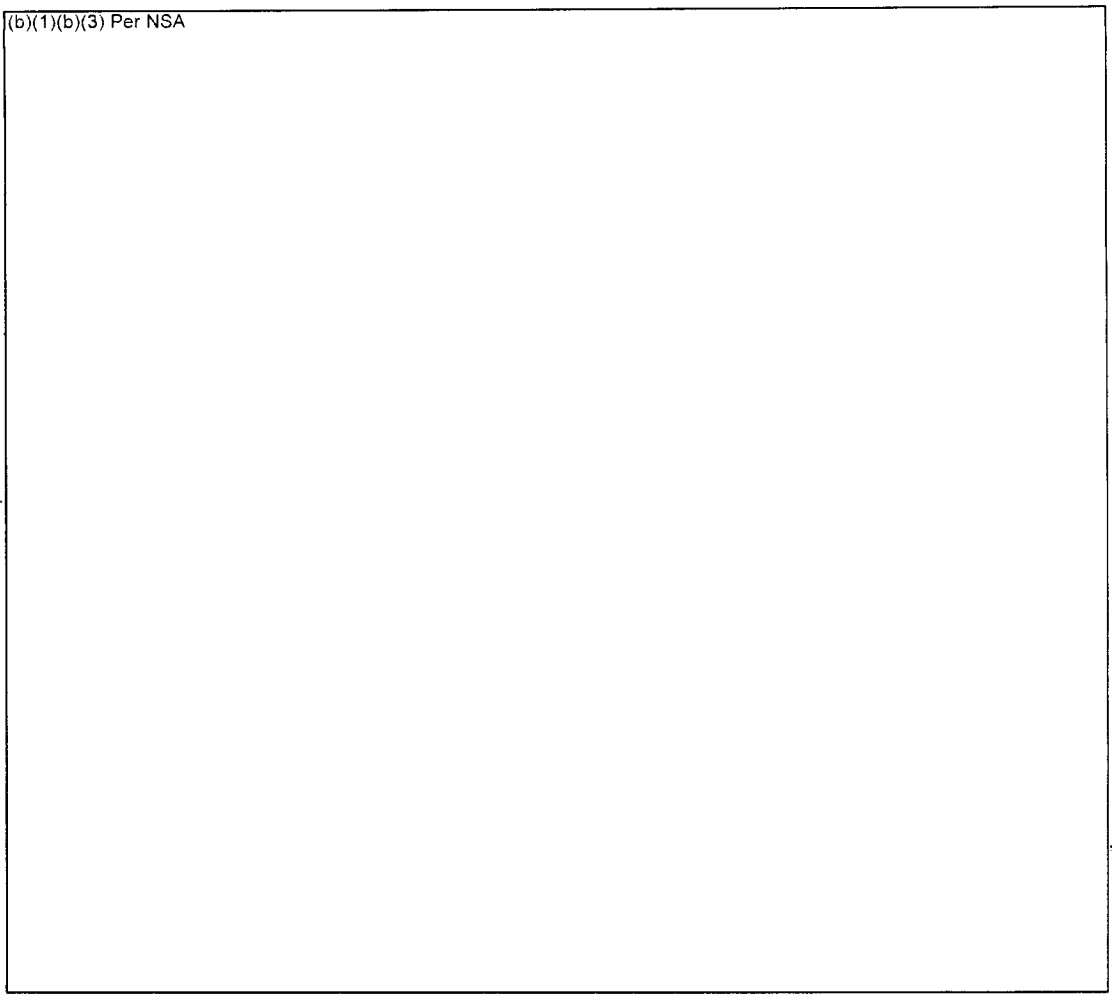
Strategic Objectives

6.1 Continually assess adequacy of command resources and structure to meet requirements.
6.2 Realign command resources to enable a knowledge-based, prediction oriented intelligence process responding to commander driven requirements.
6.3 Identify and leverage potential external sources of resourcing (funding and personnel).
6.4 Provide quality facilities and state-of-the-art Information Technology infrastructure to sustain INSCOM's people, equipment, organization, and mission.

(b)(1)(b)(3) Per NSA

~~TS~~

(b)(1)(b)(3) Per NSA



Standing Up of the Information Dominance Center (IDC). ~~(S//NF)~~ The IDC was established 2 years ago by LIWA. However, during the 4th Quarter, FY 01, the IDC evolved into becoming a "provisional" major subordinate command of the INSCOM. This change came as a result of how the IDC performed operations. The Information Dominance Center evolved into a congregation of powerful search and analytical tools, simultaneously coupled to available databases (IMINT, HUMINT, and SIGINT), and attached to a front-end SIGINT collection site. On 3 August 01, the National Security Agency assigned the SIGINT Designator

(b)(1)(b)(3) Per NSA [redacted] to the IDC. (This was a part of General Alexander's vision of offering "one-stop intelligence and information operations shopping.") The change in operations also led to organizational changes. The Commander, LIWA, was dual hated as the Commander, INSCOM IDC. Other entities wrapped into the IDC were the Intelligence Operations Center,

Futures Center, and Cyber Warfare Center. (The Intelligence Operations Center expanded its mission to provide Army-wide real-time Indications and Warnings (I&W) of count-terrorism, counterintelligence, information operations, and counter-narcotics supporting the total Army's overall "Force Protection.") The IDC possessed the necessary skilled IO and intelligence professionals along with software, hardware, and communications architectures to allow for worldwide synchronization and engagement of IO, IO-related, and focused-intelligence operations.

CHAPTER TWO

PERSONNEL, SECURITY, LOGISTICS, *Etc.*

MASINT Training. (U/~~FOUO~~) The MASINT Branch, G3, HQ INSCOM undertook a training initiative to ensure that warfighters would have greater access to MASINT scientific and technical intelligence. In October 1977, it began to offer the MASINT Basic Collector's Pilot Course; this was followed up with an Immediate Course and the MASINT Basic Analysis Training Course. These courses were directed at several different audiences. The first were to those MASINT specialists (civilian/military/Active/Reserve) being deployed. The courses provided an understanding of the MASINT community and how MASINT could be leveraged to meet intelligence requirements and contributed to the personnel's operational efficiency. A second group included members of the Analysis Control Elements, military intelligence commanders, and all the 2s (G2s, S2s, etc.). The purpose was to furnish these key intelligence types with the knowledge on how to fuse MASINT with other intelligence disciplines and how to leverage the systems to support intelligence operations. In FY 1998, 125 personnel had completed the courses; a year later, the total was 401. Formal training was also supplemented with interactive computer-based education including video tapes covering subjects that ranged from basic physics to collection management.

Reserve Status. (U/~~FOUO~~) FY 01 began with 224 allocated Reserve positions; another 19 positions were added for LIWA in the middle of the year, bringing the total to 243. (This did not include an additional 98 undocumented augmentees allocated to the Investigative Records Repository for a special screening and declassification project involving World War II records.) For FY 2001/02, INSCOM was scheduled for a plus up of 50 more individual mobilization augmentees (IMA), bringing the funded total to 293.

Overview of Security Issues. (UNCLASS/~~FOUO~~) Following the end of the Cold War, there were a number of important changes in how security threats against the Government were handled. Overall, the military, intelligence, and security environment became more complex not less so. When the Soviet Union was America's greatest potential adversary, it

was easy to ignore other threats. Once the Berlin Wall came down and the Soviet Union collapsed, the military and the intelligence community were faced with new challenges, such as China. The emergence of the United States as the sole world superpower also compounded the security problem. For instance, many countries that had been subservient to the Soviet Union or had close ties were now free to act independently.

(U) ~~(C)~~ At the same time the Soviet Union was coming to an end, computer technology was beginning to advance at an unparalleed pace. Suddenly security managers were faced with protecting information as opposed to documents, and information proved far more difficult to control. Now security types had to be aware how information was moving inside/outside their organization and by what means (phone, fax, e-mail, etc.). This required the installation of safeguards at critical points in the process. This became a tremendous challenge. The most common security violations facing INSCOM involved technology. For example, the case of an e-mail or a fax improperly classified or being sent over a nonsecure line. To complicate matters, it became easier for a person to make errors and to make them faster. The atmosphere at the major headquarters in which speed was demanded also did not help. And in future all would be compounded as technology continued to develop. For instance, the emergence of hand-held devices that plugged into systems and the use of infra-red waves for communications.

(U) ~~(C)~~ Unfortunately, many of today's security managers were not technologically savy enough to determine policy and to know the vulnerability of systems. For instance 20 years ago, security managers were concerned with double wrapping documents; now its e-mailing around the world. This has left security highly dependent upon a handful of persons with a high-degree of expertise to protect the systems. However, there are an insufficient numbers of such people in the Government to keep security up-to-date. This has led to security policy lagging behind state-of-the-art technology. Personal Digital Assistants (PDA), for example, were out before anyone had a policy on them. There is also a growing concern that even the so- called experts do not have a complete handle on all the potential vulnerabilities. For instance, the only difference between NIPRNET and SIPRNET is that the latter is encrypted, but both are using the same transmittal system. Because of

technology, those inside the system possess so much more access to information than in the past and that information can be captured in a disk and does not require a whole safe full of documents. One person walking out with a zip-drive in a pocket that cannot be searched without a warrant is our biggest threat. Through the years there has been a total break down of the "need to know" as a means of protecting information. A part of that breakdown can be attributed to the access that technology has provided the average member of the staff. SAP's are a part of the answer along with the use of stand-alone computers. Segregating information is another, but this is not a fool-proof system because individuals with sufficient know-how can break through fire walls. As we hire a new generation with increased technology smarts the vulnerabilities will only continue to increase. The bottom line is that as of today the security community remains behind the power curve in addressing these technology changes seriously. Security simply lacks the people with the know-how to do the job.

(U) ~~(C)~~ As the Cold War ended, the United States found itself dealing with more flashpoints. New alliances were formed, some of them with former enemies. How and what kinds of information can be shared? The DCI finally got serious about the whole issue of foreign disclosures in the last year and came out with guidance. For instance, HQDA has taken steps to ensure that INSCOM doesn't invite foreign personnel to the headquarters unless there is a specific reason. The Land Information Warfare Activity also plays a role in security. Its focus is counterintelligence such as having teams evaluate the vulnerability of a particular system. Information gained by LIWA in identifying and evaluating potential problem areas can be used to shape future security policy.

(U//~~FOUO~~) September 11th has brought new awareness of the threat. As a result, the overall security posture will change. Those in the intelligence business and the military will also experience changes in security, but they will not be as dramatic as the rest of the government because the intelligence/defense community is already operating at a higher level.

Contingency Funding. (U//~~FOUO~~) INSCOM continued to be tasked for the Bosnia and Kosovo contingencies. Due to scarce Army resources, it was once again necessary to justify INSCOM contingency requirements. Here, the Budget

Branch, DCSRM (HQ INSCOM) took the lead and was successful in receiving full funding. INSCOM's requirements slightly decreased for Bosnia to $11.5 million and increased for Kosovo to $8.8 million. (Resource requirements exceeding the USAREUR reimbursement were absorbed from internal funding.) INSCOM also received additional contingency funds in the amounts of $698,000 (FCI) for Southwest Asia, $1.056 million (FCI) for Bosnia, and $2.002 million (GDIP) for NGIC, Army Central, and Reserves.

Conversion of Inventory Control Systems. (U/~~FOUO~~) The Mission Stock Record Account (MSRA), which had transferred to the Intelligence Materiel Activity in FY 2000, had for years experienced difficulties with the use of the SARSS-O as an inventory control system. The problem was that SARSS-O was designed for standard items but MSRA primarily dealt with nonstandard, commercial off-the-shelf items. In early FY 2001, the G4 (HQ INSCOM) approved MSRA converting to the Inventory Control, Analysis, and Reporting System (ICARS). The conversion was considered a success.

Technical Surveillance Countermeasures (TSCM) Support. (U/~~FOUO~~) During FY 2001 the Intelligence Materiel Activity (IMA) continued to support the TSCM activity. In addition to providing acquisition and maintenance support for Army TSCM, IMA also provided these services plus training, testing, and development support for a growing number of non-Army agencies and activities. They included the Department of Energy and the Marine Corps.

Logistical MOUs/MOAs. (S) The ACofS, G4 had a record of 170 Inter/Intraservice Support Agreements and logistical MOUs/MOAs for INSCOM units both CONUS and OCONUS. The support agreements involved 85 installations, 61 of which were in CONUS and 24 OCONUS. For example, there was a memorandum of agreement between the INSCOM G4, SOUTHCOM, CECOM 12WD, and USAREUR to define the responsibilities for providing on-site electronic maintenance support for the TROJAN Air Transportable Electronic Reconnaissance System (b)(1)(b)(3) Per NSA integration and installation assistance with the TROJAN Classic upgrade to MCO3; and site support to TROJAN systems (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

Tactical Exploitation of National Capabilities (TENCAP). (U) ~~(S)~~ As part of the TENCAP effort, the Tactical Exploitation System (TES) was prepared for fielding by the 297th MI

Battalion at Fort Gordon. The system was in a HMMWV configuration which was to be upgraded to Wolf Coaches in its Final Operational Capability in FY 2002. Due to subcontractor slippage, system delivery was delayed and TES MAIN did not arrive at Fort Gordon, Georgia, until September 2001. At the fiscal year's end, fielding activities were still in process.

(~~S~~ -)

(b)(1)(b)(3) Per NSA

Gordon Facilities. (U/~~FOUO~~) The Gordon Regional Security Operations Center (GRSOC) was housed in Building 24701 (Back Hall), a two-story structure with a partial basement constructed in 1988. It had two interior open courtyards, which were accessible only from the inside first floor, plus a secure door for loading, unloading, and storage of all items shipped into or out of Back Hall. The building's footprint was approximately 79,200 square feet with approximately 50,900 square feet usable workspace for mission and mission support systems. Back Hall was planned and designed to accommodate a Satellite training mission, but was assigned to INSCOM in May 1995 for the GRSOC (operational, training, and administrative functions). In 1995, several construction projects totaling approximately $1.2 million, improved the HVAC and electrical systems, replaced and modernized the existing telephone system, and installed an uninterrupted power system. During FY 1998, three construction projects were completed that provided redundant electrical switchgear and transformers. In FY 1999, a new roof and an addition to Back Hall were added; the addition increased mission space by 1,250 square feet. In FY 2000/2001 the electrical system was again upgraded with Transient Voltage Surge Suppression (TVSS).

(U/~~FOUO~~) The Joint Language Center and the Headquarters, 116th MI Group moved from Building 21721 into Building 36708 the "Old" O'Club in November 2000. The Building 36708 was then renovated in just 8 weeks. Building 21721 underwent a 12-month $2.1 million HVAC and Electrical upgrade. Plans called for the top two floors of

the converted barracks to become a SCIF and to house J-3 classified training and the Navy Master Language Course. The first floor would serve the Headquarters, 116th MI Group.

New Home for NGIC. (U/~~FOUO~~) On 21 September 2001, the Nicholson Building (final price tag: $46.2 million dollars) was dedicated in honor of LTC Arthur D. Nicholson. (Nicholson, a member of the US Military Liaison Mission was shot and killed on 24 March 1985 while on a routine mission. He has been called "the last casualty of the Cold War.") The 256,000 square foot facility at 2055 Boulders Road, Charlottesville, Virginia, will serve as home to the National Ground Intelligence Center and will consolidate NGIC employees previously located at six rental properties within the Charlottesville area. In addition, some employees of NGIC's element at the Washington Navy Yard, District of Columbia, were also relocated to the new building.

Captured War Criminal Declassification Effort. (U) Following World War II, the US Government, including military intelligence, collected a large amount of records and information on Nazi war crimes and their perpetrators. As a result of the collapse of the Soviet Union, and their releasing records on the Nazi era, there was an increased interest in the subject, especially questions regarding the fate of Nazi-seized valuables and properties. To address these growing concerns, Congress passed the Nazi War Crimes Disclosure Act of 1998 that mandated the identification of still-classified records related to war criminals of World War II Axis governments. Once identified, they were to be reviewed and released to the American public. The Army's Investigative Records Repository at Fort Meade, Maryland, alone held 11,400 reels of microfilm representing more than 1 million documents. As commander, MG Robert Noonan committed INSCOM to completing the project within a year. (One expert estimated that manual review would take 181 man years to complete.) To meet its deadline, INSCOM turned to Sherikon, Inc., a reseller of document imaging solutions and Kofax Ascent Capture software, a high-volume document capture application that was coupled with Wicks and Wilsor high-speed microfilm scanners. Using 150 soldiers drawn largely from the 902d MI Group and 704th MI Brigade, the declassification team worked 6 days a week, 24 hours a day. The project was completed ahead of schedule and about 16,000 files related to Nazi-war crimes were identified.

(b)(1) & (b)(3) PER DIA

[redacted]

All total, the division supported [redacted] Army personnel assigned to [redacted] embassies worldwide. During the year, there was an ongoing effort to ensure that [redacted] remained a valid MI WO MOS. At the same time, the Field Support Center undertook several important initiatives: re-certified [redacted] maintained close relationship with the Soldier Support Center at Fort Jackson, South Carolina, to reconfirm the career path and promotions of NCO's; and staffed AR 611-60 that allowed the Field Support Center to recruit MI linguists for hard-to-find assignments.

(b)(1) & (b)(3) PER DIA

Impact of AG Transformation on the Field Support Center Activities. ~~(S)~~ The Adjutant General Transformation announced by the DCSPER of the Army had a number of impacts upon the Field Support Center. First, it was determined that the Military Personnel Center Chief had to be civilianized in order to maintain long-term continuity in essential knowledge and technical skills. Secondly, the coming of a "paperless" Army meant that individual soldiers would be given more overview of the management process pertaining to their careers. [redacted]

(b)(1)

[redacted]

(b)(1),(b)(3) Per CIA

(b)(1),(b)(3) Per CIA

(C)

(b)(1)

Deployment per Diem. (U) The FY 00 National Defense Authorization Act authorized "high-deployment per diem," and established the requirement to track soldiers' deployed and non-deployed time away from home. Congressional intent was to penalize all the services and their components for high deployment, and to reduce the time soldiers' spent away from home, thereby improving morale and quality of life. The Army's requirement to begin tracking started on 1 October 2000.

Accident Statistics. (U) For FY 01, INSCOM experienced 41 recordable accidents at a cost of $292,508, primarily sports and POV related.

Closure of the Army National Capital Region (ANCR) Civilian Personnel Operations Center (CPOC). (U) The closure of the ANCR CPOC led to the transfer of INSCOM Defense Civilian Intelligence Personnel System to the West CPOC at Fort Huachuca. At the same time, the Civilian Personnel Advisory Center was also transferred from the Personnel and Employment Services-Washington in the Pentagon to the Fort Huachuca CPAC. The transfer was completed by 6 October 2001. Plans called for the Fort Huachuca CPAC to establish forward based servicing at Fort Belvoir, Charlottesville, Virginia, and at Fort Meade, Maryland, to support local INSCOM elements.

Civilian Personnel Changes. (U) The transition from the Personnel Process Improvement (PPI) to the Modern Defense Civilian Personnel Data System (MODERN DCPS) took place at

the Army National Capital Civilian Personnel Operations Center in April 2001. This was part of the final phase to bring the military departments under one personnel processing system. By the close of the fiscal year, all CPOCs worldwide would be under the new system. Also in FY 01, the Inventory Based Recruiting (IBR) was put into place. When the CPOC received the recruit action all resumes that match the occupational series, lowest acceptable grade, and geographical location were entered into the applicant pool. (A resume would have to be entered into the system only one time.) The resumes of the applicant were then matched against the required and desired skills submitted by the manager. The resumes that matched all the required skills and the greatest number of desired skills were referred for consideration. A new award policy was also implemented on 1 October 2000. Commanders/Staff Heads could expend up to $2.5 percent of base pay but no more than 40 percent of the employees could receive cash performance awards and no more than 10 percent could receive Quality Step Increases or Exemplary Performance Awards. Although INSCOM had 14 man-years allotted to its intern program only 3 were actually on board at the end of the fiscal year due its ability to place personnel and to security processing delays.

Drug Testing: (U) Random drug testing for INSCOM civilian employees was implemented on 1 September 00. The program was command-wide on a monthly basis and was designed to meet DOD's requirement for testing of 50 percent of the command's occupied testing designated positions that numbered approximately 1850. Despite the interruption of testing due to 9/11, INSCOM still was able to test approximately 49 percent (904) of its pool. In addition, INSCOM conducted 222 pre-employment tests; of these entry tests, none were known to be positive.

Security Clearance Processing. (U) At the end of the FY 01, over one hundred tentative job offers had been made for INSCOM open civilian positions with 40 to 45 percent awaiting a security clearance. In September 2001, an interim clearance policy was put into place to accelerate the process for new employees. An interim clearance could be granted (given no derogatory information) following the initial National Agency Check (NAC) or a favorable NAC within the last 10 years or a SECRET clearance within the last 10 years. Those with no previous investigation could be assigned unclassified duties.

INSCOM Investment Strategy. (U) The INSCOM Investment Strategy (I2S) broke down a mission program into quantifiable strategies, and also identified the benefit to the warfighter. The strategies were then prioritized to ensure the most critical requirements were being resourced. The I2S was used as the basis for the development of INSCOM program submissions. A key result of the process was the determination of impacts for potential funding reductions or increases. This process required total staff involvement and ensured a balanced program was identified to include items such as equipment, maintenance, and automation. It also identified those requirements theater commanders addressed during the Integrated Priority List process.

FY 04-09 POM Strategy. (U) In July 2001, the Resources Management and G3 staffs' new strategy for the FY04-09 Army POM was approved for implementation. The objective was to increase INSCOM's market share of available Army resources. The new initiative changed several HQ INSCOM business processes for programming and budgeting, empowering the G-staff to take "ownership" for Management Decision Packages (MDEP) under their purview. The major changes were designating, by name and staff section, functional mangers for the existing 27 MDEPs of the command and also for 15 new MDEPs that have potential to provide additional resources; providing all MDEP managers training on the PPBES, Army POM development process and INSCOM Investment Strategy; adoption of a standard briefing to describe INSCOM's part of each MDEP, to be used for communications with HQDA. The intent of the new strategy was to increase sources of funding, better align INSCOM missions with standard Army programs, and establish or improve rapport between HQDA MDEP mangers, INSCOM MDEP mangers, and major subordinate command counterparts.

Mail Protection. (U/~~FOUO~~) The Headquarters Mail and Distribution Office operated the AS&E X-Ray inspection system on a daily basis to screen all incoming mail pieces/parcels brought into the Nolan Building from external sources for potential explosive devices. The AS&E MICRODOSE® X-Ray inspection system with BackScatter® technology was designed to detect plastic explosives.

Wearing of the Beret. (U) On 14 June 2001 (birthday of the US Army), soldiers (officers, warrant officers, and

enlisted) who were not authorized to wear the tan, green, or maroon berets donned the black beret.

CHAPTER THREE

INFORMATION AND SYSTEMS

Transfer of Billets to USAIC. ~~(TOUO)~~ As a result of the larger MI "Unified Proponency" effort going on, the DCSINT (LTG Kennedy) and CG, INSCOM (MG Noonan) agreed in early 2000 that 61 billets (representing eight combat development regulatory-based requirements) should be transferred from the control of INSCOM to USA Intelligence Center at Fort Huachuca, Arizona and thus solve a problem that had existed for 15 years. It was simply a matter of putting all combat development spaces in one basket. The CG, INSCOM, being a MACOM, served as the specified and functional proponent material developer (AR 5-22) and the organization through which ODCSINT executed its requirements. (There were other requirements, such as INSCOM being designated the Army's Service Cryptologic Element, etc.) At the same time, the CG USAIC&FH served as the branch proponent. (The location of most of the transferred spaces would not change from the Nolan Building at Fort Belvoir, but rather only the control would pass to USAIC.) These spaces would continue to focus on echelon above corps issues for the most part. However, despite the transfer, a number of fundamental problem areas still remained unresolved. In the past, Fort Huachuca had often failed to adequately address EAC architecture, and INSCOM had only done it on a project by project basis. In summary, minimal effort was given to identify the broad range of INSCOM requirements that went beyond a five-year timeline.

Overview of Information Arena (U) ~~(C)~~ Over the last several years, there were several major themes within the G-6 arena. Just 3 years ago, the headquarters was in the process of fielding a LAN system within the Nolan Building that was a combination of ATM and Ethernet. Many had jumped on the ATM wagon when it first came out, but had failed to understand that ATM was not intended for local networks. Rather, ATM was created to work in the "white area" (outside the building and for long distance.) As a result, there were growing complaints from users on how slow their systems were working. The first step in solving the problem was to get rid of ATM and to move exclusively to Ethernet. This proved to be a major milestone in networking. Since then the command took a second step to GIGABIT Ethernet. (The upgrades on IDUN and SIPRNET had

just been completed, leaving only the THOR and NIPRNET to go.) The headquarters also demonstrated the ability to make quantum improvements in networking capabilities. Just 3 months ago, the IDUN was 10 share (that means that everyone was operating at 10 megahertz which led to numerous collisions on the network). This was an example why upgrading must be ongoing. It is interesting to note that LIWA was currently experiencing many of the same problems that the headquarters had to wrestle with 3 years ago—slowdown of the desktop network due to ATM. Erroneously, consumers often believe they have a bandwith problem and go out and purchase too much. In the past, the critical question of whether or not people actually required what they requested was not being asked. As a result, a couple of trunks lines leaving the building are using only 2 percent of their capabilities.

(U//~~FOUO~~) Funding was a key to success if networks were to be systematically upgraded. Because people don't adequately articulate their needs, they often fail to obtain the necessary funding. The bottom line is that the funding cycle must be rigorously followed. To illustrate, over the last three years, the headquarters moved from Windows 3.1 on some computers to Windows SP--in all a total of seven systems--each one requiring a little bit more in hardware. The same with the switching systems. It was a never-ending process.

(U) ~~(C)~~ Other important milestones included the recent establishment of the Chief Information Officer (CIO) and the ITMC (IT Management Council). Mitre and MICROSOFT consultants were also hired as resident experts. For example, if it had not been for these consultants, the establishment of the Portal would not have been possible. Another initiative has been the consolidation of databases within the headquarters. This was a key factor leading to the reorganization of the G-6/SI/CIO. Plans called for the Systems Integration (SI) to go awa, and its present resources that are involved in development will go to the G-3. Another highlight was the professional way in which headquarters G-6 types effected the transfer of all the information networks and telecommunications from the old to the new NGIC Building. It all went off without a hitch. And this was not the first time; the same efficient transfer took place when INSCOM elements moved from Fort Shafter in Hawaii to Fords Island. Recently, teams set up a new communications center at Pyong Taek in Korea. Over the

last 2 years telephone exchanges were replaced at the Nolan Building. However, there are problem areas. Traditionally, MSC's have operated independently because they were responding to and supporting different consumers. At the same time, it was essential that there be interoperability within INSCOM. (Presently, INSCOM possesses some 10,000 desktop computers.) Ideally, all hardware could be centrally purchased. Although this has not happened, there have been improvements. For instance, since 1999, the headquarters has centrally purchased software, and command-wide Information/Technology conferences are being held. This allows for increased dialogue. Finally, there is the area of visual information. Over the last several years, upgrades in VI have been neglected, largely due to the inability to effectively work the funding process. All the while the demand remains high for such support as video conferencing.

Foreign Language Technology Website. (U//~~FOUO~~) The need for translation of foreign languages in real-world operational environments has become critical and difficult to achieve with fewer linguistic assets. HQ INSCOM recognizes the need for more rapid foreign language technology "triage" applications in support of combatant commanders. A Foreign Language Technology web site was developed with seed money from HQ INSCOM, Office of the Assistant G3, Operations Readiness; the Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (OASD C3I); and MITRE Corp. This effort provided the field with information available on government-off-the-shelf (GOTS) and commercial-off-the shelf (COTS) products and technologies for languages of interest to DOD.

501st Network Operations Center Consolidation. (U//~~FOUO~~) In October 1999, the 501st MI Brigade undertook the enormous task of consolidating subordinate battalion NOC operations and all associated communications assets into one building at the 527th MI Battalion. Project completion occurred in June 2000. This was followed by expanded NIPRNET LAN and SIPRNET LAN connectivity.

Headquarters Networks. (U//~~FOUO~~) HQ INSCOM operated four primary local and wide area networks providing connectivity to the NIPRENET (VULCAN), SIPRNET (FREY), JWICS (IDUN, and NSANET (THOR) backbone infrastructure. During the fiscal year, there was a continued effort to upgrade and expand

the server farm by obtaining 30 additional rack mounted servers. These servers were used to upgrade the email servers on all four local area networks (LAN), upgrade file and print servers, establish intranet/portal services on the SIPRNET and JWICS Lans. All Windows NT servers were migrated to Windows 2000 as the baseline. Also doing the year, efforts were underway to expand the SIPRNET LAN to meet the Command and Control requirements contained in the CIO's 5-year IT Plan.

