DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-5100

U-14-4012/FAC2A1 (FOIA)

NOV 19 2014

Mr. John Greenewald
[redacted]

Dear Mr. Greenewald:

This responds to your Freedom of Information Act (FOIA) request, dated October 20, 2009, that you submitted to the Defense Intelligence Agency (DIA) for a copy of the DIA Employee Manual or Handbook. I apologize for the delay in responding to your request. DIA continues its efforts to eliminate the large backlog of pending FOIA requests. In order to properly respond, it was necessary to consult with multiple offices within the agency. A search of DIA's systems of records located one document (218 pages) responsive to your request.

Upon review, I have determined that some portions the document must be withheld in part from disclosure pursuant to the FOIA. The withheld portions are exempt from release pursuant to Exemptions 3 and 6 of the FOIA, 5 U.S.C. § 552 (b)(3) and (b)(6). Exemption 3 applies to information specifically exempted by a statute establishing particular criteria for withholding. The applicable statutes are 10 U.S.C. § 424 and 50 U.S.C. § 3024(i). Statute 10 U.S.C. § 424 protects the identity of DIA employees, the organizational structure of the agency, and any function of DIA. Statute 50 U.S.C. § 3024(i) protects intelligence sources and methods. Exemption 6 applies to information which if released would constitute an unwarranted invasion of the personal privacy of other individuals.

If you are not satisfied with my response to your request, you may exercise your right to file an administrative appeal by writing to the address below and referring to case number 0050-2010. Your appeal must be postmarked no later than 60 days after the date of this letter.

Defense Intelligence Agency
7400 Pentagon
ATTN: FAC2A1 (FOIA)
Washington, D.C. 20301-7400

Sincerely,

Alesia Y. Williams RM
Chief, FOIA and Declassification Services Office

Enclosure

The Defense Intelligence Agency (DIA)

Committed To Excellence In Defense of the Nation

New Employee Guide

September 2009

HUMAN CAPITAL

ALL-SOURCE INTELLIGENCE STARTS HERE ♦ DEFENSE INTELLIGENCE AGENCY

The DIA New Employee Guide was compiled by:

(b)(3):10 USC 424

[redacted]

and

(b)(3):10 USC 424

[redacted]

Table of Contents

1. Introduction

Welcome to DIA! The information in this reference guide will help you navigate through DIA and the many policies governing its employees. As a DIA employee, it is your responsibility to understand and abide by the rules and regulations outlined in this manual.

This book should help:

- Acclimate you to DIA
- Familiarize yourself to DIA locations and facilities
- Answer common new employee questions
- Shed light on important employee policies
- Provide useful tips and reminders
- Highlight key acronyms, phone numbers, and contact information

2. Key

Graphic Element	Description
Attention	Highlights **critical** information or requirements for **DIA supervisors**
🎖	Indicates information applies to military personnel only
⚠	Highlights important information
💡	Calls attention to tips or suggestions; subsequent tips can be identified from the bullets below ▫ **Main Tip** ▫ **Sub Tip**
?	Poses a question: the question is in *italics* and the answer is in ***bold italics***
TOOL	Identifies tools that employees can use from the book, such as procedural checklists and instructions for filling out HR forms
☎	Highlights key point of contact (POC) information
🔍	Alerts to more information found in another section of the handbook
📄	Indicates that more information on DIA policies and procedures is located in existing documentation
☒	Indicates that an action should **not** be taken
☑	Highlights tasks to be completed
eZHR	Calls out information found in eZHR or tips for navigating eZHR
eZHR Forms	Details documents found in eZHR Forms

3. Getting Started and Sponsorship Program

Gateway

The Gateway program is designed to welcome new employees to DIA and to provide the best information on the Agency's mission, vision, culture, employee services, and security processes and procedures. Gateway helps new employees gain the knowledge and tools necessary to transition into their respective roles at DIA.

The bi-weekly program covers a variety of topics on life at DIA.