(U//~~FOUO~~) The NIPRNET ATM backbone proved difficult to monitor and troubleshoot and did not provide the increased performance promised by the technology. So it was transitioned to GIGABIT, a process that went very smoothly and resulted in no interruption in service and in the end solved many real and perceived problems.

Information Dominance Center (IDC) Portal. (U/~~FOUO~~) In response to the terrorist attacks of 9/11, the CG INSCOM directed the creation of a worldwide portal as a follow-on to the making the IDC operational. The Chief Information Officer used Microsoft's Sharepoint Enterprise Portal Server to satisfy the tasking; this represented a new technology application for the command and accomplished command and intelligence community-wide collaboration and sharing of information. Because of classification issues, the JWICS network was the location of the portal which provided for higher classification because of its ability to limit user access. However, the G6 had to perform numerous upgrades to the backbone of the network and field a significant number of PCs to adequately meet the mission. As a measure of the portal's remarkable growth and wide dissemination, over one thousand users registered in a three week period.

Viruses. (U/~~FOUO~~) Three major viruses (NIMDA, Code Red, and SirCam) hit a variety of corporations and even some military organizations extremely hard during FY 2001. However, they were a non-issue at Headquarters, INSCOM. In addition, INSCOM was able to catch and clean tens of thousands of other viruses transmitted through e-mail.

(U/~~FOUO~~)

(b)(7)(E)

(b)(7)(E)

Mandatory Deployment of Systems Management Server (SMS). (U) The Automated Systems Integration Management (SIM) Intelligence Database (ASID) was INSCOM's primary tool for managing the IT investment through tracking and reporting the command's enterprise information infrastructure. Originally, ASID was a manual web-based process without the capability of automatic updates. In order to comply with the Chief of Staff, US Army guidance of 8 August 2001 and to make not only ASID but the IT management process more robust, INSCOM was forced to migrate to a more comprehensive solution and to add automatic discovery tools. The INSCOM Chief Information Officer then created a migration strategy for Microsoft's System Management System (SMS) and began fielding the system at several of the major subordinate commands. However, it was not all smooth sailing because of lack of full cooperation on the part of some of the subordinate commands.

CHAPTER FOUR

OPERATIONS

Unified Cryptologic System (USC) Transformation. (U//~~FOUO~~) The 1998 *Unified Cryptologic Architecture Study 2010,* commissioned by the Director of Central Intelligence and the Deputy Secretary of Defense, concluded that the Intelligence Community (IC), faced major technological and operational challenges, requiring a fundamental redesign of the SIGINT system. As Manager of the US Cryptologic System (USCS) and Community Functional Lead for SIGINT, the DIRNSA established the Unified Cryptologic Architecture Office (UCAO) to assist in the "fundamental redesign" of the IC through the implementation of a Unified Cryptologic Architecture (UCA). The UCAO developed an initial Master Transition Plan (MTP) by tailoring the Capability Maturity Profile (CMP) as outlined in DOD's study, *Architecture Framework,* dated October 2000. In short, the CMP evolved into the first MTP.

(U//~~FOUO~~) At the end of FY 2001, the various IC partners were drafting cost estimates for two options. These would then be evaluated by the Expanded Corporate Management Review Group. At the same time, Army intelligence was facing a "fundamental redesign" as a result of the Army Intelligence Transformation Campaign Plan and the Intelligence Electronic Warfare Modernization Plan. The challenge for Army leaders was to ensure synchronization with national and joint transformation efforts. Failure to do so could make Army cryptologic operations inconsistent within a transformed US Cryptologic System and could place the Army in danger of becoming non-interoperable and stove-piped and not contributing to the national SIGINT effort.

(S) (b)(1),(b)(3) Per CIA

(b)(1) (S) (b)(1)

(b)(1)

(b)(1)

(b)(1) (~~S//NF~~) (b)(1)

(b)(1)

(~~S//NF~~) (b)(1)

(b)(1)

(b)(1)

(b)(7)(E) (U//~~FOUO~~) (b)(7)(E)

(b)(7)(E)

(b)(1) (S//NF) (b)(1)

(b)(1)

(b)(1) (S//NF)

(b)(1)

(b)(1)

(S//NF) (b)(1)

(b)(1)

The Army's Relationship to the National Reconnaissance Office (NRO). (U) In an article that appeared in *Military Intelligence* magazine (April-June 2000), Colonel Donald L. Langridge outlined the background of the NRO and Army's relationship to it. What follows are excerpts from "Freedom's Sentinel in Space—the National Reconnaissance Office": (It should be noted no INSCOM spaces were involved in any of the internal Army elements mentioned as being connected with the NRO.)

(U) President Dwight D. Eisenhower secretly established a small, civilian-run office in the Pentagon in August 1960 to oversee a fledgling, experimental, military satellite reconnaissance program. Eisenhower thus set into motion a chain of events that, a year later, resulted in the founding of the organization known today as the National Reconnaissance Office (NRO), with responsibility for all US national-level overhead reconnaissance activities.

(U) Operating in near-total anonymity for the next four decades, the NRO succeeded in developing for the United States an unprecedented global capability to conduct sophisticated signals and photographic reconnaissance from space. This capability remains unmatched by that of any other nation to this day.

(U) As the United States' "eyes and ears" hundreds of miles overhead through the darkest days of the Cold War and beyond, NRO satellites have logged more than 40 years of distinguished service to the nation. As the country fights the War on Terrorism and faces new challenges in the 21st century, the NRO stands proudly as "freedom's sentinel in space.

(U) Publicly acknowledged for the first time in 1992, the NRO is a separate operating agency of the Department of Defense and one of the 13-member agencies of the national Intelligence Community. The

Secretary of Defense and the Director of Central Intelligence jointly manage the NRO. The NRO Director also serves as the Undersecretary of the Air Force.

(U) Since the Gulf War, the Army and the NRO have greatly strengthened their partnership. They are working hard to improve the support the NRO provides from space-borne reconnaissance assets to the combat forces planning for contingency operations, engaged in stability operations and support operations, and in actual combat. The Army now has three structures that work directly with and for the NRO. The Army Coordination Team (performs liaison functions), the Army Element (management of Army personnel assigned to NRO), and the Army Support Group (supported Army elements preparing for exercises and deployments) work in the areas of facilitating Army-NRO issues and internal NRO missions, and directly addressing Army Component requirements to meet the challenges of the future, respectively….

(S//NF)

(b)(1)

~~FOUO~~ ~~(S)~~ The Fall of the Wall occurred in 1990, with the subsequent demise of the Warsaw Pact and the USSR. The immediate effect of this event was a reduction in the frequency of SAEDA reports. The common perception of the USAREUR population was, "We won the war, and there is no intelligence threat anymore." The statistics from 1989 to 1998 remained very consistent. However, in 1998 there began a significant increase.

(b)(7)(E)

September 11 Legal Policy Changes. (U//~~FOUO~~) As a result of 9/11, there were greater changes in legal policy than in the law itself. For example, the Defense Authorization Act held only minimal change. Under the Patriot Act, law enforcement was granted greater flexibility in obtaining flasher warrants, but no new powers were specifically

created to help the Department of Defense. However, there was a temperature change that led to new policies. For example, it became easier under legal interpretation for counterintelligence and intelligence types to obtain for example credit histories. The important changes came as a result of sections 217 and 1003 of the Patriotic Act which created authority under the Electronics Privacy Act for a Third Party to monitor computer trespasses.

(b)(7)(E)

In the latter, it was possible to observe communications of those who hacked into Government communications. (In the past the ability to conduct this type of operations was based only on legal analogy.) For the first time, Congress came out and said that there was no expectation of privacy upon breaking into any public or private system. Prior to this, it had been the subject of an ongoing debate within DOD. At the same time, it should be remembered that this authority along with many of the other provisions of the Patriot Act are subject to a Sunset Provision wherein they will go away in December 2005 and the debate may be resurrected.

(U//~~FOUO~~) The Intelligence Act of 2002 witnessed the inclusion of the Coast Guard for the first time. This was significant because the Coast Guard was the closest thing the United States had to a *gendarmerie* such as in France or Belgium--a branch within the armed forces that possessed a law enforcement responsibility. For the most part, the Coast Guard comes under the Department of Transportation, but from time to time, they also fall under DOD. Congress acknowledged for the first time that the Coast Guard possessed an intelligence role that touched upon the protection of our borders and homeland security. For the first time, their intelligence role was being codified.

(U//~~FOUO~~) Looking to the future, many things that INSCOM wants to do are driven by policy not by statute and policy continues to evolve.

(b)(7)(E)

Finally, the various services have interests of their own in protecting their personnel. "Cyperspace is a unique place and we can't have agencies bumping up against each other." The bottom line is that law and doctrine will continue to evolve. There is also a

huge disconnect between the Foreign Intelligence Surveillance Act and the Electronics Communications Privacy Act. In the United States under domestic law, foreign agents have more protection than criminals. That is because the definition of "contents" under the Foreign Intelligence Surveillance Act prevents us from keeping such network data as telephone numbers or IP addresses. Whereas, the Supreme Court has granted law-enforcement this ability to record such information.

~~FOUO~~ ~~(S//NF)~~ (U) At this time, computer operations are probably the most important thing the SJA Office is involved in and requires constant legal scrutiny. Privacy is the watchword, and one simply can't do anything in this arena without legal guidance. When you decide to conduct an operation you require a legal review because the consequences are significant without one. To add to the normal challenges of 9/11,

(b)(7)(E)

Intelligence Oversight Issues. (U)

(b)(1)

INSCOM was the successor to the Army units involved. Consequently, the command took a very rigid stance in applying its oversight responsibilities, and lawyers began to become major players in operations. The INSCOM Intelligence Oversight Office itself promoted a very narrow, bureaucratic way of processing and reporting possible violations tempered with little judgment. In fact, it was becoming increasingly evident to those in human intelligence and counterintelligence that INSCOM was

adhering to a stricter interpretation of the law than anyone else in DOD, including other Army commands.

(b)(1)

For example, during DESERT STORM, INSCOM counterintelligence was initially paralyzed due to the absence of memorandums of understanding with the host countries while their counterparts in the other Services were going about traditional counterintelligence duties in support of arriving forces.

~~TOUO~~ (U) ~~(C)~~ Through the 1990's, with increased terrorism (and the lack of HUMINT/CI often taking the blame) and the coming of a new generation of leadership, changes slowly began coming within INSCOM.

(b)(7)(E)

As a departure from the past, the new director gave the local commander more flexibility in making the call.

(U) ~~(C)~~ September 11th only accelerated this change in culture, particularly as it related to the legal side and the involvement of lawyers. This did not mean that there were not continued struggles. For example, in Afghanistan there was a call as to whether or not they could video-tape prisoners. There was also a recent effort by the legal types to censure showing pictures of US target sites mentioned in documents found in Afghanistan.

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 42

IAGPA-CSF Form 6-R
1 Sep 93

(b)(1)

(b)(1)(b)(3) Per NSA (~~TS~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Pre 9/11 Support to Counter Terrorism. (~~TS~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(b)(1)

(b)(1)

Army Counterintelligence Center. (U/~~FOUO~~) The Army Counterintelligence Center (ACIC) was the Army's only strategic counterintelligence analysis center. Located at Fort Meade, Maryland,

(b)(7)(E)

~~(C)~~ The Technology Protection Branch did most of the work. Its analysts possessed expertise in intelligence threats to specific technologies, weapons, and systems. For example,

(b)(1)

Finally, the Investigations and Operations Branch augmented counterespionage investigations by examining sensitive intelligence data for leads and by mining data sources previously unexploited.

(U) ~~(C)~~ The ACIC continued to use Intelink as the primary means for delivering finished intelligence studies to requestors. Over 90 percent of ACIC products were disseminated in soft copy, and studies were posted with 24 hours of release.

(b)(7)(E)

Since October 1997,

the ACIC had posted over 400 studies.

(b)(7)(E)

Prior to 9/11, the ACIC provided threat assessments for high-level travelers (senior Army and DOD officials). Assessments were also provided for site-specific locations as required. The Counterintelligence Periodic Summary summarized terrorist and CI events worldwide. Analysts inputted to command assessments that reported on threats to US Army interests worldwide.

NGIC's Reach to the Field. (U//~~FOUO~~) One way NGIC supported the commander on the ground was by enhancing the analytical capabilities of INSCOM's Theater Analysis and Control Elements. This was accomplished by using the concept of "reach," a virtual and collaborative process that allowed an ACE to access the center's knowledge base that included subject matter experts, intelligence products, and on-line databases. The end results were a more complete and detailed picture of enemy capabilities that the ACE could pass on to the Service Component Command, whose requirements were often greater than the Theater Joint Intelligence Center could provide.

(U//~~FOUO~~)

(b)(7)(E)

(U//~~FOUO~~) The NGIC used two types of organizations with which to support the ACE. The first was the NGIC Liaison Element, usually consisting of two personnel, who were assigned to the ACE in pre-deployment phase. They not only assisted the ACE in drawing the NGIC database but gained insights into the ASCC commander's requirements which facilitated the offering of "brilliant push" type of support. Secondly, the NGIC Crisis Action Team (CAT) were

activated at the onset of a crisis or exercise and were able to undertake 24 hours-a-day operations. (The team also grew upon other organizations such as the Army Counterintelligence Center (902d MI Group) for expertise.) The CAT monitored the friendly and opposing force situation, managed Requests for Information, directed "smart pulls" or "brilliant pushes," and facilitated collaboration and coordination with other headquarters. Finally, NGIC's Imagery Crisis Response Cell and the Army Imagery Requirements Office were also capable of operating on a round-the-clock basis to support crises or exercises.

~~(S//NF)~~

(b)(1)

~~(S//NF)~~

(b)(1)

(b)(1)

(U) ~~(S//NF)~~ During the year, significant problems arose regarding soldier deployments in support of sensitive non-Army, DOD activities. In some instances Secretary of the Army and CG, INSCOM prerogatives were being ignored by the supported organizations, resulting in unnecessary risks to soldiers and the entire ACP. As a result, clarifying guidance was issued that resulted in improved efficiency of support and reduced soldier and mission risk.

(b)(1) **Activities.** ~~(S//NF)~~ Besides its HQ INSCOM element, maintained a collection management element within NSA (b)(1)(b)(3) Per NSA for the purpose of coordinating information requests and subsequently tasked (b)(1) units worldwide. (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

~~(TS~~) During FY 2001, NSA presented (b)(1) Detachment (b)(1)(b)(3) Per NSA with the National Intelligence Meritorious Unit Citation. The basis of the award was (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

The operation was a joint effort between the Defense HUMINT Service and (b)(1) (b)(1)(b)(3) Per NSA

Polygraph Program. (U//~~FOUO~~) INSCOM's Polygraph Program conducted 1,792 CSP examinations. Of these 1,737 were no significant responses; 40 were inconclusive; 15 were significant responses; and 11 were no opinion. The command had a 94.8 percent overall resolution rate; a 2 percent non-support rate; and a 13 percent admission/deception indicated confirmed. The program completed 67 operational cases of which 58 were no deception indicated; 4 were inconclusive; 4 were deception indicated; and 1 tested no

opinion. Following the DOD Polygraph Institute Quality Assurance Program's inspection, it lauded the INSCOM polygraph program as one of the best.

(U/~~FOUO~~) Two INSCOM polygraph examiners (from the 66th and the 902d MI Groups) conducted 32 security screening examinations in Sarajevo and Tuzla, Bosnia-Herzegovina. This involved screening of civilian local hires for Stabilization Forces (SFOR). An evaluation of the process was to be used in determining the feasibility of making such screen test a routine part of SFOR's force protection program.

(b)(1) (b)(1)

(b)(1)

Deployable systems supported throughout FY 01 included several deployments of (b)(1) in exercise and contingency scenarios; rotational redeployments of the three STEAMROLLER (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA for refurbishment without a drop in effective coverage (INSCOM received 1.3 million dollars from DA/NSA) to retrofit and increase communications bandwith); numerous contingency and exercise deployments of all echelon (b)(1) and following 9/11, facilitated uninterrupted and assured high data rate secure communications for the WMD CST UCS. (On 9/11, 10 additional vans were fielded.)

EAC Information Operations Requirements. (U//~~FOUO~~) An internal plan looked at INSCOM's IO requirements for the near-term. In the plan, increased anti-terrorism counterintelligence support (including personnel) as mandated by the Cole Commission's findings and endorsed by the Chief of Staff, US Army were addressed. Under the

plan, a robust all-source analytical cell would be created that would provide "reach" support to the overall force protection mission. The plan also addressed the need for "information superiority" and called for the consolidation of all IO functions at INSCOM. But for all of this to happen, was a need for more resources.

501st (b)(1) ~~(S//NF)~~ During the year, the 501st MI Brigade operated four (b)(1) (b)(1) These included a focus on growing threats from (b)(1) (b)(1) (b)(1) (b)(1) the 501st that would address early warning and force protection reporting of terrorist acts.

~~(S//NF)~~

(b)(1)

~~(S//NF)~~

(b)(1)

Combat Development Target. ~~(TS/~~ (b)(1) The G3 alerted the Intelligence Community (b)(1) (b)(1)

General officers from STRATCOM were briefed on the matter leading to requests for additional information. The G3 also briefed Taiwanese officials (b)(1)

(b)(1)

Deployment of the G3 Information Operations Warfare Activity (IOWA) Team. ~~(S//NF)~~ The USFK and EUSA established an operational need for the development of exploitation and electronic warfare systems to counter a North Korean (b)(1)

(b)(1)

Smugglers. ~~(S//REL UK)~~ C Company, 66th MI Group passed actionable (b)(1) information to Task Force Falcon that led to the detention of two possible smugglers and the seizure of military uniforms and flak vests in the vicinity of Lovce, Kosovo, on 29 March. Three days later, the Army Europe (b)(1) provided tip-offs that allowed for the arrest of two more suspects near Podgrade, Kosovo. These

(b)(1)

~~(S//NF)~~

(b)(1)

USN EP-3 Crisis. ~~(TS~~) In April 2001, a disabled USN EP-3 reconnaissance plane collided with a PLAAF fighter and

was forced to land in China. Linguists (b)(1)(b)(3) Per NSA Group shouldered the majority of the workload (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA providing critical insights to the National Command Authority that passed the information on to Ambassador Prueher at the bargaining table. Up to the release of the crew, (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

MRSOC Role. (~~S~~) The Medina Regional Security Operations Center first (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Significant IIR. (C/~~NF~~) The Kaiserslautern MI Detachment, 66th MI Group, published a FORMICA interim intelligence report (IIR) (b)(1) (b)(7)(E)

(b)(7)(E)

CI Support to Force Protection. (C//~~NF~~) The 205th MI Battalion, 500th MI Group sent a three-person CI team (b)(1) (b)(1) to provide force protection for a USARPAC engineer platoon that was building a hospital annex (b)(1) as part of the CINC's Theater Engagement Plan. The CG USARPAC ordered the activation of the CI team in response to increased activity of a Maoist insurgency group and a rising civil unrest (b)(1) The CI team conducted vulnerability assessments, limited analysis, and liaison support (b)(1)

(b)(1)

(b)(1)

(b)(1) This was significant in that for the first time this computer-to-computer capability would take computer network attack beyond hacking/cracking into network operations that supported the operations.

(b)(1)(b)(3) Per NSA ~~TS~~, (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

~~TS~~,

(b)(1)

(S//NF)

(b)(1)

International Crime. (S/) SIGINT specialists from the 704th worked at NSA's International Organized Crime Branch

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA (S/) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(S//NF)

(b)(1)

Regraded SECRET on 16 Jan 2014 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1); (b)(1) & (b)(3) per NSA

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 54

66th Intelligence Information Report. ~~(C//NF)~~ (b)(1)

(b)(1)

Support to Counter-terrorism. ~~(S//NF)~~

(b)(1)

Counterdrug. (~~TS~~, ~~NF~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

New SIGAD. (~~U~~) On 3 August 2001, the National Security Agency assigned the SIGINT Activity Designator (SIGAD) (b)(1)(b)(3) Per NSA to the INSCOM Information Dominance Center (IDC). This allowed the IDC to conduct SIGINT within the NSA/CSS charter. (The goal of IDC was to provide Army-wide real-time indications and warnings of counter-terrorism, counterintelligence, information operations, counternarcotics, and force protection.) (b)(1)(b)(3) Per NSA comprised the SIGINT development and analytic effort associated with the CG INSCOM's initiative of enhancing counter-terrorism indications and warnings support for force protection. As the FY 2001 came to an end (b)(1)(b)(3) Per NSA was still a work very much in process.

(b)(1)(b)(3) Per NSA

Threat Assessments. ~~(S//NF)~~ (b)(1)

(b)(1)

(b)(1)

(b)(1)(b)(3) Per NSA **Support to Task Force Eagle (TFE).** (~~S~~) (b)(1)(b)(3) Per NSA continued to provide Indications and Warning and Force Protection support to TFE. In one instance, the AETCAE (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Waiver to Collect. (~~S~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Uninhabited Aerial Vehicle. (U/~~FOUO~~) In an article "March of the Robots," John D. Gresham wrote on the background of the uninhabited aerial vehicle (UAV).

(b)(7)(E)

Current systems being tested included the prototype helicopter UCAV armed

Regraded SECRET on 16 Jan 2014 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R

with Hellfire ASM on an old QH-50 DASH drone. Army engineering and ordnance disposal units had also made use of robots for years to support vital and dangerous tasks. In late October 2001, the entire DOD UAV program achieved a milestone when an RQ-1 was used in Afghanistan (Operation ENDURING FREEDOM) to target and then fire an AGM-114 Hellfire air-to-surface missile (20 lb warhead) guided by a laser.

(U//~~FOUO~~) The big question that remained unanswered was the role UAV would play in the Army's Future Combat System, currently a "paper" system designed to replace heavy Cold War-era fighting vehicles like the M1 Abrams and M2/3 Bradley. (b)(7)(E) Looking to the "possible," the UAV could serve as an off board sensor/weapons platform.

115th Support to ENDURING FREEDOM. (~~TS~~) The group's most visible contribution to the campaign was to the tactical customers prosecuting the war. The Warfighter SIGINT Integration Cell, along with the USARPAC RTCAE, provided a (b)(1)(b)(3) Per NSA to CENTCOM collection managers. (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA Support also existed in the form of real-time threat warning. (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

9/11 Changes to IDC Capabilities. (~~S~~) (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Uniqueness of the IDC. (~~TS~~) The Information Dominance Cell searched for the electronic network developed when communication occurred, and for the intelligence inherent in these relationships for cross-cueing the other intelligence disciplines. The IDC was a congregation of powerful search and analytical tools (COTS/GOTS), simultaneously coupled to available databases (IMINT, HUMINT, and SIGINT), (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

INSCOM Support to the Tactical Commander. (U//~~FOUO~~) Within each unified command, INSCOM intelligence support served as the primary conduit for intelligence information between the tactical command and national and other military services' intelligence organizations. Additionally, the Army tailored the theater intelligence brigades and groups specifically to the meet the requirements of the various Army Service Component Command (ASCC) commanders and to support the various unified commanders. An important part of INSCOM's larger effort was to provide intelligence support to the lowest possible tactical echelon, and when S2s effectively leverage INSCOM capabilities, they were able to significantly increase the intelligence support they could provide to their commanders. The primary means of exploiting this capability was through the use of effective requirements management (RM) or mission management (MM). Although a maneuver brigade or battalion could not directly task an EAC intelligence support element, it could leverage the capabilities through the RFI

process. However, one common problem with RFIs was that the request was too vague to answer.

Future Challenges. (U) As part of the Association of US Army's Intelligence Symposium held at DIA in August 2001, LTG Robert W. Noonan, Jr., DCSINT outlined a number of trends impacting upon the Army and its intelligence arm in the future. The first was that unlike the past, future conflicts will be fought in urban terrain. By 2020, 66 percent of the world's population will live in these urban areas. Secondly, the Army must maintain its technology edge in weapons and intelligence systems. This meant that Army intelligence must get its arms around technology transfer so that the Army can be prepared. Finally, the proliferation of information was making the world one global village.

CERT Support. ~~(TOUO)~~ The ACERT (Army Computer Emergency Response Team/Coordination Center) and the RCERTs (Regional CERT) responded to 14,641 incidents on Army computer systems/networks in FY 01, which was again, as in FY 00, a dramatic increase in the number of recorded incidents compared to the previous year. The breakdown was 31 denial-of-service attempts, 98 intrusions, 12,744 probes/scans, 1201 access attempts, 219 poor-security practices, 298 malicious logic incidents and 50 incidents of unknown origin.

ADDENDUM

(The INSCOM History Office was made aware of the following information too late to be included in earlier summaries.)

(b)(1) **DHS.** ~~(S,~~) In June 1993, the Department of Defense offered up a study that would create a Defense HUMINT Service (DHS). Under this proposal, all of General Defense Intelligence Program resources of DIA and the military services would be consolidated into a single agency under DIA's control.

(b)(1)

~~(S.~~)

(b)(1)

Regraded SECRET on 16 Jan 2014 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R

~~(S.~~) As a compromise, (b)(1) created a memorandum of understanding that align the program with the new Defense HUMINT Service while at the same time, maintaining its independence. For instance, (b)(1) would place representatives at various DHS operational bases (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA Mr. (b)(6) and (b)(1) would also maintain an office at DHS. (This was later eliminated when NSA sent its own person to DHS to represent all SIGINT

interests.) All these actions ensured synergy between (b)(1) and the larger Defense HUMINT effort.

Chief Information Officer. (U) The Chief Information Officer began as a concept borrowed from industry and applied by Congress in the 1996 Clinger-Cohen Act to help redesign government and dramatically change the way business was conducted. In 1996, DOD named the ASD/C3I as its CIO and the Services and Agencies rapidly followed suit. (The Director of Information Systems Command, Control, Communications and Computers (DISC4) was appointed as the Army's CIO.) In January 2000, INSCOM created its CIO on the basis of AR 25-1. The mission was to procure, build, manage, and maintain an achievable, collaborative, worldwide Army Intelligence enterprise solution that linked INSCOM with its units, partners, supported and supporting agencies, and managed future information management and information technology (IM/IT) investments. The CIO represented a new way of doing business and had the authority to look across the entire command regarding IM/IT issues.

FY 01 UNIT SUMMARIES

National Ground Intelligence Center

History: (U) With the breakup of the Army Intelligence Agency, two of its principal parts (the USA Foreign Science and Technology Center (FSTC) and the USA Threat and Analysis Center (ITAC)) were reassigned to INSCOM on 10 April 1992. On 1 October 1995, these two separate entities went away and their functions were merged into the newly created INSCOM National Ground Intelligence Center.

Location: (U/~~FOUO~~) From its creation, NGIC was located in Charlottesville, Virginia. However, on 21 September 2001, the center dedicated the Nicholson Building on 2055 Boulders Road as its new permanent home. (For more about the building see the write-up on the "Nicholson Building" elsewhere in this history.)

Mission: (U/~~FOUO~~) The NGIC produced and disseminated all-source integrated intelligence on foreign ground forces and supporting combat technologies to ensure that US forces had a decisive edge on any battlefield. The NGIC represented a true synthesis of general Military Intelligence (GMI) and scientific and technical intelligence (S&TI)—a one-stop shopping.

Organization: (U/~~FOUO~~) Internally, NGIC consisted of four major elements: The **Forces Directorate** was made up of area and military specialists studying current and future foreign ground forces from the operational level down to the small unit level. These studies were used to help plan scenarios, analyze costs of proposed defense programs, furnish information on foreign adversaries to the Center of Army Analysis, and provide information to the USA Training and Doctrine Command for use in building force structures. Within the **Ground Systems Directorate**, scientists and engineers utilized a variety of unique capabilities (such as the ELINT laboratory, Compton Compact Radar Range, Joint Assessment of Catastrophic Events Model, the Geographical Information Systems, and the Digital Imagery Operations Center, etc.) to evaluate any type of equipment or weapons that might threaten the US Army. The NGIC's Foreign Materiel Program focused on acquiring and exploiting foreign ground systems and helicopters. And finally, there was the **Imagery Assessments Directorate** located at the Washington Navy Yard in the District of Columbia. The directorate produced a wide-range

of imagery intelligence products and served as NGIC's most direct link to the war-fighter. A special strength of the imagery effort was its imagery-based modeling tools, such as the Integrated Assessment of Chemical Production Facilities. On 15 June 2001, the **203d MI Battalion**, which supported NGIC's technical intelligence mission, was inactivated at the Aberdeen Proving Ground, Maryland. In its place was created a Multi-Compo unit using personnel drawn from INSCOM and the Reserves. (See write-up on "Coming of Multi-Compo Units.")

Operational Highlights: ~~(S//NF)~~ Prior to 9/11, imagery support was being provided to warfighters deployed in Kosovo, Bosnia and Kuwait.

(b)(1)

Regraded SECRET on
16 Jan 2014
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

513th MI Brigade

History: (U) The 513th was stood up in 1982 to support the ground component of the US Central Command during contingencies in Southwest Asia. Over the years, the 513th MI Brigade became INSCOM's power projection brigade with potential worldwide focus.

Location: (U) In 1994, the 513th MI Brigade was relocated from Fort Monmouth, New Jersey, to Fort Gordon, Georgia, where it remains along with its 201st, 202d, and 297th MI Battalions. However, the 204th MI Battalion is currently located at Fort Bliss, Texas.

Mission: (U/~~FOUO~~) The 513th MI Brigade conducted theater level multi-discipline intelligence, force protection, counter-drug, electronic warfare, and information operations in support of US Army South, US Army Central Command, and other deploying forces.

Organization: ~~(C)~~ The 513th mission is divided among four battalions: The **201st MI Battalion** at Fort Gordon which was responsible for SIGINT in support of theater army components, and MASINT in support of national requirements. A Company performed SIGINT collection and direction finding and D Company conducted MASINT and manned a Technical Control and Analysis Element (TCAE). (Besides manning the Technical Control and Analysis Elements at Fort Gordon, soldiers of the 201st MI Battalion operated the TCAE (b)(1)(b)(3) Per NSA D and E Detachments and F Company were attached to (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA where they performed similar responsibilities.

~~FOUO~~ ~~(C)~~ (U) The **202d MI Battalion**, also at Fort Gordon, provided counterintelligence and human intelligence in support of theater army components.

(b)(7)(E)

(During FY 2001, the 202d had a company forward in support of the US Army South in Puerto Rico and also maintained a forward presence in Kuwait (Field Office Southwest Asia), Qatar, and Saudi Arabia).)

~~FOUO~~

~~(C)~~ The **204th MI Battalion** served as the Army's only echelon above corps aerial battalion and consisted of highly

sophisticated, multi-sensor aircraft and tactical ground downlink equipment and teams capable of deploying worldwide independently or as part of the 513th. (Presently, the battalion's main effort was directed in support of the counter-drug war efforts of the US Southern Command.)

(b)(7)(E)

~~FOUO~~ (U) ~~(C)~~ Finally, the **297th** at Fort Gordon served as the operations battalion for the 513th MI Brigade.

(b)(7)(E)

(In December 2001, these systems were scheduled to be replaced by the Tactical Exploitation System (TES)). The 297th also supported manning of Intelligence Support Elements at Fort Bragg, North Carolina; Fort Hood, Texas; Fort McPherson, Georgia; Camp Doha, Kuwait; and Eskan Village, Saudi Arabia.

~~(S)~~

(b)(1)

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 66

IAGPA-CSF Form 6-R
1 Sep 93

66th MI Group (Provisional)

HISTORY: (U) The 66th MI Group (Provisional) was established on 16 October 1997 upon the inactivation of the 66th MI Brigade.

LOCATION: (U/~~FOUO~~) In June 1998, the 66th relocated from Augsburg, Germany, to the Dagger Complex and Kelley Barracks in Darmstadt. Besides the Dagger Complex, operations were conducted from Bad Aibling, Stuttgart, Heidelberg, etc. All together, the 66th had elements in six European countries and forward deployed personnel in Kosovo and Macedonia.

MISSION: (U/~~FOUO~~) USAREUR's intelligence requirements covered a wide and complex spectrum of possible missions and operations in or out of the USEUCOM Area of Responsibility that included more than 89 countries and encompassed the entire spectrum of military operations. (b)(7)(E) The 66th was required to provide direct support to USAREUR, Southern Europe Task Force (SETAF) and 21st Theater Support Command (TSC), and to provide reinforcing support to V Corps along with other units within the USAEUR/EUCOM AOR. The 66th also responded to USAINSCOM, national level tasking authorities, and/or service agreements.

ORGANIZATION (C) (~~U/FOUO~~) Internally, the 66th MI Group was divided between the **Directorate of Operations** (responsible for (b)(1) (b)(1) and the **Directorate of Investigations** (oversaw all counterintelligence and human intelligence activities). The 66th MI Group began FY2001 consisting of a Headquarters company, C Company, and an Operations Battalion. It was also assigned (b)(1) (b)(1) C Company and Operations Battalion went away on 16 January 2001 when the **533d MI Battalion (Prov)** was organized in their place. The 533d was further broken down into a Headquarters Company, A Company (Operations), Bravo Company (CI/interrogations), and C Company (b)(1) C Company was located at Bad Aibling in concert with the 108th MI Group/field station. In addition, in theater elements of the 513th were

attached to 66th and performed (b)(1) responsibilities.

OPERATIONAL HIGHLIGHTS: (U/~~FOUO~~) Daily duties of the 66th included preparation of a briefing for intelligence officers at USAREUR and KFOR J2. If required, the 66th provided a large-picture intelligence focus for operational elements through use of its Deployable Intelligence Communications System, a reach-back capability to exploit the data gathered for the European Command, National Authorities, and other operational forces. The 66th also determined threat assessments and provided force protection through the exploitation of human resources. During FY 2001, the 66th assisted in the research of information for personal security clearances.

(b)(7)(E)

108th MI Group

HISTORY: (U) The 108th MI Group was activated on 16 June 2000 to replace the TDA organization, 718th MI Group. During FY 2001, the 108th undertook planning for an uncertain future. See write up elsewhere on closeout.

LOCATION: (U/~~FOUO~~) Bad Aibling Station was located in the town of Mietraching, just outside Bad Aibling, Germany. Its headquarters was located in Building 301. The Operations Compound was housed in Buildings 325, 325A, and 340.

MISSION: ~~(U/~~(b)(1) The 108th had (b)(1) communications security responsibilities. Its primary mission was to (b)(1) (b)(1) that supported the National Command Authority, strategic consumers, and tactical warfighters. The types of operations being supported included combat, peace-keeping/enforcement, humanitarian/disaster relief, non-combat evacuation, show-of-force, search and rescue, and counter-terrorism.

ORGANIZATION: ~~(TS~~(b)(1) The 108th MI Group was divided into four directorates to include the **Directorate of Operations** which was further divided into the (b)(1) (b)(1) (b)(1) the Support Activity provided value added (b)(1) to deployed US forces. (b)(1) (b)(1) (b)(1) Finally, the 108th MI Group commanded the 401st MI Company.

OPERATIONAL HIGHLIGHTS: ~~(TS/~~(b)(1) (b)(1)

109th MI Group

HISTORY: (U) On 16 June 2000, the 109th MI Group was activated to replace the discontinued 713th MI Group, a TDA counterpart.

LOCATION: (U/~~FOUO~~) Menwith Hill Station is located near Harrogate, England. Elements of the group were also located at Molesworth and Digby.

ORGANIZATION: (U/~~FOUO~~) The 109th MI Group over saw a Headquarters Detachment, the Molesworth Element, the Digby Element, and the 404th MI Company.

OPERATIONAL HIGHLIGHTS: (~~TS~~/(b)(1)) Menwith Hill continued to provide timely intelligence to force protection efforts in support of Operations NORTHERN WATCH and SOUTHERN WATCH and in Kosovo. The Menwith Hill Station (b)(1)

(b)(1)

902d MI Group

HISTORY: (U) The 902d MI Group had been assigned to INSCOM since 1977. However, through the years it underwent a series of reorganizations that left it in sole control of INSCOM's counterintelligence mission. In 1996, the Foreign Counterintelligence Activity was assigned, and the 308th and 310th MI Battalions activated as replacements for TDA counterparts.

LOCATION: (U/~~FOUO~~) The 902d MI Group Headquarters and subordinate Battalion/Activity Headquarters were all located at Fort George G. Meade, Maryland. In addition, the 902d MI Group had Company Headquarters, Detachments, and Resident and Field Offices in 27 other CONUS/OCONUS locations.

MISSION: (U/~~FOUO~~) The 902d MI Group conducted multidiscipline counterintelligence operations throughout CONUS and designated worldwide locations to detect, neutralize, defeat, and exploit the threat to US Army forces, secrets, and technologies, with emphasis on countering Foreign Intelligence Services. During contingencies, the 902d MI Group reinforced designated units with tactically tailored CI deployment packages or individual augmentation in support of Theater Commanders during peacetime, Security and Stability Operations, and major regional conflicts.

ORGANIZATION: (C)

(b)(1)

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 72-73

704th MI Brigade

HISTORY: (U) The brigade's origins can be traced back to 1954 and the move of the National Security Agency from Arlington Hall Station, Virginia, to Fort George G. Meade, Maryland. Through the years, the brigade continued to command personnel and units whose missions were to support NSA.

LOCATION: (U) ~~(S)~~ The 704th MI Brigade, its Headquarters Company, and the 741st and 742d MI Battalions were all located at Fort Meade, Maryland. (The Command Group of the 704th was located in Building 9805; the 741st was in 9828; and the 742d Battalion in 9802.) However, the 742d had a detachment in Utah working alongside the 300th MI Brigade (Utah National Guard); the 743d MI Battalion was headquartered in Building 1219, Fort Carson, Colorado, but also had detachments at various CONUS and OCONUS sites (including Winter Harbor, Diego Garcia, and CSGAS).

MISSION: ~~(TS//SI//TK)~~ The Brigade supported warfighters and national decision-makers' information superiority requirements through the conduct of Signals Intelligence, Information Security, and Information Operations both directly and through support to the National Security Agency. The mission of the **741st** was to conduct SIGINT operations (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA as well as provided support to NSA's various operational groups. The **742d** was to conduct operations in support of Army requirements, in support of NSA operations, provide technical SIGINT support to FORSCOM, and to exercise operational control of the 300th MI Brigade (National Guard). Finally, the focus of the **743d** was on worldwide SIGINT missions in support of strategic commanders and indirectly to operational and tactical commanders and facilitated the planning and execution of the Army Space Command.

ORGANIZATION (U) ~~(C)~~ The Brigade's Headquarters Company included senior Army personnel assigned to joint duty positions within the US Army Element of the National Security Agency. (The US Army Element remained a separate TDA organization on paper only.) Personnel assigned to the 741st MI Battalion were almost all employed within the Operations Directorate, NSA. The 742d MI Battalion operated the Army Technical Control and Analysis Element furnished soldiers to NSA support groups. The finally, the 743d MI Battalion as indicated above supported strategic commanders.

OPERATIONAL HIGHLIGHTS: (~~TS~~) A 704th soldier assigned to the Office of International Organized Crime Branch led a team

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA Members of the 704th also participated in an important brief (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA The discussions centered

(b)(1)(b)(3) Per NSA

116th MI Group

HISTORY: (U) On 16 June 2000, the 116th MI Group was activated replacing the 702d MI Group as part of a command-wide effort to present a TOE face.

LOCATION: (U/~~FOUO~~) The 116th Group remained located at Fort Gordon, Georgia, where it oversaw the Gordon Regional Security Operations Center. The 206th MI Battalion was collocated with its parent unit at Fort Gordon. In direct support to the Medina Regional Security Operations Center (MRSOC), the 314th MI Battalion was located at Lackland Air Force Base, San Antonio, Texas.

MISSION: (U/~~FOUO~~) As host unit, the 116th MI Group provided personnel and support to the Gordon RSOC and integrates Reserve Component soldiers into the center's operations. The 314th MI Battalion served as the Army component of the Medina RSOC where the battalion provided SIGINT information to satisfy warfighting and national level intelligence requirements.

ORGANIZATION: (U/~~FOUO~~) The 116th MI Group controlled the 206th MI Battalion and the 314th MI Battalion. The **206th Battalion** was broken down into a Headquarters and Headquarters Company, A Company, and E Detachment. (b)(7)(E) The **314th MI Battalion** had three companies and a detachment: Headquarters and Headquarters Company, A Company, B Company, and D Detachment. Mirroring its sister battalion, the 314th MI Battalion's A and B Companies consisted of linguists and analysts assigned to the MROC, and D Detachment served as the Medina RTCAE.

OPERATIONAL HIGHLIGHTS: (S) The 314th MI Battalion expended much of its energy preparing for (b)(1)(b)(3) Per NSA transfer from (b)(1)(b)(3) Per NSA to the MRSOC. An Integrated Military Operations Division within the J31 to coordinate the transfer. Following 9/11, the GRSOC and MRSOC, in coordination with NSA's Office of Regional Targets, were given new target responsibilities. (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA As a force provider to both the GRSOC and MRSOC, the 116th MI Group remained the center of gravity of NSA/CSS support to CENTCOM and EUCOM for the Middle East. As the host for GRSOC, the 116th was given the added task of re-configuring the GRSOC's infrastructure and support systems.

115th MI Group

HISTORY: (U) The 115th MI Group was activated on 16 June 2000 to replace the 703d MI Brigade as part of a larger effort of INSCOM to offer a TOE face.

LOCATION: (U/~~FOUO~~) The 115th MI Group occupied two principal locations on the island of Oahu, Hawaii. Operations were conducted at the Kunia Tunnel, bordering Schofield Barracks. The group's headquarters was in Building 130 on Schofield Barracks, and its subordinate battalion headquarters was in Building 131.

MISSION (U) ~~(C)~~ The 115th Military Intelligence Group, as the Army component of the jointly staffed Kunia Regional Security Operations Center (KRSOC), conducted joint signals intelligence operations responsive to warfighter and national requirements and deployed individuals to reinforce forward-based units. The group provided approximately one-third of the KRSOC Operations Directorate operations, management, training, and plans staffs. Additionally, the 115th provided administrative support to soldiers assigned to the 205th MI Battalion (500th MI Group) who operated the Regional Technical Control and Analysis Element at Kunia.

ORGANIZATION: (U/~~FOUO~~) Besides its Headquarters and Headquarters, Detachment, the 115th MI Group controlled the **406th, 407th, 408th,** and **409th MI Companies.** (To oversee these companies, the group created a provisional battalion (**732d MI Battalion**) using personnel from its Headquarters Detachment.)

OPERATIONAL HIGHLIGHTS: (~~TS~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

USAINSCOM Land Information Warfare Activity

HISTORY: (U/~~FOUO~~) LIWA's roots dates back to 1995 when an element was established at HQ INSCOM to participate in the information operations/warfare arena.

(b)(7)(E)

LOCATION: ~~(FOUO)~~

(b)(7)(E)

However, key support elements are scattered throughout CONUS and are in Korea, Germany, and Hawaii.

MISSION: ~~(FOUO)~~

(b)(7)(E)

coordinates and synchronizes support from INSCOM, Army, and other Services, the Joint IO community, and other Government activities. It projects capabilities around the world to provide offensive and defensive IO operational, planning, and training support to land component commanders.

ORGANIZATION: (~~TS~~) The Information Dominance Center was a congregation of powerful search and analytical tools,

(b)(1)

(b)(1)(b)(3) Per NSA

On 3 August 01, the National Security Agency assigned the SIGINT Designator [redacted] to the IDC. (This was a part of General Alexander's vision of offering "one-stop intelligence and information operations shopping.") The change in operations also led to organizational changes. Although no formal permanent orders were published, on paper, the IDC was established as a separate entity under the CG, INSCOM, and the commander of LIWA also wore the hat of Commander, IDC. Underneath of the IDC were the Intelligence Operations Center (from the G-3, HQ INSCOM), the LIWA, Futures Center, and Cyber

Warfare Center (CWC). The LIWA itself was divided between a Director of Support and a Director of Operations.

OPERATIONAL HIGHLIGHTS: ~~(FOUO)~~ At the end of the year, LIWA had an authorized/actual strength as follows: officers 62/37, warrant officers 10-16, enlisted 53/47, and DA civilians 85/76 for a total of 210/176. Based on its FY 04-09 Program Objective Memorandum (POM) submission, LIWA submitted requirements for 70 officers, 25 warrant officers, 115 enlisted, 167 civilian, and 234 contractor-equivalents.

~~(FOUO)~~

(b)(7)(E)

Complete graphical topology diagrams were supplied by node, base camp, and layer 2/3 device. This was the first such product produced for the SFOR and was viewed as invaluable to improving the overall security and administration of the theater networks.

~~(FOUO)~~ Do-It-Yourself Vulnerability Assessment Program (DITYVAP) became a major thrust for the year. Training personnel to carry out this mission was an ongoing mission. This included training Regional Computer Emergency Response Team (RCERT) personnel to conduct the training and training Active, Reserve, and National Guard personnel. At the close of FY 01, 187 personnel had completed mandatory Information Systems Security Monitoring (ISSM) training: 198 have completed level-1 scanning training; 45 have completed analysis level-2 training; and 9 completed level-3 supervisory training.

500th MI Group

History: (U) The 500th MI Group has been in existence, except for one brief period, from 1952, and thus has earned the title of the "Pacific Vanguard."

Location: (U) The headquarters of the 500th MI Group continued to be located at Camp Zama, Japan, with major subordinate detachments at Misawa Air Base, Yokota Air Base, Kure, Tokyo, and Yokohama, and Okinawa, Japan; Fort Shafter, Hawaii; Republic of Marshall Islands; Alaska; and Fort Lewis, Washington. (Many of these were forward-deployed CI detachments.)

Mission: (U) The 500th MI Group provided intelligence support to US Army, Pacific and engaged Asia-Pacific intelligence and security institutions in order to contribute to regional stability and crisis response. As directed, provided support to joint and national agencies.

Organization: ~~(C)~~ The 500th MI Group oversaw (b)(1) (b)(1) the 403d MI Detachment (b)(1) and the 205th MI Battalion (b)(1) In addition, there were three smaller elements: The Security Liaison Detachment, the COMTECH Detachment, and the Counter Intelligence Detachment Japan.

Operational Highlights. ~~(S/NF)~~ In March 2001, the 205th deployed a small CI team (b)(1) to provide intelligence support to force protection for an engineer platoon building a hospital. (b)(1)

(b)(1)

501st MI Brigade

History: (U) Its entire existence has been in providing intelligence and security support to US forces in Korea: First, as part of the Army Security Agency during the Korean War. Secondly, since being activated in 1978, the 501st became a part of the newly created US Army Intelligence and Security Command.

Location: ~~(POUO)~~ The 501st MI Brigade along with a number of its elements were located at Sobingo Compound, outside of the US Yongsan Military Reservation, Seoul, Republic of Korea. The same for the 532d MI Battalion. The 3d MI Battalion was at Camp Humphreys, Pyongtaek; the 524th MI Battalion at Zoeckler Station, Camp Humphreys; and the 517th MI Battalion also at Zoeckler Station.

Mission:

Organization: The 501st MI Brigade

Operational Highlights:

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

REPLY TO
ATTENTION OF:

Freedom of Information/
Privacy Office

24 JUN 2014

This is in further response to your Freedom of Information Act (FOIA) request of August 18, 2007, for a copy of the INSCOM Annual History for FY2002 and supplements our letter of October 10, 2012.

Coordination has been completed with other elements of this command and other government agencies. The records have been returned to this office for our review and direct response to you.

We have completed a mandatory declassification review in accordance with Executive Order (EO) 13526. As a result of our review information has been sanitized and four pages are being withheld in their entirety as the information is currently and properly classified TOP SECRET, SECRET and CONFIDENTIAL according to Sections 1.2(a)(1), 1.2(a)(2), 1.2(a)(3) and 1.4(c) of EO 13526. This information is exempt from the public disclosure provisions of the PA as provided unter Title 5 U.S. Code 552 (k)(1) and of the FOIA pursuant to Title 5 U.S. Code 552 (b)(1). It is not possible to reasonably segregate meaningful portions of the withheld pages for release. A brief explanation of the applicable sections follows:

Section 1.2(a)(1) of EO 13526, provides that information shall be classified TOP SECRET if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

Section 1.2(a)(2) of EO 13526, provides that information shall be classified SECRET if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

Section 1.2(a)(3) of EO 13526, provides that information shall be classified CONFIDENTIAL if its unauthorized disclosure reasonably could be expected to cause damage to the national security.

Section 1.4(c) of EO 13526, provides that information pertaining to intelligence activities, intelligence sources or methods, and cryptologic information shall be considered for classification protection.

In addition, information has been withheld that would result in an unwarranted invasion of the privacy rights of the individuals concerned, this information is exempt from the public disclosure provisions of the FOIA per Title 5 U.S. Code 552 (b)(6).

Additionally, information has been sanitized from the records as the release of the information would reveal sensitive intelligence methods. This information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(7)(E) of the FOIA. The significant and legitimate governmental purpose to be served by withholding is that a viable and effective intelligence investigative capability is dependent upon protection of sensitive investigative methodologies.

The withholding of the information described above is a total denial of your request. This denial is made on behalf of Major General George J. Franz III, Commanding, U.S. Army Intelligence and Security Command, who is the Initial Denial Authority for Army intelligence investigative and security records under the Freedom of Information Act and may be appealed to the Secretary of the Army. If you decide to appeal at this time, your appeal must be post marked no later than 60 calendar days from the date of our letter. After the 60-day period, the case may be considered closed; however, such closure does not preclude you from filing litigation in the courts. You should state the basis for your disagreement with the response and you should provide justification for reconsideration of the denial. An appeal may not serve as a request for additional or new information. An appeal may only address information denied in this response. Your appeal is to be made to this office to the below listed address for forwarding, as appropriate, to the Secretary of the Army, Office of the General Counsel.

Commander
U.S. Army Intelligence and Security Command
Freedom of Information/Privacy Office (APPEAL)
4552 Pike Road
Fort George G. Meade, Maryland 20755-5995

Additionally, we have been informed by the National Security Agency (NSA) that portions of their information has been sanitized from the records pursuant to the exemptions listed below:

5 U.S. Code 552(b)(1) – The information is properly classified in accordance with the criteria for classification in Section 1.4 of Executive Order 13526.

5 U.S. Code 552 (b)(2)

5 U.S. Code 552(b)(3) – The specific statutes are listed below:

50 U.S. Code 402 note (Public Law 86-26 Section 6)
50 U.S. Code 403-1(i)
18 U.S. Code 798

The initial denial authority for NSA information is the Director Associate Director for Policy and Records. Any person denied access to information may file an appeal to the NSA/CSS FOIA/PA Appeal Authority. The appeal must be postmarked no later than 60 calendar days of the date of the initial denial. The appeal shall be in writing to the NSA/CSS FOIA/PA Appeal Authority (DJP4), National Security Agency, 9800 Savage Mill Road, STE 6248, Fort George G. Meade, Maryland 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the

ANNUAL COMMAND HISTORY

US ARMY INTELLIGENCE AND SECURITY COMMAND

FISCAL YEAR 2002

History Office
of the
Strategic Management and Information Office
Nolan Building
8825 Beulah Street
Fort Belvoir, Virginia 22060-5246

30 September 2003

TABLE OF CONTENTS

Page

OVERVIEW

The INSCOM historians conducted an interview with MG Keith B. Alexander, Commanding General, US Army Intelligence and Security Command. MG Alexander's comments provide an overview of INSCOM from the Commander's perspective.

What guidance did you receive at the beginning of your tour? Were you charged with accomplishing specific objectives?

(U//FOUO) MG Alexander: I wasn't given anything other than the Chief's guidance on counterterrorism. I had the fortuitous opportunity to meet with the Chief on the week before I took command, and I was, at that time, the J2 CENTCOM. We were going over the USS *Cole* results and making INSCOM function according to some of the counterterrorism requirements. His comment was, "Your number one priority is to support the war on terrorism." That was a stated requirement. That spawned, in my mind, a number of unstated requirements. The reason I bring this up is that it laid the path for almost everything else we did by making INSCOM an operational headquarters. How are you focused on the war on terrorism if you are not actively taking your national and theater assets and applying them to the theater assets? How do you do all the things we are doing in the Information Dominance Center (IDC)? The evolution of the INSCOM staff had to change once again to become both an admin headquarters to do personnel, logistics, and resources and an operational headquarters to integrate our component commands.

Describe your personal philosophy of leadership, command, and management.

(U//FOUO) MG Alexander: I am a great believer in the capabilities of our people. I am the eternal optimist. They can do anything you put in front of them and our biggest short fall is that we don't ask them to do the right things or go far enough. I think we have a tremendous Army and a tremendous intelligence community. But if we don't take risks to go out further, we will be where we were 20 years ago. Part of my philosophy is that we have great people and the other part of it is to ask how far out into the future can we reach from where we are today. Can we make the future happen now? Those two things are the most important aspects of my philosophy and then I have some trite sayings to go along with it: "Our ideas, their money" etc. We have a series of those that we joke about but when observers see the accomplishments down stairs and in our mini-IDCs around the world, they are amazed at how fast it has happened. It is a tribute to how good our people are.

What was the greatest challenge you faced in this position?

(U//FOUO) MG Alexander: Working with the agencies to get information that the intel community should share freely. The biggest problems that impact our command and its ability to do its mission are bureaucratic obstacles in regard to what is prescribed as law but is actually policy. That was and remains the biggest hurdle that we have. As a consequence, we fight with the agencies to do what we think is right. In this regard, I

think we are out in front. We are doing more with information than they are and that puts them in an uncomfortable position of trying to catch up. It also puts us in the position of getting more cheap shots. Most of that is over policy. What information can you have? What information should you have? And who controls the amount of information you get. I think the intelligence community has a lot to learn in that area. We (the intelligence community) don't do it right. What we (the intelligence community) do in part prevents better analysis. We have pushed hard in that area. That remains our biggest obstacle. A lot of people say that "We don't have the resources." But I will tell you that the Army has been great in resourcing INSCOM in both people and resources. They see the value of what we do for the global war on terrorism, the counter-drug campaign, and support against regional threats. It's been superb.

What is your evaluation of the strengths and weaknesses of your subordinates? What measures did you take to correct observed deficiencies?

(U//FOUO) MG Alexander: I think the biggest problem is how to train people on the new tools. We have a very deliberate training process to get our guys to one level. In the Intelligence Community we have another set of problems. They learn their basic skills pretty well. But the communications environment is changing rapidly so that the new skills required to handle it require an individual who can adapt and train himself on programs very quickly. That's something we must learn how to do. As an example, STARLIGHT is a great program for doing analysis. It takes a lot of work to get trained on it. There are no Army courses on STARLIGHT; so people, whether they are officers, warrants, or enlisted, have to train themselves or we have to create training programs, which we are doing. We set up these programs to train, say 400 people, but that's the biggest problem, as I look at it, how do you create a force that can train themselves after you've brought them out of school. For the Intelligence Community and the Signal Community that is something we have to get to. In terms of deficiencies, when I look at our soldiers, I have not noticed deficiencies in their basic skills. It's been more in their advanced skills. If I were to really look at it, how do you take them from the basic skills and jump out?

Did you make major changes in the organizational structure of your organization? Why?

(U//FOUO) MG Alexander: Yes, we changed the functions of the headquarters from administrative to administrative/operational by setting up the Information Dominance Center, the Intelligence Operations Center (IOC), and moving slots and spaces to meet the counterterrorism requirements that were tasked to us by the Chief. That is how we started to synchronize the functions of the brigades with the analysis that's going on and how we did that globally.

Describe the efforts undertaken by your organization to promote the "Total Army" concept.

(U//FOUO) MG Alexander: In our organization, more so than in other Army units, we depend on the reserves for much of what we do. Since 11 of September we have had over 1,000 reserves activated at any one time. So we, just to do our daily jobs, both here and throughout the command, depend on that total army as one, and I think we have benefited from it and the reserve units have benefited from it.

There was a first too with the multicompo units?

(U//FOUO) MG Alexander: Right. Several of our units or intel (intelligence) brigades, including the 513th, are multicompo, which means that they have members from the reserve and when we go to war or go to a crisis, we have to activate them to do our mission. The same is true of the first Information Operations Command. When we get up to a certain ops tempo our commands can't function without reserve support. That's good and bad. The good part is that it requires that close working relationship. The bad part is that long, drawn-out campaigns, such as Enduring Freedom and Iraqi Freedom, have required continuous mobilization of some of our units for two years.

CHAPTER ONE

MISSION AND ORGANIZATION

Closure of Bad Aibling (~~TS~~/(b)(1)) At the close of FY 2001, the 108th MI Group was on the road to inactivation at Bad Aibling, Germany. (The 108th controlled one battalion size element (the 109th MI Group (Provisional) at Menwith Hill Station, England, and the 401st MI Company. The Army personnel at Bad Aibling were assigned to 401st MI Company.) After 9/11, Congress issued an official announcement postponing the closure of Bad Aibling. This halt in closure activities allowed the 108th MI Group to step up its unique contributions to the global war on terrorism. However, the departure of personnel without replacements plus warnings (b)(1) (b)(1) not to proceed on closure activities made for an interesting, if not stressful atmosphere. During the course of the year (b)(1) (b)(1) the (b)(1) to transition to Menwith Hill Station; and the station's population declined rapidly with the loss of the Air Force Detachment and the majority of the Naval Security Group (in July 2002) as tenants. (The Navy left a small contingent behind to continue ICEBOX operations.) In FY 2002, the group continued with a make-shift security force, consisting of local national police, military units, and National Guard elements. Teams from G3, HQ INSCOM also traveled to Darmstadt, Bad Aibling, and Heidelberg to check out possible sites for (b)(1) if one should come about. (USAREUR contemplated taking over base operations if it was decided that a future European Security Center should be establish at Bad Aibling. (b)(1) was planning on Bad Aibling to close by the end of FY 04.)