Gateway is a week long program for all new DIA civilian employees. During the first 2½ days, new civilian employees have the opportunity to learn about and complete all the necessary paperwork in order to begin officially as a DIA employee. New employees are briefed on security at DIA, civilian benefits, and all other HR personnel requirements.

During the last 2½ days, Gateway demonstrates how the individual supports DIA's core intelligence business function of strategic all-source analysis. All new employees are also briefed on security requirements, anti-terrorism, force protection, and procedures for classifications and markings. During this session, all new employees also complete all mandatory training requirements that are outlined in federal, DoD, and DIA regulations.

Sponsorship Program

The Sponsorship Program is designed to orient new employees to DIA. Each new employee is assigned a Sponsor to help get acclimated to their role and to serve as a new employee's primary source of reference for job-related questions and concerns.

Before the completion of Gateway:

☑ Introduce the new employee to their division supervisor and colleagues
☑ Familiarize the new employee with the facility
☑ Discuss DIA training opportunities
☑ Direct new employees to the EAP Office for information regarding childcare or schooling
☑ HR or benefits questions should be referred to the [redacted]
☑ Contact the new hire to arrange a meeting time and place after Gateway is complete

(b)(3):10 USC 424

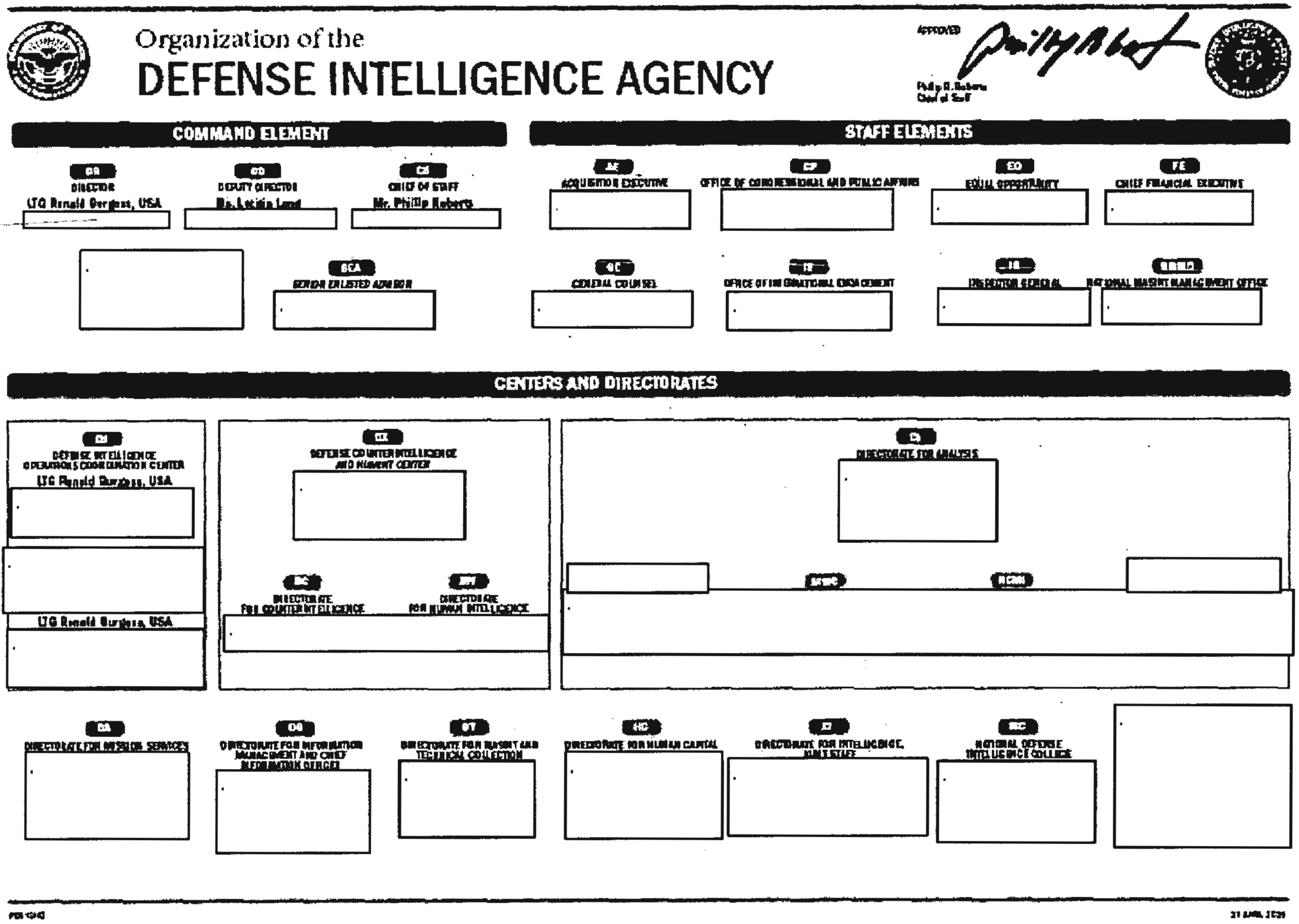
After Gateway:

☑ Help to ensure that the new employee has a workspace with furniture, basic office supplies, telephone, and computer

☑ Assist with new the employee checklists

☑ Continue to maintain contact with the new employee to ensure a smooth transition

4. DIA Organizational Chart



Organization of the
DEFENSE INTELLIGENCE AGENCY

APPROVED
Phillip R. Roberts
Chief of Staff

COMMAND ELEMENT

DR
DIRECTOR
LTG Ronald Burgess, USA
[redacted]

DD
DEPUTY DIRECTOR
Ms. Letitia Long
[redacted]

CS
CHIEF OF STAFF
Mr. Phillip Roberts
[redacted]

[redacted]

SEA
SENIOR ENLISTED ADVISOR
[redacted]

STAFF ELEMENTS

AE
ACQUISITION EXECUTIVE
[redacted]

CP
OFFICE OF CONGRESSIONAL AND PUBLIC AFFAIRS
[redacted]

EO
EQUAL OPPORTUNITY
[redacted]

FE
CHIEF FINANCIAL EXECUTIVE
[redacted]

GC
GENERAL COUNSEL
[redacted]

IE
OFFICE OF INTERNATIONAL ENGAGEMENT
[redacted]

IG
INSPECTOR GENERAL
[redacted]

NMMO
NATIONAL MASINT MANAGEMENT OFFICE
[redacted]

CENTERS AND DIRECTORATES

DEFENSE INTELLIGENCE
OPERATIONS COORDINATION CENTER
LTG Ronald Burgess, USA
[redacted]

[redacted]

LTG Ronald Burgess, USA
[redacted]

DX
DEFENSE COUNTERINTELLIGENCE
AND HUMINT CENTER
[redacted]

DIRECTORATE
FOR COUNTERINTELLIGENCE

DIRECTORATE
FOR HUMAN INTELLIGENCE

[redacted]

DI
DIRECTORATE FOR ANALYSIS
[redacted]

[redacted]

AFMIC

NCMI

[redacted]

[redacted]

DA
DIRECTORATE FOR MISSION SERVICES
[redacted]

DS
DIRECTORATE FOR INFORMATION
MANAGEMENT AND CHIEF
INFORMATION OFFICER
[redacted]

DT
DIRECTORATE FOR MASINT AND
TECHNICAL COLLECTION
[redacted]

HC
DIRECTORATE FOR HUMAN CAPITAL
[redacted]

J2
DIRECTORATE FOR INTELLIGENCE,
JOINT STAFF
[redacted]

NATIONAL DEFENSE
INTELLIGENCE COLLEGE
[redacted]

[redacted]

(b)(3):10 USC
424

5. Senior Leadership Biographies

Director: Lieutenant General Ronald L. Burgess, Jr., USA
Deputy Director: Ms. Letitia A. Long
Chief of Staff: Mr. Phillip R. Roberts
[redacted]
Senior Enlisted Advisor: [redacted]