G3, Operations and Intelligence Directorate (U//~~FOUO~~) On 17 June 2002, the G3 created the Operations and Intelligence Directorate. It was formed from elements of the Force Readiness, Plans, the Global Command and Control System (GCCS), Theater Support Officers, and the front office.

Intelligence Operations Center (IOC) (U//~~FOUO~~) The IOC became operational on 12 September 01 in accordance with the Counterterrorism I&W/Threat Mapping Initiative. The IOC synchronized the intelligence operations of all INSCOM elements to ensure multi-discipline intelligence support focused on counterterrorism, counterintelligence, counternarcotics, and information operations to theater/component warfighters, the intelligence community, law enforcement and other national-level agencies. The IOC's functions included SIGINT metadata analysis and reporting, all-source fusion analysis, and information mediation management. Included within the IOC were the SIGINT Technical Development Activity (STDA), the Fusion Branch, and the Synchronization Cell.

(U//~~FOUO~~) The IOC developed and implemented the INSCOM portal to facilitate all-source information sharing and horizontal fusion with Major Subordinate Commands in direct support of Combatant Commands and the national-level intelligence community. Additional resources were used to extend the effort by creating Information

Dominance Centers at the Major Subordinate Commands. The centers' purpose was to facilitate all-source analyst to analyst real time collaboration between the INSCOM IOC and key INSCOM nodes in support of the Combatant Commands. Specifically, the IOC provided critical intelligence support in the war on terrorism to multiple entities including the National Ground Intelligence Center, the Combatant Commanders, the Joint Intelligence Task Force-Counterterrorism (JITF-CT), Joint Special Operations Command (JSOC), NSA (Counterterrorism Office of Primary Interest) and the Criminal Investigative Task Force (CITF) utilizing all source data. The IOC provided a specialized analysis capability utilizing advanced state of the art mapping and visualization tools. These reduced processing time and provided analysis that otherwise would not have been available. It allowed comparisons of all-source products with the single source data bases to validate and improve the all-source solution. Also, the IOC included open source and imagery analysis and intelligence fusion and technical support that permitted the introduction of the most advance analytical technologies.

~~(TS//SI)~~

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Activation of the 470th MI Group (U//~~FOUO~~) The 470th MI Group (Provisional) was organized on 1 April 2002 at Fort Buchanan, Puerto Rico. Manned by forward deployed elements of the 513th MI Brigade, the new group was created to provide theater intelligence to the Commander, US Army South. (Plans called for the formal activation of the 470th on 16 October 2002 with 88 authorized spaces.) These steps were to enable HQ INSCOM to meet the requirements of the area of operations and alleviate the 513th MI Brigade resources to support ENDURING FREEDOM in Southwest Asia. Plans also called for the G2, US Army South to be dual hated as the Commander, 470th MI Group, and when the USARSO is relocated from Puerto Rico to San Antonio, Texas, in FY 2003, the 470th is to follow suit.

(b)(7)(E) (U//~~FOUO~~) (b)(7)(E)

(b)(7)(E)

(b)(7)(E) During FY 02, the mission of conducting operations throughout the computer network operations was added.

(U//~~FOUO~~) Organizational elements were located at the following sites: Headquarters LIWA and most of its operational and support elements at the Nolan

Building, Fort Belvoir; the Field Support Division in Alexandria; Regional Computer Emergency Reponses Team (RCERT)-CONUS at Fort Huachuca, Arizona; RCERT-Pacific at Fort Shafter, Hawaii; RCERT-Europe at Mannheim, Germany; RCERT-Korea at Taegu, Republic of Korea, RCERT-South at Fort Gordon Georgia; the Army Reprogramming Analysis Team – Threat Analysis (ARAT-TA) at the Air Warfare Center, Elgin AFB, Florida and the Air Force Information Warfare Center (AFIWC), Lackland AFB, Texas; (b)(7)(E) Liaison Office at the Deputy Chief of Staff, G3, Pentagon; (b)(7)(E) Element at the IO Technology Center, Fort Meade, Maryland; and the (b)(7)(E) Exercise and Training Integration Center (ETIC) at the TRACOC Combined Arms Center (CAC), Fort Leavenworth Kansas.

(b)(7)(E) (U//FOUO) In addition to operations in direct support of the global war on terrorism, the [redacted] executed operational missions in support of the Balkans (SFOR and KFOR) as well as CONUS and OCONUS exercises and Army transformation initiatives. To help absorb the OPTEMP, (b)(7)(E) requested and HQDA validated the mobilization of our reserve component organizations, two from USAR – the Information Warfare Enhancement Center (IWEC) and the 3431st MI Detachment (MID) and two from the ARNG – the Texas and Washington field support teams. Army Reserve soldiers were assigned as individuals into (b)(7)(E) divisions based primarily on civilian acquired skills, while the National Guard teams maintained unit integrity and were assigned to the Field Support Division.

CHAPTER TWO

PERSONNEL, SECURITY, LOGISTICS, ETC.

Transfer of POW Records (U) The Investigative Records Repository assigned to the 902d MI Group at Fort Meade continued to transfer permanent records to the National Archives and Records Administration (NARA). During FY 02, 16 Korean War and 2 Vietnam War POW dossiers were reviewed and transferred. On 9 March 1999, the President approved the DA File Series exemption for EO 12958. This exemption protected most of the repository's records from automatic declassification on 17 April 2000. The only records not covered under this exemption were the POW dossiers.

Nazi War Crimes Disclosure Act (U) The 902d MI Group and its 310th MI Battalion continued to place a high priority on re-scanning, manually separating, and indexing 1,600 reels of microfilm records covered under the act. During FY 02, 3,300 electronic dossiers and 7 hard-copy dossiers were transferred to NARA, and on 30 September, the remainder of the microfilm collection (20 cabinets) was also provided.

Military Fill following 9/11 (U) Following 9/11, INSCOM requested increased military in fill for 9 of its major subordinate commands. This was believed essential in dealing with the counterterrorism crisis. However, the Army only provided increase in fill for one MSC (513th MI Brigade). At the close of the year, the 513th MI Brigade possessed 96 percent authorization.

Long-Term Requisition Problem (U) INSCOM has had a long-term problem, constantly being behind the requisitioning cycle because of the lack of timely authorization documentation. For example, the 108th MI Group was scheduled for closure at the end of FY 02 but no final decision had been made. This puts a strain on all units to help fill these critical MOS shortages.

Reserve Component Mobilization (U) In response to the 9/11 crisis, approximately 1,000 Reserve soldiers were mobilized to support INSCOM.

Equal Opportunity Complaints (U) There were three formal EO complaints during the year; one involved racial discrimination and the others sexual harassment. All complaints were unsubstantiated.

Retention Statistics (U) The following retention statistics are by objective/ accomplished:

Initial Term	Mid-Career	Career	FY02 ETS	Reserve Component
243/328	323/325	119/151	219/219	93/93

G1 AHR, Vol 1 Chpt 7 (U)

INSCOM Insight (U) At the end of FY 01, the Public Affairs Office created an in-house news publication distributed via the web nicknamed the *INSCOM Insight*.

Army Attaché Management (U) As of FY 02, there were 52 warrant officer billets: 45 OCONUS billets in 44 Defense Attaché Offices (DAO) and 7 CONUS billets. There were 100 NCO billets in 88 DAOs.

MICECP Recruitment (U) In FY 02, 57 additional MICECP (Military Intelligence Civilian Exceptional Career Programs) positions were created in the Joint Military Intelligence Program, bringing the total number of authorized MICECPs to 360. This represented a 19 percent increase over FY 01. At the end of FY 02, there were 296 personnel actually assigned, an 83 percent fill. Diversity was reflected in the recruitment pool, which was made up of a disproportionate number of non-diversity candidates: 58 percent (Caucasian); 14 percent (Black); 12 percent (Hispanic); 6 percent (Asian); and 24 percent (female).

(b)(7)(E)

Readiness of Units (U/FOUO) The INSCOM IG inspected the command's units and found a variety of issues impacting upon readiness. One unit believed that soldiers straight from advance individual training as opposed from having first been assigned to a tactical unit was a readiness issue. In another, soldiers with low-density military occupation specialty without clearances impacted upon both the length of tour and the unit's readiness. Manning documents prescribing a higher level than what the unit believed necessary was also an issue. Taskings from higher headquarters with short-turn around suspenses were also a factor. However, the IG did pick up on one common theme—requirement's documents for unit manning. Overall, despite these challenges, there was a high OPTEMPO.

(S/COMINT)

(b)(1)

released and at what point. NSA types continued to monitor the activities

(b)(3):P.L. 86-36

(b)(7)(E)

DOD Force Protection Detachment Program. (U//FOUO) In February 2002, representatives of the Intelligence Materiel Activity met with DOD officials to discuss support to the a new DOD Force Protection Detachment program. DOD, through the various services, was establishing small FPDs in embassies throughout the world in order to assist US government personnel transiting foreign countries. Although the logistics were complicated, the IMA agreed to purchase, store, and ship mission equipment and vehicles for use by Army sponsored FPDs. Its success led the Navy and Air Force to request and receive similar support.

(b)(1),(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 40

(S (b)(1),(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36 remained operational. In March 2002, the system was temporarily shut down pending redeployment to CONUS.

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Afterwards, the power supply and generators were replaced and extensive effort made to upgrade site security (b)(2),(b)(3):P.L. 86-36 The new mission was to be known as

(b) (1) Per NSA, (b)(3):18 U.S.C. 798,(b)(3):50 U

(b)(1)

TS-CCO) (b)(1) continued to play a vital role in INSCOM mission around the world. To date, there were 1307 pieces of equipment (b)(1) Among the equipment there are

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

In all, (b)(1) oversaw the receipt and issue of more than 100 (b)(1) transactions consisting of more than 350 warehouse items. (MASINT remained the most active consumer.) This year, 157 pieces were removed for destruction.

(b)(7)(E) (U//FOUO) (b)(7)(E)
(b)(7)(E)
(b)(7)(E) However,
obsolescence issues have raised system repair costs to over $600,000 in unexpected repair costs for FY 02. Over the year discussions were held on proposals to upgrade the system for remote operations and on means of obtaining additional funding to support needed upgrades.

CHAPTER THREE

INFORMATION AND SYSTEMS

Army Knowledge Management (U) The Army Knowledge Management effort, begun in late FY 01, became a central effort during FY 02. Sponsored by the Army Chief Information Officer/G6, it sought to transform the Army into a knowledge-centric organization and directly affected core competencies for INSCOM. By the end of 2d Qtr, FY 02, INSCOM had registered 93 percent of its users. A potentially significant fallout from the AKM plan was the Army Centralized Installation Management initiative. This effort realigned MACOM resources into new regional installation commands, and initially ten IT personnel slots at the National Ground Intelligence Center were slated for reassignment. HQ INSCOM was successful in reversing the decision. (Later, INSCOM agreed that two IT billets in G6 would be transferred to NETCOM as the INSCOM "fair share," but nothing more.)

IT Registry (U) INSCOM had an overwhelming majority of systems defined as application databases in the DOD IT Registry. In the past, this cause confusion as AAA had desired to review the security accreditations for some of the INSCOM "systems" on the list. Following discussions, INSCOM decided on 7 March to delete all its applications from Register.

Asset Tracking (U) At the end of the fiscal year, 13.5 percent of INSCOM's PCs had processing speeds below 266 MHz, with 63 percent above 450 MHz and the remainder falling between the two. This represented tremendous progress over the year. INSCOM began with 39.6 percent under 266 MHz and 33.6 over 450 MHz and the rest in between.

Migrate to SIRRNET (U) HQ INSCOM began the process on 7 November 2001 to migrate C2 business functions from the Thor network (NSANET) to Frey (SIPRNET).

Networks (U/~~FOUO~~) HQ INSCOM operated four local and wide area networks providing connectivity to NIPRNET (VULCAN), SIPRNET (FREY), JWICS (IDUN), and NSANET (THOR) backbones. Significant progress was made using Microsoft's Systems Management Server (SMS) to provide accurate automation inventory data and to push software versions and upgrades to the desktop. The life cycle replacement program to replace the older CPUs in HQ INSCOM was continued. There was also an upgrade of network switches from Optical Data Systems to Cisco GIGABIT. SIPRNET, JWICS, and NSANET were completed, and work was begun on the NIPRNET. The Defense Messaging System (DMS) was initially implemented.

CHAPTER FOUR

OPERATIONS

XIX Olympic Winter Games. (U) The XIX Olympic Winter Games in Salt Lake City, Utah from 8-24 February 2002 was the most significant world-sporting event of the year. The increased global terrorism threat to DOD and US interests since 11 September 2001 was significant with intelligence reports suggesting that follow-on attacks were expected. Salt Lake City hosted approximately 3,500 athletes from 80 different nations in 70 medal events at 10 different competition venues, which presented a high-value target to both Foreign Terrorist Organizations (FTO) and domestic extremist groups. In accordance with OLYMPIC VIGILANCE, C Company, 902d MI Group was there to respond to any incident affecting the force protection of the Army Service Component Command, Joint Task Force—Olympics. The primary focuses of attention were the foreign HUMINT and FTO threat to the US Army and US military programs from visitors to the Olympics. Through official liaison with local and federal law enforcement and intelligence agencies and supported US Army activities, C Company assets gathered and passed time-sensitive threat information to affected US Army activities, which they used to monitor and track indicators of possible FTO targeting. This allowed decision-makers to assess the security environment and force protection measures.

Increased SAEDA Reporting. (U) Company A, 308th MI Battalion reported a 145 percent increase in initial SAEDA reporting, going from 83 in FY 00 to 221 in FY 03. The same held true for the Intelligence Information Reporting which went from 148 to 529 over the same time period. (Of the 529 reports received, 452 were published.)

(S//NF) (b)(1)

US Army Counterintelligence Center (ACIC) and the Counterintelligence (CI) Analysis Control Element (ACE). (U) The 902d was the primary strategic counterintelligence asset within the US Army (b)(7)(E) (b)(7)(E) Personnel of the 902d were located across CONUS and forward-deployed to three theaters. (b)(7)(E) (b)(7)(E) (b)(7)(E) Although the ACIC was always involved in homeland defense type issues, the attack of 9/11 refocused its priorities and how it did business. ACIC analysis focused on four basic functional areas: technology protection, force protection, information operations, and support to CI

investigations and operations. Work performed by ACIC is managed under the DOD Intelligence Production Program.

(C)

(b)(1)

(S/NF)

(b)(1)

(U) The 902d opened the new Counterintelligence (CI) Analysis Control Element (ACE). (Limited operations were begun in November 2001 while new facilities were constructed). The new CI ACE was designed to permit the 902d to provide a counterintelligence threat picture to the Information Dominance Center at HQ INSCOM and synchronize counterintelligence support to Army organizations throughout CONUS

(b)(7)(E)

(b)(7)(E) In July 2002 the CI ACE was renamed the Counterintelligence Integrated Analysis Center (CIIAC) and integrated into the ACIC.

(U) Together, the ACIC, CIOC, and CIIAC developed daily threat assessments that they fuse and forward to the Information Dominance Center. The ACIC provided the CIIAC with analytic advice and assistance, and augmented the CIIAC with analysts. The emphasis of the CI ACE remained the "Big Picture" in support of the Army, both the CIIAC and ACIC were joined in addressing the gaps in CT and FP. Palaganas, MAJ Arthur F. "The 902d MI Group's CI ACE" and Harlin, Charles "US Army Counterintelligence Center Support to Homeland Security,"

(S//NF)

(b)(1)

TEMPEST (U) In support of the DOD TEMPEST Proficiency Certification Program, the 310th MI Battalion supported 160 missions during FY 02. These included 136 TEMPEST Countermeasure missions, 8 instrumental tests, 1 low-noise enclosure, and numerous others in support of National-level committees and working groups. Over 29 percent of the missions were OCONUS.

(C//NF)

(b)(1)

(S/NOFORN)

(b)(1)

(U) **Security Liaison Detachment Highlight** (S//NF/FGI/JA) During FY 02, the Security Liaison Detachment dedicated hundreds of man hours conducting liaison with the

Government of Japan to receive information on the North Korean Mother ship sunk by Japan's coast guard as well as to facilitate technical support from US agencies.

(TS//SI)

(b)(1),(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(U//FOUO)

(b)(1)

(b)(1)

INSCOM's Polygraph Program (U//FOUO) During the fiscal year, the program conducted 1,749 CSP examinations. Of these 1,696 were No Significant Responses, 39 Inconclusive, 14 Significant Responses, and 3 No Opinion. The command CSP had 96.7 percent Overall Resolution Rate. The Polygraph Program also completed 74 Operational Cases. Of these 64-No Deception; 2-Inconclusive; 8-Deception Indicated; and 3 No Opinion. The Operational Cases had 89.2 percent Overall Resolution Rate. INSCOM's Polygraph Program assisted in cutting the backlog of NSA examinations at Kunia Regional Security Operations Center. On four occasions, Polygraph resources were used in support of Task Force 170, the testing of terrorist detainees held at GTMO, Cuba.

(U//FOUO) After repeated attempts to reestablish a military polygraph examiner program, the DCSINT finally directed INSCOM to transition to an all-civilian workforce. This was due to the critical shortages in the 351B warrant officer career field.

Army Central Control Office (ACCO) (U//FOUO) The ACCO exercised worldwide technical control of Army-involved foreign counterintelligence/counter-terrorism and security related investigations, Passive Source Operations, Offensive CI Operations

(OFCO), and other special collection techniques. The ACCO conducted its mission through the various command Sub-Control Offices located with the following units: 902d MI Group, 66th MI Group, 500th MI Group, 501st MI Group, 513th MI Group, and 650th MI Group.

(S//NF)

(b)(1)

ARL Missions (S//X1)

(b)(1)

Target Exploitation Detachment-Europe (S//NF)

(b) (1) Per NSA,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Army Technical Control and Analysis Element (ATCAE) (TS//SI)

(b)(1),(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(U) The Naval Security Group Command Admiral's Award for Teamwork was given to the Gladiator Team of the ATCAE. As a participant of the Special High Interest Analysis and Reporting Cell Team at Naval Security Group Detachment Potomac, Washington, D.C., Gladiator Team was tasked to support Project Dull Knife II, a national level cooperative emitter and performance test. The team's 24 hour watch produced the most successful results of five national systems participating in the project despite limited manning. Their effort has given national tasking authorities concrete performance measures to improve the efficiency of cross program processing.

Army RC-12 Guardrail (TS//SI) Guardrail was declared operational as of 14 May (b)(1),(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86 Guardrail is the second operational aircraft to conduct cooperative operations with the national systems following U-2.

(b)(1),(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Drug War (S (b)(1),(b)(3):P.L. 86-36 have been observed by the Medina Regional Security Operations Center (MRSOC).

(b) (1) Per NSA, (b)(3):18 U.S.C. 798,(b)(3):50 U.

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(TS//SI)

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1) and (b)(3)- 18 USC 798, 50 USC 403 & P.L. 86-35 - per NSA

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 24-25

Counterintelligence (S//NF)

(b)(1)

Cyanide Theft (S) (b)(1) alerted authorities on 10 May of three individuals who hijacked a tractor-trailer carrying 96 drums of cyanide in rock form. President Bush and numerous executive agencies were briefed of this situation. The CIA has requested more information from the Mexican government.

NGIC Support (S)

(b)(1)

CHAPTER FIVE

The Global War on Terrorism

Operation Enduring Freedom--Afghanistan

Introduction. (U) In the aftermath of the terrorist attacks of 11 September 2001, the theme behind military action became retaliation, which is known collectively as the "Global War on Terrorism" (GWOT). Defensive measures were established on 12 September under the mission codenamed Operation Noble Eagle. In the initial phase, President George W. Bush was successful in bringing more than 90 other nations and multilateral organizations from every region of the globe into a new style of warfare. The President's first response came with a stroke of his pen as the financial assets of terrorist organizations were seized, disrupting the terrorist fundraising network. The military response began on 7 October 2001 and was named Operation Enduring Freedom (OEF). The objectives of OEF, as stated by the President, include the destruction of terrorist training camps and infrastructure within Afghanistan, the capture of al-Qaeda leaders, and the cessation of terrorist activities in Afghanistan. Operations were supported by significant contributions from the international community. By 2002 the coalition had grown to more than 68 nations with 27 nations having representatives at CENTCOM headquarters. US troops led by General Tommy Franks fought terrorists with unconventional means by blending 21st-century technology with 19th-century tactics. Special Operations troops chased terrorists on horseback while using mobile phones and global positioning systems to pinpoint targets for the Air Force.

(U) INSCOM was required to play a leading role in the GWOT. The Budget Branch immediately solicited a data call for projected requirements. After they were submitted and validated, INSCOM was allotted 204 million dollars for use in specific projects or missions. Foreseeing the unique and essential role of intelligence in such an asymmetric conflict, INSCOM was not discouraged in making punctuated changes with regard to its mission and tools. CENTCOM initiated the campaign in Afghanistan, deploying the 513th MI Brigade as its eyes and ears. Troops deployed at short notice.

The 513th MI Brigade. (U) Based in Fort Gordon, Georgia, the 513th Military Intelligence Brigade provides intelligence to support a wide variety of missions. The brigade assets are divided among four battalions: the 201st, 202nd, 204th, and 297th. In accordance with President Bush's directive, the 513th altered existing plans and focused on the GWOT for the purpose of force protection missions in Afghanistan and Uzbekistan. On 11 September, nearly 120 soldiers from the 513th MI Brigade were already stationed in the Middle East and were operating systems that would become crucial in the days to come. Within weeks 200 additional soldiers were deployed. The Brigade staff promptly identified many of the specific skills needed from the Reserve component to reach a wartime capacity and a by-name list was submitted to the Pentagon by late September. The reservists, who were mostly

designated with the military occupational specialty of 98G (cryptologic linguist) with a further specialization in Farsi and Arabic languages, processed at Ft. Gordon and joined the brigade. Despite the call-up, the demand for linguists was not fulfilled. Without a large pool of linguists with a background in Uzbek, Pashto, and Dari from which to drain, the brigade was given permission to contract with civilians. On a Thanksgiving Day, soldiers from the 202d MI Battalion departed Ft. Gordon for Camp Stronghold Freedom in Uzbekistan. One month later they entered Afghanistan as part of a mobile interrogation team, assisting national level agencies. Because the Army had decided to divest in tactical SIGINT, the 201st MI Battalion (the SIGINT unit of the Brigade) was challenged to meet the intelligence needs of CENTCOM. Having lost half of the Battalion from force reductions, it was reinforced with reserve personnel. This situation has made the Army reconsider its decision to eliminate SIGINT units at echelons above corps.

(S)

(b)(1)

(S)
(TS//NF)

(b)(1)

(b)(1)

(S) (TS// //NF)

(b)(1)

The 66th MI Group. (S) (TS// //NF)

(b)(1)

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1) and (b)(3)- 18 USC 798, 50 USC 403 & P.L. 86-35 - per NSA

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 30-31

IAGPA-CSF Form 6-R
1 Sep 93

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The 115th MI Group. (S//SI) As opportunities arose, many other units in INSCOM made contributions to the GWOT and OEF in Afghanistan. The 115th MI Group made one such contribution when it supported CENTCOM with SIGINT reports. As a part of the Kunia Regional Security Operations Center (KRSOC),

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(TS//SI)

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(S//SI) In response to a formal request for assistance from the CENTCOM J2 the Army Technical Control and Analysis Element (ATCAE) collaborated with several NSA organizations to solve many collection difficulties for OEF. In November of 2001, ATCAE bridged the HFDF intelligence gaps in threat signals emanating from Afghanistan. Later in the same month, ATCAE's Operational Electronic Intelligence (OPELINT) Emitter Mapping section reported on probable communications between Taliban elements camped at Samakay, Afghanistan, and a command and control element in Quetta, Pakistan. In early December, the Technical Feedback Cell of ATCAE, issued two critical messages in support of OEF.

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The 116th MI Group. (S//SI) The 116th MI Group/Gordon Regional Security Operations Center (GRSOC) established an Afghan section in January of 2002 which

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The 742d MI Battalion. (TS//SI) The 742d MI Battalion supported OEF by completing 12 assignments in the week preceding 29 January 2002.

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The National Ground Intelligence Center (NGIC). (U) Within weeks after the attacks of 11 September, CENTCOM asked the US Army National Ground Intelligence Center to produce accurate representations of current minefields in Afghanistan. In response, NGIC established a dynamic web-based mapping service using geographic information systems (GIS) technology. The dissemination of this information provided ground commanders with the most reliable data and graphics that depict the location of minefields. By discarding paper maps and static digital displays, tactical units are able to visualize and query multiple data-layers. Soldiers now have customized maps at their disposal. The new product has allowed for rapid dissemination of GIS minefield data to operational planners supporting OEF. GIS is a computer-based mapping tool capable of assembling, manipulating, and displaying geographically referenced information within a layered system. The layers of information that can be combined only depends upon the user's need, such as for determining suitable helicopter landing zones, analyzing cross-country movement, or, as in this case, locating minefields from old Soviet hardcopy maps. Working with the Central Intelligence Agency Map Library, NGIC digitized, re-projected, and posted 81 original Soviet maps on classified websites within three days. In an effort to obtain more data, NGIC personnel decided to review intelligence message traffic over the last twelve years to find evidence of minefield incidents. The reported incidents were then designated geographic locations as another geospatial layer of data. When US soldiers landed at Kandahar Airfield, mines depicted on NGIC sites proved timely and invaluable.

(U/FOUO) In a continuation to perfect these minefield representations in late December 2001, members of the NGIC visited the James Madison University Mine Action Information Center (MAIC) to get a better understanding of the mission and access the availability of landmine data for use in support of OEF. The director, Mr. (b)(6) and deputy director, (b)(6) discussed humanitarian mine clearance, victim assistance, and other landmine-related issues. As an established information clearing house, MAIC is capable of obtaining geographic data on minefields of current interest to NGIC, and they have indicated their willingness to provide NGIC with the necessary assistance. Much of the MAIC's funding comes from the Defense Security Cooperation Agency, Office of Humanitarian Demining.

(U) As a result of its tasking and unique capabilities, NGIC made a number of other notable contributions to OEF. NGIC printed more than 15 thousand handbooks and reproduced thousands of maps in various formats for troops in OEF. These products were scanned and disseminated on CDs and maintained on a Multi-Media Regional Data Base for immediate access. NGIC also ensured that a complete set of maps was immediately available for all OEF-related countries. It trained more than 200 personnel to defend against threats to security on the internet by screening traffic

and refining electronic profiles. Screening also eliminated the flow of low-value traffic.

The Army Cryptologic Office (ACO). (TS//SI) The Army Cryptologic Office, as part of the INSCOM Headquarters G3, deployed the Steamroller-1, TROJAN remote collection system, to provide force protection and warning in January of 2002.

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(S//SI)

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(b)(1) (S//NF) The (b)(1) Program Manager in the G3 staff of INSCOM Headquarters selected a team of five soldiers to deploy in support of OEF in December of 2001. Throughout FY02 the team reported extensively to NSA and theater SIGINT assets

(b) (1) Per NSA, (b)(3):50 U.S.C. 403,(b)(3):P.L. 8

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Operation Enduring Freedom--Philippines

Introduction (U) Being the military and operational arm of the GWOT, OEF responds to al-Qaeda whereever it may be in the world. Bin Ladin's al-Qaeda network embodied more than just a network in Afghanistan. Having cells and spheres of influence in many locations ranging from remote villages to populated urban centers all over the world, al-Qaeda would appear ubiquitous; therefore, the military campaign required a hasty expansion to encompass operations around the planet. More than 60,000 American troops are deployed in OEF of which only 9,000 are in Afghanistan; others are in the Philippines, Georgia, and Yemen. World-wide, approximately 2,290 terrorist-related arrests were made in 99 countries between 12 September 2001 and 22 October 2002.

(U) The determination of when and where to strike terrorism next was initially unanswered. When the President announced the first US strikes on Afghanistan, he explained to the nation that "the battle is broader" and suggested other nations aiding terrorism could also come under attack. In response to this declaration, the US armed forces went to support the Philippine Government and its war against the Abu Sayyaf Group (ASG). As part of the GWOT this military campaign is a part of OEF, dubbed Operation Enduring Freedom-Philippines (OEF-PI).

(U) The relationship between the US and the Philippines has had highs and lows. A century ago, the US, as an occupying power, fought to quell an insurrection in what is often called the Philippine-United States War. After the Japanese occupation, the US has generally been considered a friend; however, this condition has remained a tenuous relationship. In 1992 the Filipino government refused to renew long-term leases for military bases at Subic Bay and Clark Airfield primarily because of support by the US government to Ferdinand Marcos during the 1970s. Through the late 1990s relations had cooled so much that no joint military exercises occurred for five years and in the fiscal year 2000, military assistance in the form of economic funds reached zero. In light of the recent terrorist attacks, however, a new partnership has emerged in a new century. President Arroyo of the Philippines received 150 million in counterterrorism assistance of which 100 million will be in the form of reconditioned military equipment. In addition to equipment, US military forces have renewed direct contact with the Philippine military during annual exercises and counterterrorism training. US soldiers also provide specialized support to the Philippine army and naval marines in operations against Abu Sayyaf guerillas. One of the more critical means of support to the Philippine military comes through the benefit of US military intelligence assets. During phase two of a three-phase exercise, US and Philippine forces trained in receiving, processing, and exploiting intelligence to enhance joint capability in conducting military, civil, and psychological operations.

(U)

The 115th MI Group. (~~TS//NF~~) In support to PACOM and Operation Enduring Freedom-Philippines in April and May of 2002, the G3-IO (Information Operations) section conducted intensive SPEA (Special Purpose Electronic Attack) planning. Working with PACOM, the 1st IOC and the 704th MI BDE, the operations section

deployed a 704th SPEA team to the Philippines to attack the communications of terrorist cells where American and Philippine hostages were being held. As part of a rescue mission the team planned to participate either in the mission using SPEA weapons or train Special Ops Forces who would use the weapons. The mission was never completed, however, because Philippine forces elected to carry out the rescue by themselves. The preparation was still valuable as a training exercise for future deployments. The 704th with the help of G3-IO made a similar deployment to Afghanistan in support of CENTCOM in September of 2002.

(TS/

(b)(1)

(b)(1)

The 500th MI Group. (S) The 500th MI Group was tasked in January to provide (b)(1) support to (b)(1) Philippines (JTF-510).

The War on Terrorism Throughout the World

Introduction. (U) Although a large portion of resources for FY02 have been marked for Afghanistan and the Philippines, INSCOM remains successful all over the world in the war against terrorism. No nation can say with certainty that it is impervious to terrorist infiltration. Thus, INSCOM has expanded its field of vision in an attempt to detect terrorist threats from any place in the world.

The 704th MI Brigade. (TS//SI// INSCOM units were active in a number of states in an attempt to contain the spread of terrorism. In March, the 704th MI Brigade provided force protection for US forces deployed

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Upon reception of this information, the Deputy CINC commented that the work was impressive.

The 109 MI Group. (TS//SI)

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

This information will be used to build information on suspected terrorist networks.

The 116th MI Group. (TS//SI)

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The Army Technical Control and Analysis Element (ATCAE). (TS//SI//NF) The Army Technical Control and Analysis Element focused on

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(S//SI)

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The Information Dominance Center at Fort Meade (IDC). (TS//SI) The Information Dominance Center at Fort Meade performed a critical analysis that led to

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The IDC conducted traffic analysis and technical development

The NSA's approval to disseminate the report validates the techniques and procedures of IDC.

The Intelligence Operations Center (IOC). (TS//SI) In an effort to target a major practitioner of terrorism, the INSCOM Intelligence Operations Center developed

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Such analyses have been useful in validating other sources of intelligence In a similar effort the IOC hosted a meeting of the Joint Intelligence Task Force-Counter Terrorism (JITF-CT) and INSCOM representatives on 30 May of 2002 to discuss an

initiative to collaborate. They agreed to begin a concerted effort against the more formidable of terrorist groups:

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

The Operations and Intelligence Signals Technical Development Activity. (S//CCO) (b) (1) Per NSA,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(b) (1) Per NSA,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Counterintelligence as Counter Terrorism

Introduction. (U) At the start of operations against terrorist organizations, there could be no doubt that counterintelligence would play a vital role. The key to successful terrorism has always rested in infiltration. This became disturbingly evident after examining the attacks of 11 September 2001. Defending against infiltration has long been a primary function of counterintelligence. The role of counterintelligence as a line of defense against terrorism, therefore, remains critical to the security of the Army and the Nation.

The 902d MI Group. (S/NF)

(b)(1)

(b)(1)

(S//~~NF~~)

(b)(1)

(S//~~NF~~) As a direct result of the attacks on the World Trade Center and the Pentagon, it is not surprising that the Offensive Counterintelligence Operations Program (OPCO) of the S-3 of the 902d MI Group concentrated on the terrorist threat for FY02. (b)(1)

(b)(1)

The Army Central Control Office (ACCO). (S//~~NF~~) The Army Central Control Office (ACCO), as part of the INSCOM Headquarters G3, addressed a high number

of CI investigative and operational issues during FY02 with the initiation of [redacted] (b)(1)

(b)(1) ACCO also initiated and managed an unusually large number of foreign counterintelligence and counter-terrorism investigations. (b)(7)(E) [redacted]

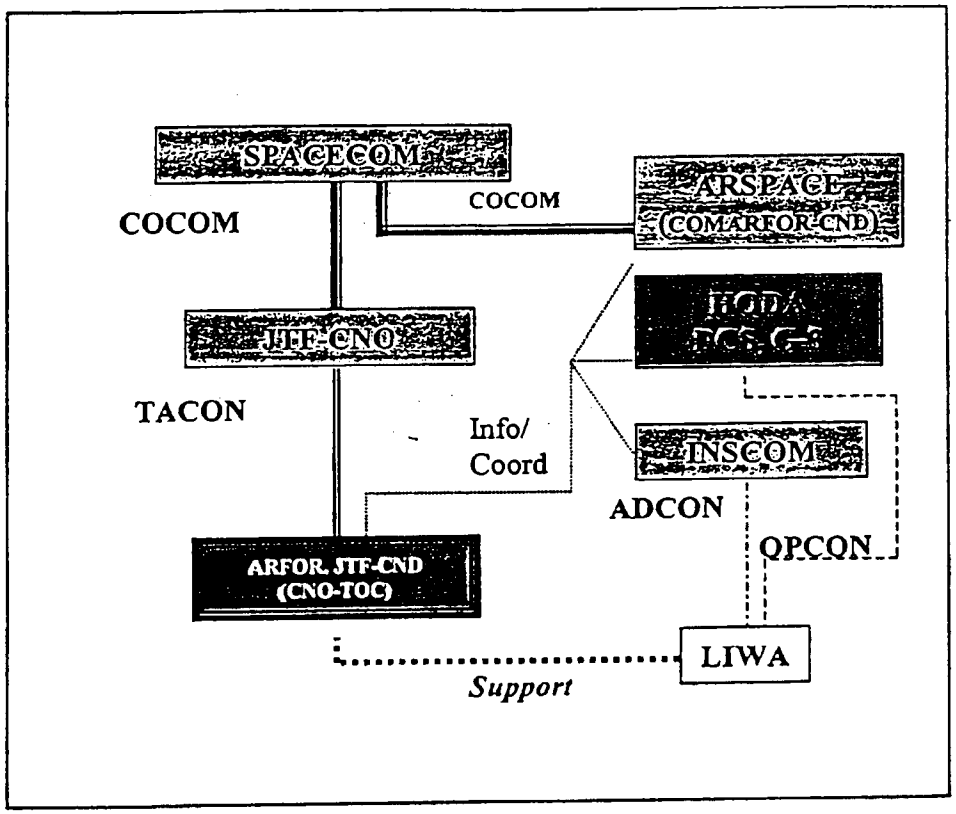
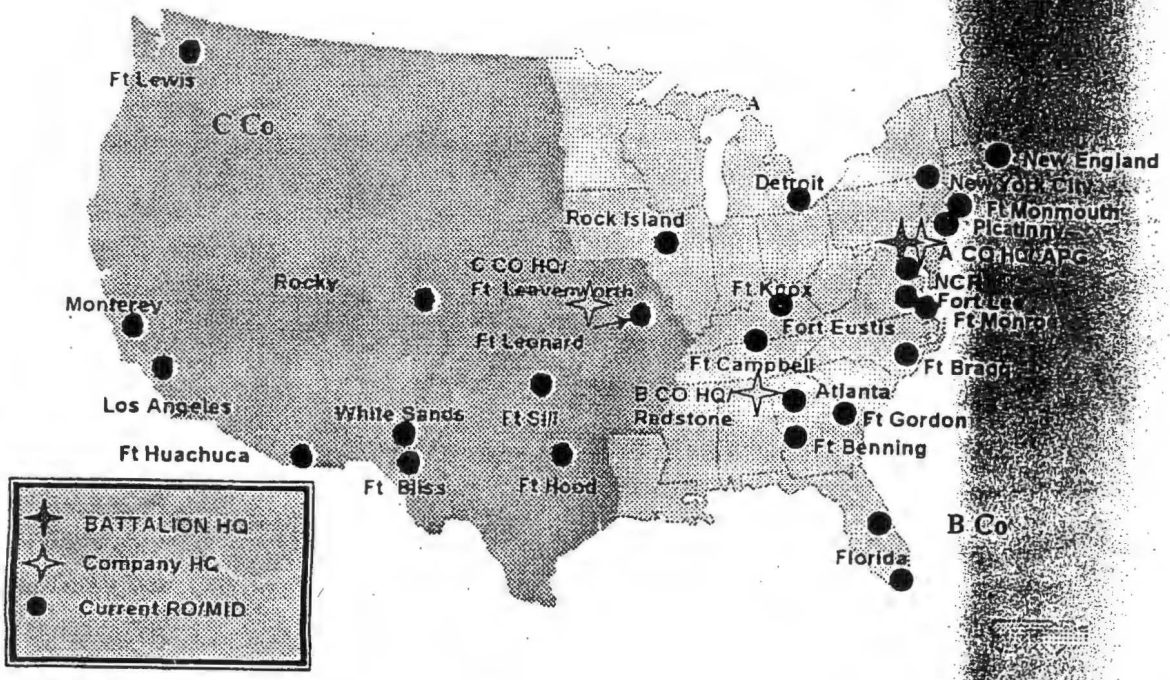


Figure II-5. LIWA Command Relationships

308th Military Intelligence Battalion
Area of Responsibility



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

REPLY TO
ATTENTION OF:

Freedom of Information/
Privacy Office

23 JUN 2014

This is in further response to your Freedom of Information Act (FOIA) request of August 18, 2014, for the INSCOM Annual History for FY 2003 and supplements our response of October 10, 2012.

As noted in our letter, coordination has been completed with other elements of this command and other government agencies and the records have been returned to this office for our review and direct response to you.

We have completed a mandatory declassification review in accordance with Executive Order (EO) 13526. As a result of this review, information has been sanitized and three pages are denied in their entirety, as the information is currently and properly classified TOP SECRET, SECRET and CONFIDENTIAL according to Sections 1.2 (a)(1), 1.2 (a)(2), 1.2 (a)(3) and 1.4 (c) of EO 13526. This information is exempt from the public disclosure provisions of the FOIA pursuant to Title 5 U.S. Code 552 (b)(1). It is not possible to reasonably segregate meaningful portions of the withheld pages for release. A brief explanation of the applicable sections follows:

Section 1.2 (a)(1) of EO 13526, provides that information shall be classified TOP SECRET if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

Section 1.2 (a)(2) of EO 13526 provides that information shall be classified SECRET if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

Section 1.2 (a) (3) of EO 13526 provides that information shall be classified CONFIDENTIAL if its unauthorized disclosure reasonably could be expected to cause damage to national security.

Section 1.4 (c) of EO 13526, provides that information pertaining to intelligence activities, intelligence sources or methods, and cryptologic information shall be considered for classification protection.

The deleted information is also exempt from automatic declassification in accordance with EO 13526, Section 3.3(b)(1) because its release would clearly and demonstrably be expected to reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.

Information has been sanitized from the records that would reveal sensitive intelligence methods, techniques and sources. This information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(7)(E) of the FOIA. The significant and legitimate governmental purpose to be served by withholding is that a viable and effective intelligence investigative capability is dependent upon protection of sensitive investigative methodologies.

The withholding of the information described above is a partial denial of your request. This denial is made on behalf of Major General George J. Franz III, Commanding, U.S. Army Intelligence and Security Command, who is the Initial Denial Authority for Army intelligence investigative and security records under the FOIA. You have the right to appeal this decision to the Secretary of the Army. Your appeal must be postmarked no later than 60 calendar days from the date of this letter. After the 60-day period, the case may be considered closed; however, such closure does not preclude you from filing litigation in the courts. You should state the basis of your disagreement with the response and provide justification for a reconsideration of the denial. An appeal may not serve as a request for additional or new information. An appeal may only address information denied in this response. Your appeal is to be made to this office, for forwarding, as appropriate to the Secretary of the Army, Office of the General Counsel.

In addition, coordination has been completed and we have been informed by the National Security Agency (NSA) (FOIA Case: 54911), that their information contained in the records has been sanitized from the records pursuant to Title 5 U.S. Code 552 (b)(1) and (b)(3).

5 U.S.C. 552 (b)(1) - The information is properly classified in accordance with the criteria for classification in Section 1.4 of Executive Order (EO) 13526.

5 U.S.C. 552 (b)(2)

5 U.S. C. 552 (b)(3) – The specific statutes are listed below:
50 U.S.C. 402 note (Public Law 86-36 Section 6)
50 U.S.C. 403-1(i)
18 U.S.C. 798

The initial denial authority for NSA information is the Deputy Associate Director for Policy and Records, Ms. Diane M. Janosek. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days of the date of the initial denial. The appeal shall be in writing to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road, STE 6248, Fort George G. Meade, Maryland 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS FOIA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent unusual circumstances. Please cite NSA FOIA Case: 54911 assigned to each case so that it could be easily identified.

Additionally, coordination has been completed and we have been informed by the Federal Bureau of Investigation that their information contained in the record is releasable to you.

We apologize for any inconvenience this delay may have caused you.

There are no assessable FOIA fees for processing this request.

If you have any questions regarding this action, contact this office at 1-866-548-5651, or email the INSCOM FOIA office at usarmy.meade.902-mi-grp-mbx.inscom-foia-service-center@mail.mil and refer to case #0683F-09.

Sincerely,

Joanne Benear
Chief
Freedom of Information/Privacy Office

Enclosure

ANNUAL COMMAND HISTORY

US ARMY INTELLIGENCE AND SECURITY COMMAND

FISCAL YEAR 2003

History Office
of the
Strategic Management and Information Office
Nolan Building
8825 Beulah Street
Fort Belvoir, Virginia 22060-5246

30 September 2004

DERIVED FROM: MULTIPLE SOURCES
DECLASSIFY ON: X1
DATE OF SOURCE: 30 September 2003

TABLE OF CONTENTS

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

45

Location of Iraqi Deputy Prime Minister

46

OVERVIEW

(U) The following is a "MEMORANDUM FOR ALL INSCOM Personnel" written by General John F. Kimmons, the Commanding General of INSCOM. The subject of the memorandum is the commander's vision and operational imperative.

(U) We are in the post-9/11 world—our Nation and Army are engaged in the 3rd year of a Global War On Terrorism (GWOT). As part of the Joint and Interagency Team, INSCOM is concurrently engaged in enduring intelligence operations to counter the use of Weapons of Mass Destruction (WMD) by terrorists/rogue sponsor states and prepare for other regional contingencies. This is consistent with National Security Strategy (NSS) goals to ensure political and economic freedom, achieve peaceful relations and advance respect for human dignity worldwide. During Operation Iraqi Freedom (OIF), the US exercised "preemptive action," one of eight methods outlined in the NSS, to accomplish the above US goals. The nature of transnational terrorism suggests that we will utilize this method again. Preemptive action places a premium on rapid fusion of all-source intelligence to facilitate high confidence planning and operational action.

(U) Success in GWOT/OIF/OEF remains the Army's "#1" priority. Towards that end, the CSA recently identified 16 "Immediate Focus Areas" for near term actions. Two of these (#6 Modularity & #16 Actionable Intelligence) hold special significance for INSCOM. We must adapt and focus our efforts across the MACOM to develop and field capabilities that satisfy "Immediate Focus Area" objectives and keep INSCOM a high payoff member of the Joint and Interagency intelligence team.

(U) This is a tough, but achievable wartime challenge. Getting there will require us to expand the INSCOM Information Dominance Center (IDC) horizontal integration capabilities linked, regionally dispersed "Knowledge Centers" which directly support ongoing operations (i.e., G2/J2/C2's in contact). Deployed INSCOM "modules" will provide inputs and leverage horizontal integration in support of better analysis. The personal engagement of INSCOM leaders at every level is required. Each of us is "in the warfight" regardless of discipline or location. We must bring a warrior and wartime mindset to every job in the work force. We need to produce fused, relevant intelligence everyday. Each action must be held up against these wartime measures of merit. Thanks for your commitment and focus.

CHAPTER ONE

MISSION AND ORGANIZATION

Activation of the 1st Information Operations Command (Land). (U//~~FOUO~~) The 1st Information Operations Command (Land) was organized and activated on 16 October 2002 at Headquarters INSCOM, Fort Belvoir, VA. Organized from elements in the Land Information Warfare Activity (LIWA), the new command continues the mission of (b)(7)(E) a TOE unit. (b)(7)(E) TDA unit, had been discontinued on 15 October 2002 in anticipation of its replacement by the 1st IO Command. (b)(7)(E) established in 1995 to coordinate, arrange, and synchronize IO intelligence support, and conduct operations throughout the computer network operations (CNO) spectrum to include force protection. The name change is part of a larger plan to reduce the number of TDA units in INSCOM for purpose of protecting essential units from potential TDA cuts in the Army. Originally the command had decided on the 1st MI Center as the new designation, but the (b)(7)(E) command protested having a name that did not reflect its unique mission. Thus the 1st IO Cmd was chosen.

Change of Status for the 470th MI Group and relocation. (U//~~FOUO~~) The 470 MI Group (provisional) changed its status to the 470th MI Group in 16 October 2002 at Fort Buchanan, Puerto Rico. One of INSCOM's oldest subordinate commands, the 470th was inactivated in 1997 as a downsizing measure. As a result of the recently completed Military Intelligence Functional Area Assessment, however, Army Vice Chief of Staff, General John M. Keane has directed the conversion of INSCOM's two force projection brigades into five theater-support elements to which each is dedicated to one of the Army Service Component Commanders stationed worldwide. One product of this decision has been the reactivation of the 470th MI Group to support SOUTHCOM operations in Latin America.

(U//~~FOUO~~) In September 2003, the unit moved its HQ with that of SOUTHCOM from Fort Buchanan, PR to Fort Sam Houston at San Antonio, Texas. The 470th MI Group will establish its headquarters with an interim SCIF at Camp Bullis, a sub-installation of Fort Sam Houston. The unit will move into a permanent facility and SCIF when renovations on the old Brooks Army Medical Center, which began on 9 June 2003, are completed. In accordance with AR 5-10 Stationing, the 470 MI Group, by moving to Fort Sam Houston, will provide the most benefit to USARSO through proximity and cost effectiveness of spacing.

Change of Status for the 66th MI Group. (U//~~FOUO~~) The 66th MI activated on 16 October 2002, removing its provisional status. During the activation ceremony at Kelley Barracks in Darmstadt, Germany, the 533rd MI Battalion (provisional) was discontinued and replaced with the newly activated 2nd MI Battalion. As MTOE units they will have direct ownership of manning and equipment.

Activation of the 205th MI Battalion. (U//~~FOUO~~) The 205th MI Battalion was activated on 16 October 2002 at Fort Shafter, HI. The battalion will be a subordinate of the 500th MI Group. The unit provides CG USARPAC with theater-level, multi-disciplined intelligence. Its companies are deployed throughout the Pacific Ocean and western United States: Japan; Phoenix, Arizona; Hawaii; Fort Lewis, WA; and Alaska.

Change of Status for NGIC. (U//~~FOUO~~) The National Ground Intelligence Center, a TDA unit, was officially inactivated and the 2d Military Intelligence Center was stood up in place of NGIC as an MTOE unit on 17 October 2002. The name change is part of a larger plan to reduce the number of TDA units in INSCOM for purpose of protecting essential units from potential TDA cuts in the Army. Unofficially the 2d MI Center has elected to retain its original designation, and for all INSCOM's intents and purposes, it is still referenced as NGIC.

The imagery elements of NGIC at the Washington Navy Yard, the Imagery Assessment Directorate (IAD), which was redesignated as the 3rd MI Center on 16 October 2001 (FY02), is now a separate but subordinate command to the 2nd MI Center. Previously the IAD had been an organic part of NGIC with no Unit Identification Code (UIC). Now the 3rd MI Center as a TOE unit has a UIC under the command and control of the 2nd MI Center. Another subordinate unit to the 2nd MI Center (NGIC) is the 203rd MI Battalion at Aberdeen Proving Grounds. The status of the 203rd MI Battalion recently changed from an active unit to a reserve unit.

US Army Central Personnel Security Clearance Facility (CCF) Realignment (U//~~FOUO~~) Effective on 1 Oct. 2002 the CCF became a subordinate command of INSCOM. Formed in 1977 CCF, originally under PERSCOM, has the responsibility for granting, denying, or revoking the security clearances of Army personnel worldwide. CCF also screens drill instructors, recruiters, and command sergeant major candidates; conducts LTC, COL, and General Officer command board screens; and assists the Immunization and Naturalization Service by assisting with soldier citizenship applications. The move from PERSCOM to INSCOM came as part of the Transformation Business Process initiated by the Secretary of the Army.

Computer Network Operations Way Forward Study Senior Information Operations Review Council (SIORC) Meeting (U//~~FOUO~~) The DCS G2, G3, and G6 convened with CG INSCOM (MG Alexander) and CG NETCOM (MG Hylton) on 20 November 2002 to finalize recommendations from the Computer Network Operations (CNO) Way Forward Study. The CNO Way Forward Study, initiated by CG, INSCOM and CG, NETCOM, began from an examination of the results of the Mannheim Exercise of April 2002, a CNO event conducted in Europe, involving the 1st IOC and 5th Signal Command of NETCOM. The exercise demonstrated how the Army could not afford to operate Computer Network Defense in isolation and the need to integrate CNO with Information Operations. Many large-scale organizational changes were implemented. CG, USAINSCOM was designated Deputy Commander, Army Forces-Computer Network Operations (DEPCOMARFOR-CNO, less CND) for the Commander, US Strategic Forces Command, effective 1 January 2003. The Deputy Chief of Staff, G3 designated Army CNO assets as necessary between USARSPACE, USA INS COM, and

USACOMARFOR: CG INSCOM was designated Army Computer Network Attack (CNA) director for available forces, providing assets to CG USARSPACE and CG USACOMARFOR for tasking. CG INSCOM also directs Army Computer Network Exploitation Forces as support for CG, USARSPACE. CG, INSCOM remains in administrative command of the 1st IOC. The INSCOM CWC, 1st IOC ACERT, and NETCOM/9th ASC ANOSC TACON were collocated in the INSCOM IDC.

Relocation of the Army Network Operations and Security Center (ANOSC) in the Nolan Building (U//~~FOUO~~) As part of the Computer Network Operations Way Forward Study, the Department of the Army moved the US Army Network Operations and Security Center (ANOSC) from Fort Huachuca, AZ to Fort Belvoir, VA. The collocation of ANOSC and INSCOM facilitates the interaction with the Defense Information Systems Agency, the Joint Task Force-Computer Network Operations, the 1st Information Operations Command, and the Army Computer Emergency Response Team, all of which have HQs in the National Capital Region.

(U//~~FOUO~~) US Army Forces Command originally established ANOSC as an operational element of the former Army Signal Command. On 1 October 2002, it was made a subordinate command of the US Army Network Enterprise Technology Command/9th Army Signal Command at Fort Huachuca. ANOSC, an enterprise-level Army activity, provides a network interface between DA and Department of Defense activities.

(U//~~FOUO~~) The relocation effectively brings all computer network operations in the Army together as one team to protect Army computer operations. Phased over several months during the summer of 2003, the move initially brought 14 military positions, 14 department-of-the-Army civilian positions, and 32 contracted positions to Fort Belvoir.

Collection Branch of the Counterintelligence/Human Intelligence/Special Activities Division (U//~~FOUO~~) INSCOM G3 reassigned the Collections Branch and the CI and HUMINT collection management functions to the CI/HUMINT Division in May 2003. These functions had been with the G3 Operations and Intelligence; however, the position had traditionally been located in the CI/HUMINT Division since the mid-1990s.

Formation of the Strategic Management and Information Office (U//~~FOUO~~) From a string of events and decisions, spurred from the FY 00/01 INSCOM Performance Plan and the HQ Structure and Functions Review Final Report, MG Alexander acted on the proposed recommendation for a Command Information Cell, the only component of the original three-phase implementation to remain under consideration after the 911 attacks. According to the plan as outlined by the Chief of Staff, (b)(6) in a memorandum to staff elements, "those offices that tell the INSCOM story"—Strategic Plan/Command Quality Office, Public Affairs Office, Command Briefing, Speechwriter, Marketing, and the History Office—were to be moved from their respective directorates and consolidated "into a single office under the Office, Chief of Staff," effective 1 September 2002. Along with consolidation, funding lines and related contracts were

transferred to the new organization, officially titled as the Strategic Management and Information (SMI) Office. ACofS, RM Jo Ann Mettile was assigned to be the primary action officer for this transition. The SMI Office opened for business on 1 September 2002. Throughout FY03 designated elements have moved their operations under the SMI umbrella. In that time its mission was further defined as the Command focal point for all information concerning HQ INSCOM functions: development of a long-range corporate strategy; publication of the INSCOM Strategic Plan and Annual Performance Plan (AR 5-1); management of the Total Army Program, service as MACOM POC, implementation of management through publications, development of programs, procedures, and mediums to tell the INSCOM story; service as public affairs advisor to the Commander, staff, and major subordinate commanders; implementation of the command history program; response to requests for historical information on INSCOM; and direction of the Strategic Information Office, Public Affairs Office, and the Command History Office.

(U//~~FOUO~~)

(b)(7)(E)

Cyber Counterintelligence Activity (U//~~FOUO~~) On 1 May 2003, the Information Warfare Branch, a subordinate unit of the 310th Military Intelligence Battalion, 902d MI Group was officially redesignated as the Cyber Counterintelligence Activity (CCA)

(b)(7)(E)

CCA is one of many ways INSCOM has chosen to obviate vulnerabilities as information warfare becomes reality.

(U//~~FOUO~~) The founding authority for the CCA is the newly established (b)(7)(E) approved by the Secretary of the Army. This authority allows the CG, INSCOM to direct CI technical collection against computer trespassers who attempt to exploit Army Information Systems (AIS). The 310th MI Bn, as a result of this action, is more responsive to attempted intrusions in the AIS and able to conduct more extensive investigations.

(U)

Formation of the US Army Operational Activity ~~(S//NF)~~ The Army activated the Army Operational Activity (AOA) as of January 2003.

(b)(7)(E)

Ground Work Initiave (~~S~~) The 105th MI Battalion executed the Ground Work Initiative which is the preliminary step toward the establishment of the European Security Center (ESC). The initiative encompasses the unit's

(b)(1)

Plans for the European Security Center (~~S~~)

(b)(1)

Regraded SECRET on
30 April 2010
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

CHAPTER TWO

PERSONNEL, SECURITY, LOGISTICS, ETC.

Mold Remediation at the Nolan Building (U) During the course of remodeling, workers discovered mold behind the walls of the northeast corner and stairwell of the Nolan Building. G4, in conjunction with Fort Belvoir, Director of Installation Services (DIS), contracted to remove the mold from all affected areas on 21 October 2002.

INSCOM Units make Semi-Finals in Army Maintenance Excellence Awards (U) Five US Army INSCOM units were selected as semifinalists in Phase I of the 2002 Chief of Staff Army Awards for Maintenance Excellence (AAME) competition in January 2003. The following units were selected: 527th MI Battalion, 524th MI Battalion, 3rd MI Battalion of the 501st MI Brigade, 205th MI Battalion of the 500th MI Group, and the 206th MI Battalion of the 116 MI Group. The AAME improves, sustains, and recognizes unit-level maintenance programs throughout the Army. The competition criteria are based on mission accomplishment, effectiveness, management status, innovation and personnel quality of life programs. In the final decision, the 527th MI Battalion won the 2002 AAME award in the large Table of Distribution and Allowances of Service Support category.

Promotion of MG Alexander (U) Secretary of Defense Donald Rumsfeld announced the promotion of MG Keith B. Alexander to Lieutenant General and his assignment to Deputy Chief of Staff for Intelligence on 5 May 2003.

Transfer of Command (U) MG John F. Kimmons assumed command of INSCOM during a ceremony in front of the Nolan Building, Fort Belvoir, VA on 28 August 2003. He replaced General George F. Fay, who had been acting commander since the departure of Lieutenant General Keith B. Alexander, who relinquished command of INSCOM on 02 July 03. The Department of the Army made the announcement during the week of 20 to 25 April 2003 that BG John F. Kimmons would succeed MG Alexander. MG Kimmons had previously been the Director of Intelligence, US Central Command, MacDill Air Force Base, FL.

(b)(1)

(b)(1)

~~(S//NF)~~

(b)(1)

Polygraph Program and Transition (U//~~FOUO~~) INSCOM Polygraph program conducted 1744 CSP examinations. 1707 were no significant responses; 30 were inconclusive; 7 were significant responses; and 5 were No Opinion. The command CSP had a 97.4 Overall Resolution Rate, 1% Non-support rate, and a 43% admission/DI confirmed statistics. The Polygraph Program completed 152 operational cases. Among the operational tests, 121 were no deception indicated; 22 were inconclusive; 9 were deception indicated; and 9 were no opinion. The OPS test had a 79.6% overall resolution rate, a 2% Non-support rate, and a 40% admission/DI confirmed statistics.

(U//~~FOUO~~) In July 2003 INSCOM initiated a transition to an all-civilian polygraph workforce. PERSCOM has only agreed to allow INSCOM to retain military personnel until 2005. For many years, the INSCOM Polygraph Program struggled to recruit and retain military polygraphers (351BK); however, during the fiscal year PERSCOM revealed that new personnel would not be forthcoming. Due to the constant shortage in this military field, Army G2 conceded that replacing military personnel was no longer feasible and authorized a transition to an all-civilian workforce.

~~(S//NF)~~

(b)(1)

(b)(7)(E) (~~S~~) In response to the weaknesses identified in the Trojan Vulnerability Assessment in 2001, HQDA has initiated the construction of the (b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36 (b)(1),(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 40 The assessment identified the (b)(7)(E) Belvoir at Fort Belvoir as a single point of failure for the (b)(7)(E) network and recommended a Continuity of Operations Plan (COOP) site. With $3.91 million dollars to fund the effort (5 million when equipment, facility upgrades, and manpower are included), HQDA constructed a Quick Reaction Capability in March 2003 to support units deployed in Iraq. HQDA expects

(b) (1) Per NSA,(b) (3):18 U.S.C. 798,(b) (3):50 U.S.C. 403,(b) (3):P.L. 86-36

completion of the [redacted] by the end of FY04. In addition, a DODIIS Disaster Recovery Center (DRC) and backup database repositories for various government facilities will be in the same facility. The second (b)(7)(E) will cut the load on TROJAN circuits at the Fort Belvoir (b)(7)(E) by fifty percent.

Metro Park Facility (U//~~FOUO~~) As Headquarters INSCOM grew as a result of reorganization and the accommodation of NETCOM personnel, INSCOM elected to lease space, create a SCIF environment, and move 400 personnel out of the Nolan Building. Accepting a new operational mission will require INSCOM to reconfigure its headquarters arrangement, a task not undertaken since the completion of the Nolan Building fifteen years ago. The Metro Park Facility consists of 101,700 square feet of rented space on the top four floors of a six-story building in close proximity to the Nolan Building. The move began in late July and finished by August of 2003. The move began with the migration of thirteen staff elements: ACofS, G1, ACofS, RM, SMIO, DOC, VAD (LIWA), FSD (IMP blg), SMIO-PAO (blg. 1499), ACofS, G4, ACofS, G6, Small Business, PI&T (training staff), ACofS, G4 (blg 1498).

Equal Opportunity Complaints (U) There were three formal EO complaints filed among INSCOM units during FY 2003. Of the formal EO complaints, one was an allegation of racial discrimination and two were allegations of sexual harassment of which all three were unsubstantiated.

Retention Statistics (U) The following retention statistics are by objective/ accomplished:

Initial Term	Mid-Career	Career	FY02 ETS	Reserve Component
403/403	249/259	120/128	256/303	105/114

Career Intern Programs (U//~~FOUO~~) The Civilian Personnel Division of G1, in an effort to bolster both the DA Intern and INSCOM Career Intern Programs, expanded its College Recruiting Program. New recruiting sites included the City University of New York, Mercyhurst College, Norfolk State University, and the University of Maryland Eastern Shore. Members of CPD staff attended job fairs at Norfolk and Maryland, selecting an ICIP from each. Coordination visits to establish relationships for FY04 went to Mercyhurst and CUNY. CPD will attend job fairs at all four universities.

Relocation of the Army Operational Activity (U//~~FOUO~~) The Army Operational Activity (AOA) was moved at the beginning of FY03 to leased space. Army planners searched for an alternative location on government property due to the high cost of leased space. They identified and acquired permanent space on the second floor of building 8544 at Fort Meade, which had been occupied by the 310th MI Battalion. The AOA required extensive renovations to support a SCIF and other architectural requirements.

Most of these renovations were completed in September 2003, allowing the AOA to move before incurring another yearly leasing obligation.

SCIF Renovations for the 902d MI Group (U) ~~(S)~~ The SCIF occupied by the command group of the 902d MI Group was renovated and expanded after nearly two decades of operation with few improvements. The renovations facilitated better access to S3, CIIAC, the Command and Control Conference Room, and operational assets.

Investigative Records Repository (U//~~FOUO~~) During FY03, the Investigative Records Repository (IRR) reviewed 68,137 dossiers (a decrease of 22,000 actions from FY02), 139 FPAs, and 33,147 supplemental and adjudicative material pieces. New dossiers amounted to 24,236—22,399 in Records Processing Division and 1,837 in Special Records Repository.

Military Intelligence Civilian Excepted Career Program (MICECP) Recruitment (U//~~FOUO~~) Through FY03 MICECP recruited a record 85 new employees; however, it lost 28 employees.

Army Attaché Management (U//~~FOUO~~) As of FY03, there were 52 Warrant Officer billets: 47 OCONUS billets in 44 Defense Attaché Offices and 7 CONUS billets. There were 100 NCO billets in 88 Defense Attaché Offices. DIA intends on establishing billets in Afghanistan, Iraq, and Mauritania during the upcoming FY04.

(b)(7)(E)

Organizational Inspection Program (U//~~FOUO~~) In September of 2002 INSCOM signed an inspection memorandum, mandating an evaluation of the INSCOM Organizational Inspections Program (OIP) from Major Subordinate Commands to separate detachments. The Office of the Inspector General, in compliance with Army regulations oversaw the OIP. When staff inspections did not include appropriate coverage IG Special Inspections reviewed a number of topics of particular interest to the Commanding General (CG) and Department of the Army Inspector General (DAIG): Article 15 processing, OER/NCOER processing, personnel counseling, US Army Homosexual Conduct Policy understanding, Government Credit Card Program management, and US Army Voting Assistance Program. Inspections frequently incorporated sensing sessions as well. In 32 inspections at 27 locations, OIG prepared 19 written reports, which recommended corrective actions for a total of 44 findings—violations of law, regulation, or policy--and 51 observations—recommendations to the inspected unit for increased effectiveness and efficiency.

(U//~~FOUO~~) One year later, September of 2003, the INSCOM IG briefed the CG and MSC Commanders of the summary results of the FY03 special inspection of the OIP. Among a long list of deficiencies, the IG made some critical remarks: Major Subordinated Commanders lacked understanding of the OIP; OIPs were not always

conducted; Commanders did not always participate in the OIP as required in AR 1-201; most MSCs did not have plans of follow up.

Force Protection in South Korea (U//~~FOUO~~) Demonstrations in South Korea over the presence of US troops have been on the rise since 1997. Almost daily protests have aroused concerns in the Army leadership about force protection as a few protestors have become violent. The 501st Military Intelligence Brigade naturally plays an important role in this matter and maintains vigilance over protest activities. The latest demonstrations follow a few trends related to events that have occurred recently. Four major themes of demonstration prevail: opposition to the Land Partnership Plan—ongoing demonstrations against overpass and family housing projects at Yongsan Garrison and host nation cost incurred for relocating Camp Hialeah; opposition to the war in Iraq; candlelight vigils for the death of two teenage girls struck by a military vehicle on 28 June 2002; and protests calling for the revision of the Status of Forces Agreement (SOFA). Several of the candlelight vigils have become aggressive and have provided a political platform for anti-US groups. The vigils increased after two US servicemen, who were charged with striking and killing two middle-school girls in an accident with an armored vehicle, were found not guilty in court-martial proceedings. Since the acquittal, hundreds of thousands of South Koreans have taken to the streets in protest, demanding revision of SOFA to give South Korea more leverage in judicial proceedings. A recurring strategy with the demonstrators has been to provoke reaction or overreaction with US Soldiers, thus capitalizing on the negative publicity.

(U//~~FOUO~~) Demonstrations did decrease, however, after the elections held on 19 December 2002 and with the coming of winter. A recent public poll indicated that thirty-two percent of South Koreans favor the expulsion of US military forces. The majority, composed of older citizens, still favor an American presence. The lull in demonstrations was only short lived as protests increased in the spring of 2003, brought on by warmer weather and the deployment of 700 South Korean Soldiers in support of OIF. Throughout FY03, the number of demonstrations has not declined; Force Protection Assessments report that Hanch'ongnyon, a leading protest group, declared October 2003 to be anti-US month.

CHAPTER THREE

INFORMATION AND SYSTEMS

DOCEX Suites (U//~~FOUO~~) The Modernization Division of the G3-FM evaluated Data Management Systems capabilities, and selected the Vredenburg High View Document Exploitation (DOCEX) Suite, a software collection, to solve immediate mission needs in support of OCONUS requirements. (b)(7)(E) In conjunction with the contributions in support of the Language and Speech Exploitation Resources (LASER), the DOCEX process has become a mainstream intelligence activity.

Information Dominance Center Portal (U//~~FOUO~~) The Intelligence Production Office continued to improve and refine the INSCOM IDC Portal to provide daily support in the global war against terrorism. Improvements include the CG read file and daily brief and Significant Activities Reports (SIGACTS) from the INSCOM MSCs. Furthermore, subscribers are able to post their own documents for intelligence collaboration and access restricted material with caveats.

Blue Force Tracking System (U//~~FOUO~~) The Global Command and Control System-Joint (GCCS) implemented a tracking and daily reporting system tailored to INSCOM requirements for SOUTHCOM. These two capabilities are in the process of being merged and reengineered to form the INSCOM Database Tracking System (IDTS). This implementation comes from the successful establishment of a feed from SOUTHCOM which enables INSCOM to view assets in the SOUTHCOM AOR.

(~~S//NF~~)

(b)(1)

(~~S//NF~~)

(b)(1)

(b)(1)

~~(S//NF)~~

(b)(1)

~~(S//NF)~~

(b)(1)

~~(TS/ /NF)~~

(b)(1)

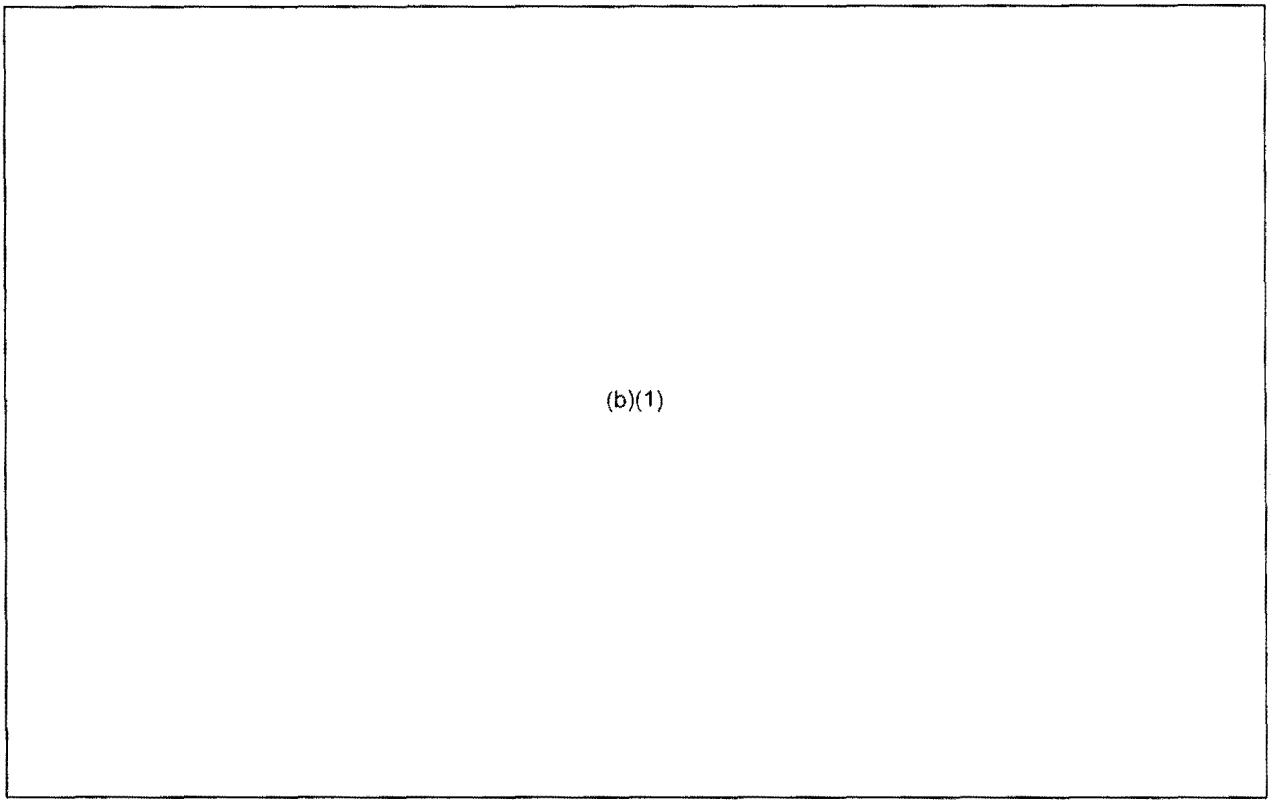
~~(TS/~~

(b)(1)(b)(3) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

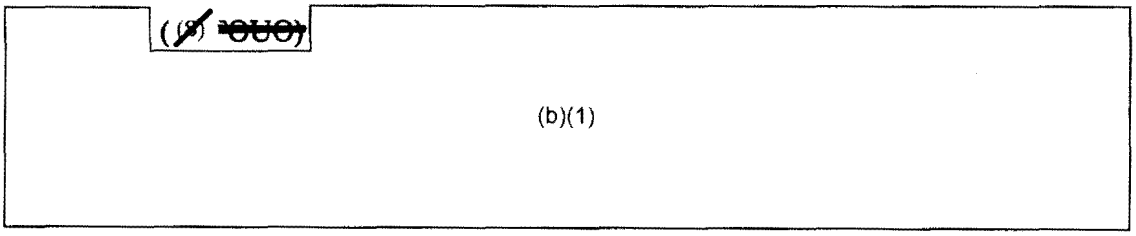
CFLCC has requested the deployment of four complete systems in April 2003. In May 2003 the training team arrived (b)(1)(b)(3) Per NSA and began training members at their respective locations. Altogether, the US Army has purchased ten systems for division MI use during OPLAN 1003V execution for fielding with MI units. The Kunia Regional Security Operations Center received a model, (b)(1)(b)(3) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

~~(S)~~

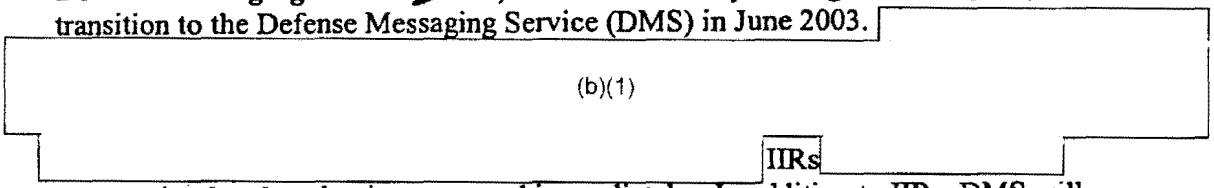
(b)(1)



Defense Travel System (U) The implementation of the Defense Travel System (DTS) was scheduled for FY03 at which time the Carlson Wagon Lite on site services would remain until a smooth transition was completed. The transfer during FYO3, however, was delayed due to difficulties in the system. INSCOM could not afford to drop the travel on site support and services due to command involvement in OIF and GWOT.



Defense Messaging Service ~~(S//NF)~~ The 500th Military Intelligence Group began its transition to the Defense Messaging Service (DMS) in June 2003.



IIRs retransmitted and evaluations returned immediately. In addition to IIRs, DMS will transmit Force Protection Reports (FPRs).

Army Records Information Management System (U//~~FOUO~~) In January of 2003, the INSCOM records management system had become obviously out of date. The records management POC, Ms. Patricia Dionne (G6), therefore, took the initiative by requesting from the Chief Information Officer an investigation into acquiring a new system. At first the paramount issue was finding a new system, since all could agree that the system required replacement. Debate over a choice out of a variety of systems as well as over implementation policies—a centralized or decentralized system—continued until such points were made academic by the promulgation in mid-April of Army regulation 25-400-2, which mandated the use of the Army Records Information Management System (ARIMS) for electronic records management. Following further debate, INSCOM settled the issue by implementing a centralized record system throughout the command. Although dissention remained, especially in the 902^{d} MI Group and G3 INSCOM, ARIMS was implemented.

Automation Upgrades in the Central Clearance Facility (U//~~FOUO~~) The Central Clearance Facility (CCF) underwent extraordinary changes in number and significance during FY03. In addition to its transferal from the PERSOM to INSCOM, the CCF implemented two automation upgrades in an attempt to provide more timely information on security clearances. The first initiative created an interface with the Army Contractor Verification System (ACAVS), eliminating delays in the contractor hiring process. The second initiative was a system that will send DA-873 and Green Mailer forms via e-mail to Army security managers, thus receiving instantaneous correspondence.

(U//~~FOUO~~) Such upgrades are more than timely as CCF is faced with an ever-growing backlog of clearance applications caused by the great need for intelligence in the GWOT. Fourteen Soldiers assigned to the 742nd MI Battalion of the 704th MI Brigade, for example, came without a valid Top Secret (TS) clearance/Single Scope Background Investigation (TS/SSBI). A considerable amount of time and intelligence is lost to the NSA while Soldiers, who are qualified in essential positions, await a TS/SSBI clearance, which currently requires twelve to eighteen months of processing. In this regard, the CCF has maintained representation in the Joint Personnel Adjudications System (JPAS), Program Management Office, and the Automated Continuing Evolution System (ACES), a related JPAS system. Despite all efforts, however, the CCF is unable to completely transition to JPAS because of a number of unresolved functional problems in the automation system. Only through continuing upgrades in automation and organization can the CCF hope to lessen the backlog of pending clearances, which affects not only Army employment but also the screening of contract linguists in the field. The limited number of adjudicators in all functions has resulted in an exigent search for accelerative improvements in the clearance system.

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 25-26

(b)(1)

(U//~~FOUO~~) To break the bottleneck, (b)(6) at INSCOM, and his staff at the have developed technologies and techniques that fuse databases by using IDC infrastructure. As (b)(6) (b)(6) said, "Data doesn't get better when it ages. The quicker you get it out and understand it, the quicker it's actionable and useable." The first of three phases of (b)(7)(E) began in July of 2003 and will last until March of 2004. Successful technologies and procedures from the experiment have been identified and shared with other commands.

CHAPTER FIVE

THE GLOBAL WAR ON TERRORISM

Introduction

(U//~~FOUO~~) The Global War on Terrorism (GWOT) goes into its second full year as of the end of FY03. In October of 2001, the United States organized an international coalition to pursue the Al Qaeda terrorist organization around the world. In Operation ENDURING FREEDOM, United States and allied forces have eliminated Al Qaeda terrorists in the mountains of Afghanistan and the Abu Sayyaf Group terrorists in the Philippines. Yet, neither enemy is completely subdued. These efforts, however, have turned surviving members of these organizations into fugitives. At the same time, US and allied forces have organized a temporary government in Kabul, one that is facilitating a more stable regime and precludes the return of another Taliban. Bin Laden's Al Qaeda, nevertheless, remains a global organization, especially in Indonesia, Malaysia, the Philippines, Somolia, and Yemen.

(U//~~FOUO~~) Having completed the second year of the GWOT, INSCOM personnel have identified and succeeded in correcting a number of problems. A key problem made apparent from Operation ENDURING FREEDOM has been the lack of skilled translators. By funding and contracting nationals and developing new digital technologies, INSCOM is making every effort to lessen this deficiency. INSCOM personnel also experienced difficulties in intelligence sharing. By interfacing databases, (b)(6) Deputy Chief of Staff for Operations at INSCOM, has demonstrated that access to raw data, rather than just finished products, from other US Intelligence agencies can be disseminated; time-sensitive intelligence from national-level cryptologic assets was relayed to the front lines within minutes, saving countless American lives on the battlefield.

(U//~~FOUO~~) Although great successes came in collection such as the utilization of MASINT, new problems have emerged as byproducts. General Noonan has said that the army needs to improve data-mining, metatagging, automated link-node analysis, and database tools: "We are in danger of overloading commanders with data." He has also added that we could have used a better signal intelligence geo-location capability in Afghanistan. In the category of successes, he cited the RQ-1A Predator unmanned air vehicle, which is "working so well."

(U//~~FOUO~~) According to (b)(6) contributor historian for INSCOM to the Army's history of the GWOT and Operation IRAQI FREEDOM, "the Army's intelligence forces played unprecedented roles." The following is an excerpt from (b)(6) Historical Narrative of Operational Intelligence in Operation IRAQI FREEDOM in regard to the GWOT.

(U//~~FOUO~~) Intelligence organizations carried a large responsibility for antiterrorism and force protection missions worldwide, especially following the

terrorist attack on the USS *Cole* in October 2000. The dedication and hard work of Army soldiers, civilians, and contractors in the new environment allowed a rapid change of methods and procedures, to track a very difficult and nebulous target. The resources and attention given to the Army intelligence community made possible a historic contribution to Operation Iraqi Freedom.

(U//~~FOUO~~) The seamless integration of intelligence "from space to mud" represents years of effort. Before Operation Desert Storm, Army doctrine divided military intelligence into tactical intelligence at Echelons Corps and Below (ECB), and strategic intelligence at Echelons Above Corps (EAC), unfortunately called "Echelons Above Reality." By doctrine a corps contains approximately 75,000 soldiers in three divisions; echelons above this level were accused of being out of touch. National-level intelligence often did not make a difference in the field. Strategic analyses influenced the political decisions of the Congress and President, but the intelligence data could not save lives when it was needed because it came too late.

(U//~~FOUO~~) This had changed by the twenty-first century. The Army Intelligence and Security Command leadership reduced cultural barriers between strategic and tactical levels, but even more important were technological breakthroughs.

(b)(7)(E)

The Army's communications achievement allowed real-time reachback for national intelligence, pushed from sources across the globe to troops in the field.

Operation Enduring Freedom and the Global War on Terrorism, which formed the context for Operation Iraqi Freedom, raised the profile and capabilities of the Army's intelligence forces to a new level. Antiterrorism missions fell largely to intelligence organizations. After the suicide attack on the USS *Cole* on 12 October 2000, preventing terrorism became the number one priority of the Army Intelligence and Security Command (INSCOM). Intelligence was sought out by commanders, who demanded agility, flexibility, and worldwide situational awareness. Intelligence organizations also received the necessary resources from the Department of the Army, the Department of Defense, and the U.S. Congress. The leaders of Army intelligence commands were able to implement the developments and programs they had long thought necessary, particularly in upgrading technological equipment and access to databases. The September 11 attacks on the World Trade Center and Pentagon, and the subsequent Operation Enduring Freedom, raised the operation tempo as intelligence commands balanced counterterrorism operations in Afghanistan, the Philippines, central and southern Europe, the Balkans, and the United States, as well as continued support to Korea. The rapid pace, with accompanying rapid progress and change, was carried right into Operation Iraqi Freedom.

(U//~~FOUO~~) To prosecute the global fight against terror, in February 2001 the Army Chief of Staff, General Eric Shinseki, charged Major General Keith Alexander, the incoming Army Intelligence and Security Commander, with moving Army intelligence out in front of developing terrorist threats. International terrorists ignore the military's traditional division of the world into theaters and commands; the Army needed a single command to leverage military intelligence from around the world and from across the intelligence disciplines. Beginning in August 2001, the Information Dominance Center began to fuse signals intelligence, focused on terrorist activity, with open-source intelligence, MASINT, and imagery on known terrorists and their associates. General Alexander led INSCOM further to experiment with new ways to create and display intelligence information. This venture was made possible by activating reservists and employing Defense Advanced Research Projects Agency scientists. The Intelligence Operations Center, created at INSCOM Headquarters in November 2002, drew upon the work of strategic intelligence brigades assigned to Central Asia, Europe, and the Pacific, combining all-source intelligence to better focus and target the collection and interpretation of signals intelligence around the globe. This allowed a real synergy of intelligence analysis, disseminated out to the INSCOM brigades through Information Dominance Center extensions. In 1993 Major General Paul Menoher had established a new slogan in the Army Intelligence and Security Command: "When one INSCOM soldier deploys, all of INSCOM follows." By 2002, for the first time, advances in communications technology made this a reality. INSCOM also worked to break down the traditional barriers among the national intelligence organizations at the Defense Intelligence Agency, Central Intelligence Agency, Federal Bureau of Investigations, and National Security Agency, using liaisons to share intelligence and leverage all-source analytical support. These extensive communications pipelines and relationships would themselves prove invaluable conduits of intelligence.

(U//FOUO) The Reserves and National Guard were absolutely necessary to meet the added demands on Army intelligence. These forces were designed to provide a strategic reserve to support the United States in its time of need. The threat of international terrorism was such a time. Mobilized under Operations Enduring Freedom and Noble Eagle, reservists accomplished all kinds of missions, providing nearly half the 513th MI Brigade's operational strength and backing up an extended operations tempo in many locations. Reservists filled some of the highest levels of military intelligence command, as Major General Alfonso Gilley served as the Deputy G-2 for Intelligence on the Army Staff, and Brigadier General George Fay served as Deputy Commanding General of the Army Intelligence and Security Command. Reservists from all kinds of units also provided security at the Pentagon and at major Army installations. The variety of call-ups demanded new levels of administrative support from reserve and active duty commands.

(U//FOUO) The Global War on Terrorism has demanded a truly worldwide intelligence effort, drawing upon soldiers around the world. The 513th MI Brigade split its attention between the Central Command Theater (Southwest and Central Asia) and Southern Command (South America). Pending the reactivation of the 470th MI Group, which will support the South American theater, the 204th MI Battalion deployed its Aerial Reconnaissance-

Low (ARL) Platform in Colombia. The 66th MI Group, which was disbanded as a brigade in 1995 and stood up from provisional status in late 2002, maintained its support to task forces in Bosnia and Kosovo, while reorganizing its Analysis and Control Element to support operations in Turkey and northern Iraq. The 116th MI Group made significant contributions to the Global War on Terrorism in a direct support role from its location in the United States. Even the 500th MI Group in Japan became involved in the conflict in Iraq, while providing ongoing counterterrorism support in the Philippines, Indonesia, Malaysia, and Thailand. The 500th deployed individual intelligence soldiers and teams from Hawaii to Afghanistan, Uzbekistan, and Kuwait.

(U//~~FOUO~~) Videoconferences also supported the Global War on Terrorism, as the INSCOM commander held biweekly conferences with his major subordinate intelligence commands in Germany, Japan, Korea, and across the United States. Such communications proved an excellent means of tracking international terrorist activity and coordinating resources across the globe.

(U//~~FOUO~~) The successes to date are due to the judicious and coordinated use of the full range US national power and the instruments put in place to utilize that power to its fullest potential. The US Army Intelligence and Security Command is one such instrument. In a speech delivered on 26 September, President George W. Bush cited the vital role intelligence would play in the coming struggle. INSCOM—a member of the intelligence community and a part of the US Army—is, by any measure, one of the key players in this intelligence war.

OPERATION ENDURING FREEDOM—Afghanistan

(~~S//NF~~)

(b)(1)(b)(3) Per NSA,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(~~S~~)

(b)(1)

(~~S//NOFORN~~)

(b)(1)

(b)(1)

513th Military Intelligence Brigade in support of CENTCOM (~~S~~ ~~OUO~~) In November 2002, the 202nd MI Battalion, 513th Military Intelligence Brigade, deployed

(b)(7)(E)

(b)(1)

OPERATION ENDURING FREEDOM

(b) (1) Per NSA,(b)(3):18 U.S.C. 798, (b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(~~TS~~//[ ]//~~NF~~) (b)(1)(b)(3) Per NSA

the 115th MI Group

The KRSOC informed the Joint Special Operations Task Force (b)(1)(b)(3) Per NSA

KRSOC accepted the counterterrorism mission during FY03 and were able to complete transfers and training for the mission within two months.

The War on Terrorism throughout the World

Global War on Terrorism Medals (U) By Executive Order 13289 dated 12 March 2003, the President has established two new medals for service in the Global War on Terrorism (GWOT): the Global War on Terrorism Expeditionary Medal and the Global War on Terrorism Service Medal. The two medals are awarded to recognize all members of US armed forces serving in or in support of the GWOT operations after 11 September 2001.

IDC-E Fielding (~~S~~)

(b)(1)

(b)(1)

Intelligence Assessments (U) ~~(S)~~ The Intelligence Operations Center produced 52 Intelligence Assessments on detainees who were nominated for the Transfer Review Board. The assessment outlines the detainee's prior activities (regardless of source) for the purpose of determining potential crimes and in turn deciding whether the detainee should be released to his country of origin or remain in US custody to stand for section 2—Crimes and Elements for Trials by Military Commission—of the Military Commission's Instructions.

Emergency Operations Center (U) ~~(S//NF)~~ The S3 Current Operations section of the 902d MI Group established an Emergency Operations Center (EOC) as a 24-hour operation, which functioned as the Group's main point of contact for incoming and outgoing information related to OIF and the GWOT.

(b)(7)(E)

1st IO Command (U~~//FOUO~~) As of 13 May 03, the 1st IO Command had 71 personnel deployed in support of Operation IRAQI FREEDOM and 13 personnel deployed in support of Operation ENDURING FREEDOM. Deployed personnel consisted of Field Support, CNO and VA Divisions' soldiers, civilians, and contractors. The four Field Support Teams supporting operations in Iraq and Afghanistan have completed relief in place with new personnel as of Sep 03.

(b)(7)(E)

Counterintelligence as Counter Terrorism

Counterintelligence/Human Intelligence Activities Division (CHS) (S) CHS Operations Support as part of the G3 supported many critical and sensitive Army missions worldwide and worked to establish new operational capabilities.

(b)(1)

(S//NF)

(b)(1)

(b)(1)

Task Force Language Vigilance (~~C/NF~~) Part of the 308th MI Battalion, a contingent of reserve Counterintelligence Agents mobilized for one year in Task Force Language Vigilance (TFLV). TFLV has screened in FY03 in support of GWOT and OIF

(b)(1)

902d Military Intelligence Group Investigations (~~S~~) The 902d MI Group produced a (b)(7)(E) reports during FY03 and conducted counterintelligence/ counterterrorism investigations at a volume not seen in ten years.

(b)(1)

(~~S//NF~~)

(b)(1)

(~~S//NF~~)

(b)(1)

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

5 USC 552 (b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 35

Department of Defense Counterintelligence Award (U) An award sponsored by the Counterintelligence Field Activity (CIFA), which recognizes an individual for one of nine categories, was given (b)(6) This year, due to the Global War on Terrorism, the award sponsors added the category of intelligence sharing (collaboration). Individuals are nominated by all CI agencies. CIFA then makes a selection. (b)(6) was nominated for sharing and analysis of law enforcement information with the intelligence community and reciprocating information with the law enforcement community. (b)(6) position, conceived as a result of the GWOT, is a USACIDC Special Agent whose duties include being a criminal analyst, liaison officer, and law enforcement officer.

CHAPTER SIX

OPERATION IRAQI FREEDOM

Introduction (U//~~FOUO~~) INSCOM, in support of the CENTCOM OPLAN 1003—the preparations for Operation Iraqi Freedom—developed its own OPLAN 1003V. The plan outlined what INSCOM would provide in support of CENTCOM and ARCENT. Many different subordinate organizations, in turn, developed their own individualized versions (b)(7)(E) which registered as smaller brushstrokes on the larger 1003 canvass. INSCOM G3, for instance, produced annexes to the INSCOM plan, which describe how INSCOM would employ and control assets in conducting operations for ARCENT.

(U//~~FOUO~~) The following is an excerpt from (b)(6) Historical Narrative of Operational Intelligence in Operation IRAQI FREEDOM.

(U) *Introduction*

(U//~~FOUO~~) In Operation Iraqi Freedom, military intelligence went beyond its traditional role as a force multiplier. Intelligence shaped the battlefield, dominated the enemy, opened possibilities for the coalition forces, and guided every step of the campaign. New applications of intelligerice validated the ongoing transformation of the U.S. Army. America's Army has undergone revolutionary changes since Operation Desert Storm in 1991, and continues along the same path. In the goals of the Force XXI modernization program of the 1990s, military intelligence in the 21st century would leverage every offensive capability of the Army on the battlefield. This was proven true in Iraq. With well-coordinated joint operations, the Army fought smart and fast, with devastating effect on enemy targets and remarkable success in preserving life. Intelligence was crucial to force protection, saving civilian infrastructure, and identifying and destroying the Iraqi regime's center of gravity.

(U//~~FOUO~~) Intelligence remains a key advantage of the American military over its enemies, as the United States faces new threats in an uncertain world.....Military Intelligence is the third largest branch, after Infantry and Artillery, for U.S. Army officers, comprising 7.5% of the officer corps. MI commissioned officers, warrant officers, and enlisted personnel together make up 4% of the Active Army. The second brigade deployed to Kuwait for Operation 1003V (Operation Iraqi Freedom) was the 513th MI Brigade, part of the Army Intelligence and Security Command (INSCOM). INSCOM, the Army's operational intelligence command, was able to bring strategic intelligence from around the world into theater for the ground commander and his subordinate U.S. Army, Marine, and coalition elements, as the 513th fell under the direct operational control of the Coalition Forces Land Component Command (CFLCC). The Army's strategic intelligence resources at the 902d MI Group (Counterintelligence) and National Ground Intelligence Center (Analysis and Production) were also directed to support operations in Iraq. Critical intelligence support came from the 116th MI Group at Ft. Gordon, Georgia; the 108th MI

Group at Bad Aibling Station, Germany, together with the 105th MI Battalion from the 66th MI Group; and the 704th MI Brigade at Ft. Meade, Maryland. The surge to 24-hour activity was supported by activating thousands of Reserve and National Guard soldiers; nearly half of the 513th MI Brigade's deployed strength came from the Reserve Component. Thanks to a variety of communications channels, commanders received critical, time-sensitive intelligence when it was needed on the ground.

(S) ~~FOUO~~ Army intelligence groups provided important groundwork for the United States' case to go to war against Iraq. In February 2003, Secretary of State Colin Powell went before the United Nations with four excerpts of Iraqi conversations which showed that Saddam's regime was thwarting the work of United Nations weapons inspectors. Proof of the Iraqi regime's duplicity in readmitting the inspectors became a pillar of the argument to commit U.S. forces. Army intelligence demonstrated that it would be pointless to wait for inspectors to work into the summertime, without real Iraqi cooperation. This timely intelligence was gathered by [redacted] soldiers and civilians under Army command, all outstanding linguists and analysts, including [redacted] Army sergeants and [redacted] Presenting the intelligence before the world was a justified risk and directly answered urgent questions of national strategic policy.

(b) (1) Per NSA, (b)(3):50 U.S.C. 403,(b)(3):P.L. 8

(U//~~FOUO~~) This intelligence was garnered thanks to years of effort focused on Iraqi systems and the Iraqi dialects. Army cryptologists had developed a thorough understanding of Iraqi tactics and procedures over the years since Desert Storm. The concerted strategic intelligence focus would yield great dividends for the U.S. military. Army counterintelligence developed its efforts against Iraq from 1998, years before national agencies launched a coordinated program. Operational intelligence collectors and analysts accompanied the first special operations forces entering Iraq, supported by signals intelligence from the United States. Intelligence assets were committed much earlier than the main combat forces, and the demands on Army intelligence would rapidly increase with American commitment to this theater.

(U//~~FOUO~~) The integration of Reserve forces into Operation Iraqi Freedom missions went much more smoothly than in Operation Desert Storm. The "Total Army" concept, developed in the 1990s, broke down some of the traditional cultural prejudices between the active and reserve forces. Reserve units trained with their "wartrace" active duty commands, who would command them in a conflict. The Army also created "multicomponent" battalions and brigades comprised of both reserve and active forces. In 2001, the Army Intelligence and Security Command made the 203^{d} MI Battalion at Aberdeen Proving Ground, Maryland, the first MI unit structured with active and reserve soldiers. This battalion carried the Army's technical intelligence mission of analyzing and exploiting enemy materiel. The reserve assets brought enormous depth and personal potential to bear. Several specialized intelligence detachments trained where they worked full-time, as chemists, computer consultants, or intelligence analysts. Other intelligence reserve soldiers included business executives, lawyers, university professors, engineers, and others with advanced professional and doctoral degrees. Even with a rank of junior sergeant, some of these men and women brought the experience of senior warrant officers.

(U//~~FOUO~~) By spring of 2003, from the pool of available Reserve Component soldiers qualified in their military occupational specialty, a remarkable 98% of the Army Reserve unit intelligence soldiers and 45% of the National Guard intelligence soldiers had been called to active duty. Reservists had been activated for six months for Desert Storm and nine months for the Bosnian conflict, and were now called for one or two years. These demands strained the capacity of the reserve and active duty commands, as soldiers' promotions were delayed and Defense Finance fell months behind in paying for soldiers' housing. Reserve and Guard units created family readiness groups to organize mutual support for the families left behind, many of whom faced economic hardship. Yet these challenges were met with the patriotic professionalism that characterizes the U.S. Army Reserve component's "citizen soldiers" and their dedicated families.

(U//~~FOUO~~) Reserve intelligence units mobilized from across the country to support Operation Iraqi Freedom. Army intelligence organizations across the United States relied upon reserve forces to complete their mission. The National Ground Intelligence Center mobilized all sixteen of its wartrace reserve analytic detachments from states across the country: Connecticut, Illinois, Maryland, New York, Ohio, Florida, Indiana, Vermont, Nebraska, and Kansas, including the Army's only chemical warfare intelligence detachment. Many reservists activated after September 11, 2001 for Operation Enduring Freedom stayed on duty a second year for Iraqi Freedom. The 116th MI Group activated reservists with linguistic and communications intelligence expertise, to support ongoing missions as active duty soldiers developed targets for Operation Enduring Freedom; the 902d MI Group (Counterintelligence) called twenty reservists to duty to support its command center and liaison activities, even as fifteen civilian employees were activated for reserve duty elsewhere. The 704th MI Brigade called upon an augmentation detachment to support the Army Technical Control and Analysis Element, strengthening the primary link between tactical warfighters and the National Security Agency and Central Security Service, for information superiority and full-spectrum signals intelligence support. The Headquarters, Army Intelligence and Security Command activated reservists to help stand up the Intelligence Operations Center, transforming INSCOM into a state-of-the-art operational headquarters. All these reservists worked to support non-stop operations during the fight, allowing Army intelligence organization to act with outstanding agility.

(U//~~FOUO~~) Despite calling upon the reserves, the Army did not have enough linguists proficient in regional languages to send into theater. As a strategic resource, the 116th MI Group prepared an invaluable course package in the Iraqi dialect of Arabic and shared it with all the U.S. military services for strategic intelligence collection. To move human assets forward into theater, the Army relied upon contract linguists, recruited through the Army Intelligence and Security Command. The 902d MI Group was responsible for screening applicants before Iraqi American citizens could be granted security clearances. These native Iraqi speakers were imbedded in the American Army and Marine units. They gave true patriotic service under difficult conditions to accomplish their mission. During the first week of fighting, following an Iraqi ambush on an

American unit, several soldiers' bodies were recovered from shallow graves, but one remained missing. The brigade commander ordered that his forces would not advance until the missing soldier was found. A contract linguist, on his own initiative, sought out all the children of the village and spoke with them until a child led him to the body. Shortly after this incident, Iraqis feigned surrender to American forces, then treacherously killed several Marines. Thereafter, Army contract linguists used loudspeakers to clearly instruct surrendering Iraqis on every movement as they disarmed themselves. This saved many Iraqi and American lives, bridging a linguistic gulf in which misunderstandings would prove deadly.

(U//~~FOUO~~) Other strategic intelligence groups balanced global priorities to give Operation Iraqi Freedom particular support. (b)(6) commander of the National Ground Intelligence Center, explained that they both reduced support to missions in other theaters, (b)(7)(E) Both turned to 24/7 operations to coordinate their organizations' efforts with needs in the theater of operations. The NGIC surged from its five analysts who normally concentrated on Iraq, to 100 analysts, later peaking at a total of 370 analysts dedicated to the Iraqi theater, to ensure a quick turnaround on all requests for information. By concentrating on Operation Iraqi Freedom, the NGIC (b)(7)(E) helped make the conflict shorter with timely and accurate intelligence support.

In December 2002, the Army Intelligence and Security Commander, Major General Keith Alexander, traveled to Kuwait to meet with Lieutenant General David McKiernan, the Coalition Forces Land Component Commander (CFLCC). General Alexander offered INSCOM's assets to the ground forces commander; General McKiernan responded that his greatest intelligence shortfalls related to Sensitive Site Exploitation and personality databases. The Defense Intelligence Agency had prepared intelligence packets as the framework for searching several dozen of the most prominent Iraqi sites related to Weapons of Mass Destruction (WMD), but the preparatory work for hundreds of other sites was unfinished. The 75th Exploitation Task Force, created from the 75th Field Artillery Brigade with the help of the 513th MI Brigade, needed detailed intelligence on how to approach each location, and what to stabilize in the area. Timely intelligence work on personalities was also necessary to identify the thousands of scientists, commanders, and politicians connected to weapons programs and Baath party war crimes, beyond the notorious 55 people portrayed on the Defense Intelligence Agency's deck of cards. Creating the necessary intelligence packets became the first test of the newly created INSCOM Intelligence Operations Center. In three months, the Center put together nearly six hundred individual target folders on suspect sites, and files on seven hundred individuals, in direct support of the Coalition Forces Land Component Commander, the exploitation task force, and its successor, the Iraq Survey Group.

(U//~~FOUO~~) Strategic intelligence blurred with tactical intelligence as the Army's combat roles expanded. In the Cold War paradigm, American battalions and brigades fought against enemy formations of similar size. (b)(7)(E)

who focused on political, economic, and cultural factors, detached from the perspective of soldiers on the ground. But with the collapse of the Communist bloc, battlefields became more complex and nuanced, requiring more sophisticated intelligence. In 2001, Army doctrine changed the focus to "METT-TC," adding Civilian Considerations to the concerns of commanders at every level. All Army combat units must consider civilian casualties and collateral damage when planning their missions, understanding that the attitudes and sensitivities of civilian authorities and local groups may make the difference between the success or failure of American policy. Specialized national intelligence, made available to the "tip of the spear," leveraged America's technological capabilities in support of rapidly changing missions.

(U//~~FOUO~~) (b)(7)(E) *bridges gap*

(U//~~FOUO~~) Communications were the key to bridging the gulf between national-level strategic intelligence and tactical units who could apply intelligence immediately. In Operation Desert Storm, even as the 513th MI Brigade's deployment in Saudi Arabia was delayed into December 1990, outside the theater the Army's strategic debriefers could gather human intelligence, and communications field stations could provide signals intelligence, on the Iraqi target. INSCOM's (b)(7)(E) mobile satellite terminals proved critical as a dedicated conduit for timely intelligence to combat forces. The seamless architecture practiced by Army intelligence in Desert Storm included imagery products of Iraqi positions sent from the Army's production agency in Washington, D.C., within hours through (b)(7)(E) satellite systems to commanders on the ground. In the battle for the Rumailah oilfields west of Basra in March 1991, the 24th Infantry Division commander reported that U.S. Army intelligence on the Iraqi Republican Guard was so accurate that he held his forces out of range and destroyed Iraqi artillery based on imagery intelligence received from across the Atlantic Ocean.

(U) *Contrast to old methods*

(U//~~FOUO~~) This timely strategic analysis contrasted with the Army's previous capabilities. Some did not trust the new computers, doubting they would withstand the rigors of a real-world battlefield. The VII Corps Commander in Desert Storm, Lieutenant General Frederick Franks Jr., relied upon his staff to mark acetate map overlays with a grease pencil. To meet this requirement for hard copy publications, the Army Intelligence Agency printed map overlays of Iraqi doctrinal force disposition in Washington D.C. and flew them across the ocean to the theater operations center in Saudi Arabia. When a satellite connection was established, the Third Army G-2, Brigadier General John Stewart, arranged for the templates to be published and disseminated in hard copy by courier in theater. Intelligence was thus distributed more quickly, but commanders still relied upon analysts to mark maps by hand.

(~~S~~//~~FOUO~~) Yet the success of Trojan satellite communications proved that the Information Age had reached the battlefield. All kinds of intelligence could be moved quickly and reliably in digital format to warfighters on the move. Two achievements helped establish a new mindset: timely, useful tactical

intelligence arrived from outside of theater, and tactical computers were proven reliable.

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

For the first time, INSCOM had become the Intelligence Command for all of the Army.

(U) *Development of Intelligence on Iraq*

(U//~~FOUO~~) Like much of the U.S. Army, the intelligence community had concentrated on the Warsaw Pact rather the Iraqi theater before 1990. The situation would be completely different for Operation Iraqi Freedom. Army intelligence organizations would bring more than a decade of special experience to bear. With the drawdown of Army forces in Europe, the 513th MI Brigade was reconfigured as a force projection strategic intelligence brigade, comprised of Signals Intelligence (201st MI), Counterintelligence and Human Intelligence (202d MI), Aerial Reconnaissance (204th MI), and All-source Intelligence (297th MI) Battalions. The 513th Brigade deployed elements to South America in support of counterdrug and counterterrorism operations, also retaining a special mission to support the Army Central Command, for whom Iraq remained the major threat. Other national Army organizations also developed the intelligence picture of Iraq. The Army Intelligence Agency fell under INSCOM command in 1991, and was reorganized with two elements combining to form the National Ground Intelligence Center (NGIC), the Army's all-source analysis production center, in 1994. In June 2001, shortly before the tragedies of September 11, the NGIC moved into a new, state-of-the art facility in Charlottesville, Virginia. Another premier Army asset was the 116th MI Group, created in 1994 at Ft. Gordon, Georgia. The 116th would become a major intelligence resource, providing significant support for the Army and the other armed services operating in Iraq, together with a strategic Army intelligence group at Bad Aibling, Germany, and an Army battalion at Menwith Hill, England. The 116th was recognized with the National Intelligence Meritorious Unit Citation in 1998 and 2000. Army groups would win the National Security Agency's Travis Trophy for the most significant contributions to the Department of Defense in 1991, 1995, 1997, 1998, 1999, and also 2002, for outstanding support to Operation Enduring Freedom.

(U) *New intelligence disciplines*

(U//~~FOUO~~) The traditional intelligence disciplines of Human Intelligence, Signals Intelligence, and Imagery Intelligence were supplemented by new technological developments in the 1990s, most notably Measurement and Signature Intelligence (MASINT). MASINT emerged from research and development to become a lucrative source of timely intelligence reports. The flexibility of MASINT technology allows the monitoring of enemy electromagnetic emissions, radar signatures, and even the different sounds produced by vehicle engines. Like Signals Intelligence (SIGINT), MASINT yields intelligence that can be turned around within minutes to inform and guide commanders on the battlefield. After September 11, 2001, the Army pushed

national-level resources down to operational real-time applications, to counter threats in an unfamiliar environment.

(U) *Information Operations*

(U//~~FOUO~~) The Information Age produced new threats and new opportunities for the U.S. Army. With the burgeoning communications channels of broadcast media, cable and fiber networks, e-mail, and the Internet, the American military faces the challenges and possibilities of Information Operations. To enter this fast-changing arena, the Army Intelligence and Security Command created the Land Information Warfare Activity in 1994, under the operational control of the Army Staff G-3 for Operations. Based at Ft. Belvoir, Virginia, the organization received the mission of defending Army automated communications and data systems from outside intrusion, responding to any computer emergencies, and developing Army capabilities for offensive and defensive operations in any future conflict in cyberspace. The defensive mission quickly became a necessary consideration for all Army operations. A priority on civilian relations also demanded the participation of information operations in counter-propaganda, counter-deception, and civil affairs campaigns. Renamed the 1st Information Operations Command in October 2002, the group organized Field Support Teams to strengthen the defenses of Army systems around the world, leveraging the capabilities of the Information Dominance Center at INSCOM headquarters.

(U) *Linguists*

(U//~~FOUO~~) Despite calling upon the reserves, the Army did not have enough linguists proficient in regional languages to send into theater. As a strategic resource, the 116th MI Group prepared an invaluable course package in the Iraqi dialect of Arabic and shared it with all the U.S. military services for strategic intelligence collection. To move human assets forward into theater, the Army relied upon contract linguists, recruited through the Army Intelligence and Security Command. The 902d MI Group was responsible for screening applicants before Iraqi American citizens could be granted security clearances. These native Iraqi speakers were imbedded in the American Army and Marine units. They gave true patriotic service under difficult conditions to accomplish their mission. During the first week of fighting, following an Iraqi ambush on an American unit, several soldiers' bodies were recovered from shallow graves, but one remained missing. The brigade commander ordered that his forces would not advance until the missing soldier was found. A contract linguist, on his own initiative, sought out all the children of the village and spoke with them until a child led him to the body. Shortly after this incident, Iraqis feigned surrender to American forces, then treacherously killed several Marines. Thereafter, Army contract linguists used loudspeakers to clearly instruct surrendering Iraqis on every movement as they disarmed themselves. This saved many Iraqi and American lives, bridging a linguistic gulf in which misunderstandings would prove deadly.

(U) *Drawing upon MI soldiers worldwide and Videoteleconferences (VTC): A key coordination tool*

(U//~~FOUO~~) A technological development which greatly improved the coordination, resourcing, and planning of force projection was the secure videoteleconference (VTC) system, (b)(7)(E) The VTC gives participants the illusion of being in the same room together, even as commanders forward, their rear detachment commanders, their support commanders, and Department of the Army representatives, meet with their staffs at widely dispersed locations.

(b)(7)(E)

The commanders of warfighters in theater and reachback support organizations elsewhere could clearly explain and understand emerging requirements, opportunities, and limitations.

(U//~~FOUO~~) During Operation Iraqi Freedom VTCs also boosted troops' morale. The special "morale telephone calls" to home, a feature of Operation Desert Storm for the 513th MI Brigade, were replaced by ten-minute family videoconferences between Kuwait and Ft. Gordon, Georgia, beginning with the holiday season of December 2002.

(b)(7)(E)

(U) *Support to ground forces*

(S)

(b) (1) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(U) *Counterintelligence*

(U//~~FOUO~~) In addition to directly supporting ground combat operations, Army intelligence operations shaped the battlespace on many levels. The Army Intelligence and Security Command executed offensive counterespionage operations to great effect, in direct support of the theater commander, General Tommy Franks, and his attack plans for the Iraqi campaign.

(b)(7)(E)

(U) *Information Operations*

(U//~~FOUO~~) Information Operations also benefited from well-planned, synergistic operations. The 1st Information Operations Commander, (b)(6) (b)(6) agreed with the Army Signals Command to join efforts with Army Network Operations, as well as with counterintelligence and criminal investigations divisions, for a united effort.

(b)(7)(E)

The resulting lack of communication and coordination between the Iraqi units led directly to the rapid collapse of resistance in Baghdad, without the dreaded house to house fighting long feared before the war began.

(U) *Analysis Center - JACE*

(U//~~FOUO~~) Ground intelligence in theater was coordinated by the central Joint Analytical Control Element (JACE), attached to the ground forces command center. The JACE fuses the intelligence in theater into a coherent picture, supports the commander's priority intelligence requirements, and tasks intelligence collection management. Commanded by the 297th MI Battalion, the center relied upon national-level intelligence and support from the United States, and itself processed intelligence from aerial drones for immediate action and

battlefield awareness. The Army's Hunter Unmanned Aerial Vehicle (UAV) system performed superbly in its intelligence missions. Company A, 224th Aviation Battalion could launch a Hunter within two hours of a request, and up to four imagery feeds from four UAVs could stream simultaneously into the JACE in real time, for analysis and immediate targeting. For the first time, UAVs supported intelligence requirements down to the combat brigade level.

(U//~~FOUO~~) The focused success of the JACE in meeting unprecedented requirements owed much to the training and professionalism of the 345th MI Battalion, mobilized from the Reserves for a second year after providing excellent analytical support to operations in Afghanistan. Soldiers gained support from teamwork in the command climate between the 513th Brigade commander, (b)(6) who provided soldiers and support, and the staff of the Ground Forces C-2 Director of Intelligence, Major General James Marks, called into theater from his command of Ft. Huachuca, Arizona. Intelligence was communicated across the ocean to U.S. forces in Iraq at several levels: directly to the customer on the ground, through liaison officers, and also through the chain of command. This kept all echelons informed, without delaying time-sensitive intelligence when it was needed most. As (b)(6) G-2 of V Corps, stated, "It wasn't that everything has to go through me to get to them." If one headquarters was overwhelmed, this did not stop up the pipelines. The 3d Infantry and 101st Airborne Division Analysis and Control Elements turned directly to Headquarters, Army Intelligence and Security Command, for intelligence through the Global Command and Control System (GCCS) on Iraqi minefields, tunnels, and obstacles. With robust communications and a flexible liaison network, there was no fighting within the U.S. forces over who could eat from which "rice bowls" of intelligence.

(U) *Prisoners of war*

(U//~~FOUO~~) (b)(7)(E) Her liberation was an emotional turning point in the campaign, after several setbacks had slowed the American advance. Americans had hoped that the people of southern Iraq would welcome the coalition as liberators, but the Saddam Fedayeen paramilitaries had dispersed through the civilian populace, terrorizing them and attacking the U.S. Army and Marines with guerilla tactics.

(b)(7)(E) Rescuing American prisoners of war is always a top intelligence priority for American commanders, and intelligence units at all echelons immediately focused on the task.

(U//~~FOUO~~)

(b)(7)(E) Speaking through an Army contract linguist, the Marines asked him to return to the hospital in al-Nasiriyah, where his wife worked as a nurse, and draw

a sketch of the compound, the soldier's location, and where paramilitary troops were located. Hostage rescues are exceptionally dangerous, as hostages and their rescuers have often been killed in poorly planned and executed missions.

(b)(7)(E)

From its rear detachment in Ft. Gordon, Georgia, the 513th MI Brigade provided a map of power lines which could entangle the helicopters during the night-time rescue. The joint operation was executed flawlessly and without casualties.

(U) *Intelligence on Baghdad*

(U//~~FOUO~~) As Army and Marine forces closed in on Baghdad, they turned to an intelligence product completed months before the war began. The Imagery Analysis Division of the National Ground Intelligence Center had distributed a CD-ROM with virtual three-dimensional "fly-through" models of Baghdad and major Iraqi targets. This directly helped targeting by Army, Marine, and Air Force close air support and deep strike assets, as the terrain covered in this campaign was significantly different from Operation Desert Storm.

(U) *Joint Interrogation Facility*

(~~C~~) ~~FOUO~~) The coalition's mission to locate Iraqi Weapons of Mass Destruction (WMD) was carried out by a team effort, including the (b)(1) (b)(1) the Defense Intelligence Agency, and Army strategic intelligence units on the ground.

(b)(7)(E)

Learning from experience in Afghanistan, the 902d MI Group sent computer forensics specialists to exploit captured hard drives and digital devices. Data mining search engines, developed by the National Ground Intelligence Center, continue to support the enormous analytical efforts necessary in dissecting the regime of Saddam Hussein. Under 513th MI Brigade command, these capabilities of the interrogation and document exploitation facilities were integrated into the Intelligence Exploitation Base at Camp Udairi, Kuwait. Combined with the 75th Exploitation Task Force, the base would become the launch pad for Sensitive Site Exploitation operations to pursue Iraqi war criminals, investigate Iraqi chemical and biological weapons programs, and recover coalition Gulf War POWs.

(U//~~FOUO~~) The 513th MI Brigade also established two other interrogation sites. A team from the Joint Interrogation Facility traveled northward in Iraq with the 205th MI Brigade of V Corps, then established the

first interrogation facility in Baghdad. The team began interrogating high-value detainees at the Baghdad International Airport in mid-April. (b)(7)(E) The interrogation team interrogated thousands of Enemy Prisoners of War and civilian detainees throughout the campaign.

(U) *Returning soldiers*

(U//~~FOUO~~) All eight of the returning American prisoners of war were debriefed by soldiers of the 513th MI Brigade and 902d MI Group for counterespionage and counterintelligence collection. Before the war, soldiers from the 902d had also trained the six soldiers later captured from the 507th Maintenance Company on how to resist anti-American espionage, as part of a training program for thirty thousand soldiers going into theater.

(U) *Success*

(U//~~FOUO~~) The most feared possibilities from war in Iraq, such as prolonged fighting into the summertime, heavy coalition casualties, and another disastrous terrorist strike on the United States, were all averted in Operation Iraqi Freedom. Army intelligence, in a team effort with the national intelligence agencies, helped guide American power and thwart enemy initiatives with tremendous success. (b)(7)(E) allowed the U.S. military to target the Iraqi regime to devastating effect, while preserving the coalition forces and innocent civilians.

(U) *Counterintelligence*

(U//~~FOUO~~) Quiet successes in counterintelligence prevented many nightmares. Continued intelligence support to the interrogations of al-Qaeda operatives at Guantanamo Bay helped to block ongoing terrorist operations. Careful technical countermeasures and information operations protected Army and joint communications systems during Operation Iraqi Freedom. Force protection in Iraq's enormous rear area was supported by the 202d MI Battalion, and the 308th MI Battalion of the 902d MI Group worked against terrorism in the United States. With liaison officers in more than fifty field stations of the Federal Bureau of Investigation, Army soldiers gathered timely intelligence to support operations in Iraq and to oppose terrorist activities against the Army worldwide. As an illustration of the intelligence collaboration practiced by the 116th MI Group, National Ground Intelligence Center, INSCOM, and other commands, a terrorism analyst from the Army Criminal Investigations Division, Chief Mauro Orcesi, won the Department of Defense Counterintelligence Award

in 2002 for his liaison work at the 902d MI Group. By working with other services and combining intelligence disciplines, Army intelligence is reducing the risks of intelligence gaps and failures, to protect the United States from future terrorist disasters.

(U) *Intelligence in the future*

(U//~~FOUO~~) Like Desert Storm, Operation Iraqi Freedom revealed enormous advances in a seamless intelligence architecture, which moved national-level intelligence down to the tactical warfighter. Yet Iraqi Freedom was not simply the first Gulf War fought a second time. The Army has rapidly adapted to face changing threats in a creative way. The future of Army intelligence lies with a single intelligence system for all echelons, featured as a centerpiece of Army transformation. Originally planned for implementation in 2012, the Common Ground System will be implemented much sooner, to link together operations centers and knowledge centers from around the world. For example, the Army and Air Force's Joint Surveillance Target Attack Radar System (JSTARS), pioneered in Desert Storm, proved even more effective in Iraqi Freedom, as its intelligence products went directly to operations centers and combat brigades. By pooling resources and developing automated tools, Army intelligence will process and analyze an unprecedented amount of information, allowing even greater effectiveness on the battlefield.

(U//~~FOUO~~) The accomplishments of Operation Iraqi Freedom demonstrate that the U.S. Army will continue to fulfill its mission of defending the United States with intelligence, courage, and total dedication.

(U)

513th MI Brigade Deployment to Kuwait (~~S~~) On 18 October 2002, 513th Military Intelligence Brigade received an order from CFLCC to deploy in Kuwait. Movement for the brigade commenced on 22 October and continued with airlifts into November. The brigade command sergeant major carried the colors into Kuwait on 13 November 2002. All brigade functions formally transferred to Kuwait on 24 November with only a rear detachment at Fort Gordon, GA.

(U) The following is an excerpt from (b)(6) Historical Narrative of Operational Intelligence in Operation IRAQI FREEDOM.

(U//~~FOUO~~) To streamline the intelligence footprint forward, the 513th MI Brigade commander, (b)(6) successfully executed split-based operations. Long practiced in exercises with varying degrees of success, the idea of relying on transatlantic support was finally validated in Operation Iraqi Freedom. With the support and coordination of higher headquarters, elements of the 513th Brigade headquarters and its subordinate 201st MI, 202d MI, and 297th MI Battalions remained at home station in Ft. Gordon, Georgia, as the main body of the brigade deployed to Camp Doha, Kuwait, in November 2002. Because much MI equipment relies upon emerging technology, which develops at a faster pace than the Department of Defense acquisitions process, fielding "nonstandard" equipment sometimes creates logistical difficulties. Assets in the United States face fewer limitations, and the National Ground Intelligence Center and 116th MI Group quickly adapted to "Doha time," analyzing intelligence and

communicating with theater in a united battle rhythm. These units sent massive amounts of intelligence through secure network chat sessions, file transfers, and internet portals to Army commands in theater. The door for communications was finally wide open.

(~~S~~ ~~FOUO~~) The brigade's early deployment, months before the movement of major combat elements, helped resolve one of the shortfalls of Operation Desert Storm. Priority for movement had gone to combatant units, so strategic intelligence units had arrived in theater only weeks before the campaign began. In the fall of 2002, the Coalition Forces Land Component Command wisely allowed the 513th MI Brigade to posture itself in theater for pending intelligence operations, which paid decisive dividends throughout the preparations and execution of Operation Iraqi Freedom. Each MI battalion fulfilled its missions with outstanding success. The 297th MI Battalion's Joint Analysis Control Element (JACE) integrated personnel from sister services, other operational intelligence units, national agencies, and coalition partners, in the theater's premiere intelligence fusion center. The 201st MI Battalion established a (b)(1) furnishing essential intelligence. The battalion's powerful technological capabilities allowed it to conduct (b)(1) operations in support of American forces in Iraq and Afghanistan simultaneously. The 202d MI Battalion reinforced counterintelligence operations in southwest Asia, providing critical support to force protection throughout the theater of operations.

(U//~~FOUO~~) More than a thousand of the 513th MI Brigade's deployed strength of 2,200 soldiers and civilians came from reserve components, including the multicomponent 203d MI Battalion (Technical Intelligence); the 142d MI and most of the 141st MI Battalions (Linguist) from the Utah National Guard; the 221st MI Battalion (Theater Operations) from Atlanta, Georgia; the 323d MI Battalion (Theater Exploitation), from Ft. Meade, Maryland; the 415th MI Battalion (Linguist), from Baton Rouge, Louisiana; elements of the 331st MI Company (Imagery and Analysis) from Staten Island, New York; and the 306th MI Company (Linguist) from Ft. Sheridan, Illinois. The 345th MI Battalion (Operations) from Augusta, Georgia, was mobilized in October 2001 to support the Army Central Command's Joint Analytical Control Element (JACE) in Georgia during the major fighting in Afghanistan. The battalion was due for demobilization in October 2002, but the 513th Brigade Commander, Colonel Jon Jones, and the theater J-2 for intelligence, Brigadier General John Kimmons, decided that this intelligence unit was essential if Central Command were to stage another major effort in Iraq. The 345th was involuntarily extended for a second year, and deployed to Kuwait in December 2002. Many of these soldiers, together with soldiers from the 306th and 331st MI Companies, had already volunteered for an additional year. Reservists and Guardsmen were also among the five hundred soldiers and civilians of the 513th MI Brigade supporting operations in Iraq from Ft. Gordon, Georgia.

513th Military Intelligence Brigade in support of CENTCOM (U//~~FOUO~~) The Delta Company of the 201st MI Battalion maintained a forward deployed Cryptologic Support Group (CSG) during FY03, providing support for Operations SOUTHERN WATCH, PEGASUS VENTURE, AND IRAQI FREEDOM. CSG also supports the Analysis and

Control Element of the 513th MI Brigade. Permanently deployed, the element increased the SIGINT single-source analytical capability. The majority of Delta Company's Soldiers maintained sanctuary operations at Fort Gordon in support of IRAQI FREEDOM.

(S) ~~FOUO~~ The 201st MI Battalion tasked 22 soldiers (b)(1) (b)(1) in support of IRAQI FREEDOM. 19 Soldiers participated in numerous activities in support of OIF. They filled analyst positions in (b)(1) Deployments decreased in size when in July the Reservists began to demobilize.

(S) ~~FOUO~~ The 202nd MI Battalion deployed to Kuwait to support OPLAN 1003V. The battalion provided HUMINT, CI, DOCEX, computer exploitation, and sensitive site exploitation to CENTCOM forces. The personnel assigned to the battalion swelled from a normal complement of 220 to over 700, including Active Duty, National Guard, Reserve, FBI, (b)(1) DIA, (b)(1) civilians and coalition forces. Ten CI teams were deployed: five in "Rear Area Operations" and five in direct support of V Corps. DOCEX in conjunction with the (b)(1) FBI, and DIA translated and exploited over seven tons of sensitive documents. CI Computer Exploitation (CITE) analyzed captured computer media. The battalion also contributed 40 Soldiers as part of the 75th Exploitation Task Force, a multidiscipline unit to provide linguistic debriefing, DOCEX, and force protection on over 158 sensitive sites. Exploited information led directly or indirectly in the capture of three of the 50 most wanted in Iraq, the destruction of over fifteen tons of captured weapons and munitions, examination of sites of war crimes, including Saddam Hospital in An Nasariya and the mass grave site outside Basra. Three Soldiers were awarded the Bronze Star.

(U//~~FOUO~~) The 297th MI Battalion, after returning from Kuwait and stationing in Fort Gordon for only five or six months, returned to Kuwait at the beginning of FY03. With soldiers integrated from the 345th MI Reserve Battalion, the 297th Battalion deployed 700 Soldiers to monitor Iraq and its preparations for war. The JSTARS Company deployed in Qatar for force protection in Jordan. During OIF UET analysts participated in the identification of oil fires in Southern Iraq. Following the fall of Baghdad, Soldiers of the 297th were some of the first to enter Baghdad International Airport as part of the CFLCC EECP. After an eight month deployment, Soldiers of the 297th began returning to Fort Gordon, leaving an Intelligence Support Element in support of peacekeeping operations in Iraq.

Troops from the 513th MI Brigade Return (U//~~FOUO~~) Nearly 100 Soldiers of the 201st and 297th Military Intelligence Battalions of the 513th MI Brigade, who had been deployed in Iraq and Kuwait for eight months, returned from Kuwait to Fort Gordon, GA on 21 May 2003 as the combat phase of Operation IRAQI FREEDOM came to a close.

Counterintelligence/Human Intelligence Activities (CHS) (S) (b)(1) (b)(1) Annex B (for the 513th MI Brigade)

to support CENTCOM (b)(1) (b)(1)

~~(S//NF)~~

(b) (1) Per NSA,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Special Programs Office ~~(S//NF)~~ Special Programs Office (SPO) personnel supported IRAQI FREEDOM by chairing a multi-agency crisis working group (b)(1) SPO, in conjunction with ACIC analysts, developed a new format for assessments for the purpose of providing "a better bottom-line picture." The new format has the approval of the US Army G2 and TMO.

Target Folders ~~(S)~~ The Intelligence Operations Center, as the operational center for the IDC, (b)(1)

(U)

Support to CJTF-7 ~~(S//SI//NF)~~ As the IDC concept began to expand in the summer of 2003, the INSCOM Command Center (ICC) was integrated into the communications architecture as a means of providing a continuous source of communications between the IOC and the Combined Joint Task Force 7 (CJTF-7). The Information Dominance Center assumed a 24X7 operational status in support of the CJTF-7 in August 2003. IOC placed emphasis on support to CJTF-7 and INSCOM established the Information Dominance Center- Extension (IDC-E) with CJTF-7.

(S)

Joint Task Force Computer Network Operations ~~(TS//NF)~~ INSCOM provided two Computer Network Attack (CAN) soldiers to the JTF-CNO in support of CENTCOM (b)(1) They provided weapons system expertise to JTF-CNO planners and operators who were coordinating Computer Network Operations. As part of the larger effort INSCOM G3-IO produced CNA and SPEA supplements to the INSCOM plan.

Technologies in OIF ~~(S//SI)~~ In support (b)(1) OIF, and CJTF-7, INSCOM has fielded a number of new devices utilizing the latest in SIGINT technologies.

(S//SI) INSCOM fielded ten systems to subordinate units. (b)(1)(b)(3) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(S//SI) Five (b)(1)(b)(3) Per NSA systems were fielded with five additional systems in the planning stage.

(b)(1)(b)(3) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

Phase IV SIGINT Planning (TS//SI) CFLCC is moving to Phase IV from which it will deploy of the NSA Musketeer, (b)(1)(b)(3) Per NSA Phase IV is a plan outlined by the NSA which can be summarized in four goals:

The SIGINT plan ISO Phase IV operation has also quickened. NSA conducted Rock Drill V on 24 April, with representatives from both CFLCC and CENTCOM, for the purpose of completing a Phase IV FRAGO to the NSA 1003 OPORD.

(S//NF)

(b)(1)

(S)

(b)(1)

allows (b)(1)(b)(3) Per NSA,(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

(C//~~REL~~) ~~(U//FOUO)~~ Beginning in September 2002, the (b)(7)(E) program began to identify and develop an understanding of contingency requirements for 1003V. The program hosted a conference in September that allowed the ARCENT/CFLCC intelligence staff to present their requirements and concepts for collecting and disseminating intelligence for 1003V. The (b)(7)(E) staff began analysis to ensure the (b)(7)(E) network had the ability to satisfy the stated 1003V requirements. Certain network infrastructure bottlenecks were discovered and remedied. Back up processes were implemented to alleviate any single point of failure. To accommodate the intelligence demands certain circuits were provided expanded bandwidth. The work for a second (b)(7)(E) Network Control Center was accelerated to allow the transfer of priority 1003V circuits to remain operational in the event of a catastrophic failure at the single network control center in the program at Fort Belvoir.

(b)(1) Per NSA, (b)(3):18 U.S.C. 798,(b)(3):50 U

(C//~~REL~~) ~~(U//FOUO)~~ The intelligence requirements for 1003V led to the production and fielding of 2 special purpose built intelligence collection systems and 8 satellite communications systems. The intelligence collections systems were fitted with technical insertion devices to accommodate unique collection requirements for this mission. The program expedited the completion of a facility (b) (1) Per NSA for the distributed signals intelligence collection network inherent to the (b)(7)(E) program. The facility collection configuration was altered to execute the unique signals intelligence mission of 1003V.

(U//~~FOUO~~) The (b)(7)(E) distributed network allowed the collection of CENTCOM theater specific signals intelligence collection, collected from 3 distinct areas within the CENTCOM AOR, to be processed in 5 CONUS and 2 OCONUS sanctuary locations. The subsequent intelligence reporting and feedback, via the (b)(7)(E) communications network, to combat commanders in theater was timely and reliable.

(b)(1),(b)(3):18 U.S.C. 798,(b)(3):50 U.S.C. 403,(b)(3):P.L. 86-36

~~(C/NF)~~

(b)(1)

Regraded CONFIDENTIAL on
30 April 2010
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

USAINSCOM KEY PERSONNEL

Position/Name	**Dates Served**
COMMANDING GENERAL	
MG John F. Kimmons	28 Aug 03 – Present
MG Keith B. Alexander	12 Feb 01 – 2 Jul 03
DEPUTY COMMANDING GENERAL/INDIVIDUAL MOBILIZATION AUGMENTEE	
BG George R. Fay	19 Oct 99 - Present
BG Alfonsa Gilley	15 Aug 96 – 19 Oct 00
DEPUTY COMMANDER	
(b)(6)	8 Aug 02 - Present
	13 Jul 00 - May 02
COMMAND SERGEANT MAJOR	
(b)(6)	31 Jul 01 - Present
	11 Jul 98 – 31 Jul 01
CHIEF OF STAFF	
(b)(6)	Nov 02 – Present
	21 Jul 00 – Nov 02
SECRETARY OF THE GENERAL STAFF	
(b)(6)	01 Sep 95 – Present
STRATEGIC MANAGEMENT & INFORMATION OFC	
(b)(6)	01 Sep 02 – Present
PROTOCOL	
(b)(6)	13 Mar 95 – Present
INTERNAL REVIEW OFFICE	
(b)(6)	06 Jan 03 – Present
	01 Apr 84 – 03 Jan 03

Position/Name	**Dates Served**
PRINCIPAL ADVISOR RESPONSIBLE FOR CONTRACTING (PARC)	
(b)(6)	01 Nov 01 - Present 01 Sep 94 - Nov 01
COMMAND HISTORIAN	
(b)(6)	07 Jan 80 – Present
DIRECTOR, INTELLIGENCE OVERSIGHT OFFICE	
(b)(6)	17 Jun 01- Present 16 Feb 00 – 1 Dec 00 xxxxxxxx – 15 Feb 00
INSPECTOR GENERAL	
(b)(6)	28 Aug 02 - Present 12 Mar 02 – 28 Aug 02 15 Jul 00 – 11 Mar 02
STAFF JUDGE ADVOCATE	
(b)(6)	8 May 03 – Present 15 Jul 01 – 8 May 2003
COMMAND CHAPLAIN	
(b)(6)	Jun 03 – Present 01 Jul 99 – Jun 03
CHIEF INFORMATION OFFICER	
(b)(6)	XX Jan 00 - Present
COMMAND ANTITERRORISM OFFICER	
(b)(6)	15 Jan 03 - Present

Position/Name	**Dates Served**
ASSISTANT CHIEF OF STAFF, G-1	
(b)(6)	27 Aug 03 – Present 15 Aug 02 – 27 Aug 03
ASSISTANT CHIEF OF STAFF, G-2	
(b)(6)	01 Jan 93 – Present
ASSISTANT CHIEF OF STAFF, G-3	
(b)(6)	7 May 03 – Present Jul 02 – 7 May 03
ASSISTANT CHIEF OF STAFF, G-4	
(b)(6)	Jul 02 – Present 01 Jul 98 – April 02
ASSISTANT CHIEF OF STAFF, G-6	
(b)(6)	01 Jul 02 – Present 01 Aug 96 – 31 May 02
ASSISTANT CHIEF OF STAFF, RESOURCE MANAGEMENT	
(b)(6)	12 Jul 02 – Present 30 Dec 98 – 16 Jul 02
ARMY CRYPTOLOGIC OPERATIONS	
(b)(6)	Jul 02 - Present 29 Oct 01 - Jul 02

Unit/Commander	Dates Served
USAINSCOM TRAINING DOCTRINE SUPPORT DETACHMENT (ITRADS)	
(b)(6)	11 Aug 03 – Present 03 Apr 00 – 11 Aug 03
1st INFORMATION OPERATIONS COMMAND (LAND) (formerly LAND INFORMATION WARFARE ACTIVITY)	
(b)(6)	14 Jun 01 – Present 15 May 98 – 14 Jun 01
501st MILITARY INTELLIGENCE BRIGADE (EAC)	
(b)(6)	Jul 02 – Present 22 Jun 00 – Jul 02
513th MILITARY INTELLIGENCE BRIGADE (EAC)	
(b)(6)	Jul 02 – Present 07 Jul 00 – Jul 02
704th MILITARY INTELLIGENCE BRIGADE	
(b)(6)	Jul 02 - Present 15 Jul 00 – Jul 02
66th MILITARY INTELLIGENCE GROUP (PROVISIONAL)	
(b)(6)	Jul 02 - Present 18 May 00 - Jul 02
108th (718th) MILITARY INTELLIGENCE GROUP	
(b)(6)	Jul 02 – Present 18 Jul 00 – Jul 02
115TH MILITARY INTELLIGENCE GROUP	
(b)(6)	Jun 03 – Present Jun 01 – June 03

Unit/Commander	Dates Served
116th MILITARY INTELLIGENCE GROUP (b)(6)	30 July 03 - Present 19 Sep 01 – 30 Jul 03
470th MILITARY INTELLIGENCE GROUP (b)(6)	Sept 03 ~~16 Oct 02~~ - Present
500th MILITARY INTELLIGENCE GROUP (EAC) (b)(6)	Jul 02 – Present Oct 00 – Jul 02
902d MILITARY INTELLIGENCE GROUP (b)(6)	Jul 02 - Present 30 Jun 00 - Jul 02
SECURITY COORDINATION DETACHMENT (b)(6)	Jul 03 - Present 09 Jul 01 – Jul 03
NATIONAL GROUND INTELL CENTER (b)(6)	01 May 03 – Present 01 May 01 – 01 May 03
2nd MILITARY INTELLIGENCE BATTALION (Activated 4 June 2002) (b)(6)	24 Jun 02 - Present 22 Jun 00 – 24 Jun 02
105th MILITARY INTELLIGENCE BATTALION (P) (b)(6)	Sep 02 – Present 16 Aug 02 – Sep 02

Unit/Commander	Dates Served
3d MILITARY INTELLIGENCE BATTALION (AERIAL EXPLOITATION)	
(b)(6)	3 Jun 03 – Present 10 Jun 01 – 3 Jun 03
201st MILITARY INTELLIGENCE BATTALION (SIGINT) (EAC)	
(b)(6)	Jun 02 – Present 02 Jun 00 – Jun 02
202d MILITARY INTELLIGENCE BATTALION (INTG & EXPL) (EAC)	
(b)(6)	24 May 03 – Present 30 May 02 – 24 May 03 07 Jun 00 – 30 May 02
204TH MILITARY INTELLIGENCE BATTALION (AERIAL RECONNAISSANCE)	
(b)(6)	10 Jul 03 – Present 24 Aug 01 – 10 Jul 03
205th MILITARY INTELLIGENCE BATTALION (OPERATIONS)	
(b)(6)	Jul 03 – Present 09 Jul 01 – Jul 03
206th (116th MI GP) MILITARY INTELLIGENCE BATTALION	
(b)(6)	13 Jun 02 – Present 08 Jun 00 – 13 Jun 02
297th MILITARY INTELLIGENCE BATTALION	
(b)(6)	Jul 03 – Present 31 Jul 01 – Jul 03

Unit/Commander	Dates Served
308th MILITARY INTELLIGENCE BATTALION	
(b)(6)	18 Jun 02 - Present 16 Jun 00 – 18 Jun 02
310th MILITARY INTELLIGENCE BATTALION	
(b)(6)	27 Jun 03 – Present 15 Jun 01 – 27 Jun 03
314th MILITARY INTELLIGENCE BATTALION	
(b)(6)	19 Jun 03 – Present 29 Jun 01 – 19 Jun 03
524th MILITARY INTELLIGENCE BATTALION (COLL/EXPL)	
(b)(6)	19 Jun 03 – Present 14 Jul 01 – 19 Jun 03
527th (751st) MILITARY INTELLIGENCE BATTALION	
(b)(6)	10 Jun 02 - Present 28 Jun 00 - Present
532d MILITARY INTELLIGENCE BATTALION (OPERATIONS)	
(b)(6)	20 Jun 03 – Present 1 Oct 02 – 20 Jun 03
741st MILITARY INTELLIGENCE BATTALION	
(b)(6)	Jun 03 – Present Jun 01 – Jun 03
742d MILITARY INTELLIGENCE BATTALION	
(b)(6)	Aug 03 – Present Aug 01 – Aug 03

743d MILITARY INTELLIGENCE BATTALION

(b)(6)

Jul 02 – Present
15 Jul 00 – Jul 02

U.S. ARMY FOREIGN COUNTERINTELLIGENCE ACTIVITY

(b)(6)

25 Jul 03 – Present
11 Jul 01 – 25 Jul 03

FIELD SUPPORT CENTER (-)

(b)(6)

12 Jul 02 - Present
10 Aug 00-12 Jul 02

U.S. ARMY ASIAN STUDIES DETACHMENT

(b)(6)

Feb 99 – Present
14 Jan 89 – Feb 99

~~FOR OFFICIAL USE ONLY~~

CHANGES TO UNITS
FY2003

UIC	Unit Designation	Location
Xxxxxxx	(b)(7)(E)	
	Action: Revoke Organization per P.O. 283-1 dated 10 Oct 02	
W1ERAA	(b)(7)(E)	
	Action: Discontinue Effective Date: 14 15 Oct 02	
WNERAA	1st Information Operations Command (LAND)	Fort Belvoir, VA
	Action: Activate Effective Date: 16 Oct 02	
WNER99	Augmentation, 1st Information Operations Command (LAND)	Fort Belvoir, VA
	Action: Organize Effective Date: 16 Oct 02	
WNDVAA	1st Military Intelligence Center	Fort Belvoir, VA
	Action: Activate Effective Date: 16 Oct 02	
	Action: Revoke Activation per P.O. 282-1 dated 9 Oct 02	
WNDV99	Augmentation, 1st Military Intelligence Center	Fort Belvoir, VA
	Action: Organize Effective Date: 16 Oct 02	
	Action: Revoke Organization per P.O. 282-4 dated 9 Oct 02	
WBUZAA	108th Military Intelligence Group	Bad Aibling, GE
	Action: Inactivate Effective Date: 15 Oct 02	
	Action: Revoke Inactivation per P.O. 332-1 dated 28 Nov 01	
WBUZ99	Augmentation, 108th Military Intelligence Group	Bad Aibling, GE
	Action: Discontinue Effective Date: 15 Oct 02	
	Action: Revoke per P.O. 332-2 dated 28 Nov 01	
WAYJAA	401st Military Intelligence Company	Bad Aibling, GE
	Action: Inactivate Effective Date: 15 Oct 02	
	Action: Revoke per P.O. 332-3 dated 28 Nov 01	
WAYJ99	Augmentation, 401st Military Intelligence Company	Bad Aibling, GE
	Action: Discontinue Effective Date: 15 Oct 02	
	Action: Revoke per P.O. 332-4 dated 28 Nov 01	
WNDDAA	205th Military Intelligence Battalion	Fort Shafter, HI
	Action: Activate Effective Date: 16 Oct 02	
WNDD99	Augmentation 205th Military Intelligence Battalion (Carrier)	Fort Shafter, HI
	Action: Activate Effective Date: 15 Oct 02	

W6A6AA	Central Personnel Security Clearance Facility Action: Organize Effective Date: 1 Oct 02	Fort Meade, MD
WBU7AA	66th Military Intelligence Group Action: Activate Effective Date: 16 Oct 02	Darmstadt, GE
WBU799	Augmentation 66th Military Intelligence Group Action: Organize Effective Date: 17 Oct 02	Darmstadt, GE
WBVDAA	2d Military Intelligence Battalion Action: Activate Effective Date: 17 Oct 02	Darmstadt, GE
WBU8AA	470th Military Intelligence Group Action: Activate Effective Date: 16 Oct 02	Fort Buchanan, PR
WBU899	Augmentation, 470th Military Intelligence Group Action: Organize Effective Date: 16 Oct 02	Fort Buchanan, PR

INFORMATION PAPER

IACF-RM 5 Jan 04

SUBJECT: US Army Central Personnel Security Clearance Facility (CCF) Realignment

1. PURPOSE: Realignment from PERSCOM (W4AFAA) to INSCOM (W6A6AA)

2. NARRATIVE: 1 October 2002 CCF realigned from PERSCOM to INSCOM.

3. FACTS: As part of the Secretary of the Army's transformation business process, CCF realigned under INSCOM on Permanent Order number 207-8, dated 26 July 2002. The realignment was virtually seamless to the employees.

4. (b)(6) Chief, Management Support Branch, is the CCF representative at (b)(6)

APPROVED BY:

(b)(6)

COL, MI
Commanding

S: 9 December 2005

IASE-FP 1 DEC 2005

MEMORANDUM FOR Heads, Staff Elements

SUBJECT: INSCOM Antiterrorism Committee and Working Group

1. Effective immediately, the Antiterrorism Committee is re-established IAW AR 525-13, chaired by the Chief of Staff. Committee members are the G1, G2, G3, G4, G6, RM, SJA, CIO, SMIO, PARC, IG, IO, IR, SJA, HQ, COMDT, and Chaplain.

2. The AT Committee will meet quarterly to assist the INSCOM commander in developing, integrating, and managing the command AT program. The committee will focus on planning, coordinating, and executing an AT program that includes prioritization of funding, repairs, and construction projects; command AT Plan development; AT training, and exercise initiatives.

3. Additionally, an Antiterrorism Working Group will meet monthly under the direction of the Command Antiterrorism Officer. This working group includes representatives from all AT Committee staff elements and will develop issues for presentation to the AT Committee, evaluate threats, and recommend security counter measures.

4. AT Committee members will provide the name of their AT Working Group representative to the point of contact in paragraph 6 below NLT 9 December 2005.

5. The initial Antiterrorism Working Group meeting is scheduled for 15 Dec 2005.

6. Point of Contact (b)(6) Command Antiterrorism Officer, Facilities and Security Division,

(b)(6)

Chief of Staff

ENCLOSURE:
ATC/ATWG Calendar

Antiterrorism Committee/ Antiterrorism Working Group Calendar

15 Dec 05

19 Jan 06*

16 Feb 06

16 Mar 06

20 Apr 06*

18 May 06

15 June 06

20 July 06*

17 Aug 06

21 Sep 06

19 Oct 06*

16 Nov 06

21 Dec 06

18 Jan 07*

*** Denotes AT Committee Meeting**

ENCLOSURE 1

89

(b)(6) mi.army.mil