(b)(3):10 USC 424

(b)(3):10 USC 424

BIOGRAPHY
DEFENSE INTELLIGENCE AGENCY

Lieutenant General Ronald L. Burgess, Jr., USA
Director
Defense Intelligence Agency

Lieutenant General Ronald L. Burgess, Jr., was commissioned in Military Intelligence through the Auburn University ROTC Program in 1974. He earned a Master of Science degree in Education from the University of Southern California in 1980, and a Master of Military Arts and Science from the U.S. Army Command and General Staff College in 1986.

His military education includes the Armor Officer Basic Course, the Military Intelligence Officers Advanced Course, the Command and General Staff College, the Advanced Military Studies Program, and the Air War College.

Lieutenant General Burgess has held a variety of key staff and command positions.

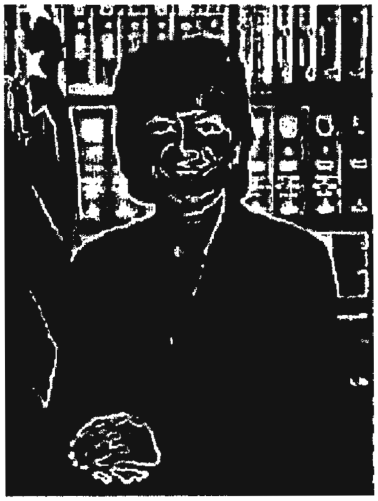
His staff assignments include: Assistant Executive Officer to the Deputy Chief of Staff for Intelligence, Washington, D.C. in 1990; G-2, 25th Infantry Division (Light) from June 1993 to June 1994 at Schofield Barracks, Hawaii. He served as J-2, Joint Special Operations Command (JSOC), Fort Bragg, North Carolina from July 1997 to June 1999; Director for Intelligence (J2) U.S. Southern Command from July 1999 until May 2003, and J2, Joint Staff from June 2003 to July 2005. Lieutenant General Burgess assumed duty as the Deputy Director of National Intelligence for Customer Outcomes in August 2005 transitioning to Director of the Intelligence Staff in February 2007. He was dual-hatted twice as the Acting Principal Deputy Director of National Intelligence from May 2006 to October 2007, and January to February 2009.

Command assignments include: Company Commander, 124th Military Intelligence Battalion, 24th Infantry Division (Mechanized) at Fort Stewart, Georgia; command of the 125th Military Intelligence Battalion, 25th Infantry Division (Light), Schofield Barracks, Hawaii from June 1991 to June 1993; and command of the 470th Military Intelligence Brigade in Panama from July 1995 to June 1997. LTG Burgess became the 17th director of the Defense Intelligence Agency on March 18, 2009.

His personal awards and decorations include the Defense Distinguished Service Medal, Defense Superior Service Medal (Two Oak Leaf Clusters), Legion of Merit, Meritorious Service Medal (Four Oak Leaf Clusters), Joint Service Commendation Medal, Army Commendation Medal, Army Achievement Medal, NATO Medal for Yugoslavia, Army General Staff Identification Badge, Joint Staff Identification Badge and Parachutist Badge.

Lieutenant General Burgess and his wife Marta have five children: Lee, Regina, Julia, Mary, and John.

BIOGRAPHY
DEFENSE INTELLIGENCE AGENCY



MS. LETITIA A. LONG
Deputy Director

Ms. Letitia A. Long became the Deputy Director of the Defense Intelligence Agency on 14 May 2006. Previously she was the Deputy Under Secretary of Defense for Intelligence (Policy, Requirements, and Resources) from June 2003 until May 2006. She also served in the positions of Deputy Director of Naval Intelligence from July 2000 to June 2003 and the Director of Central Intelligence's (DCI) Executive Director for Intelligence Community Affairs, responsible for community wide policy formulation, resource planning and program assessment and evaluation between January 1998 and June 2000.

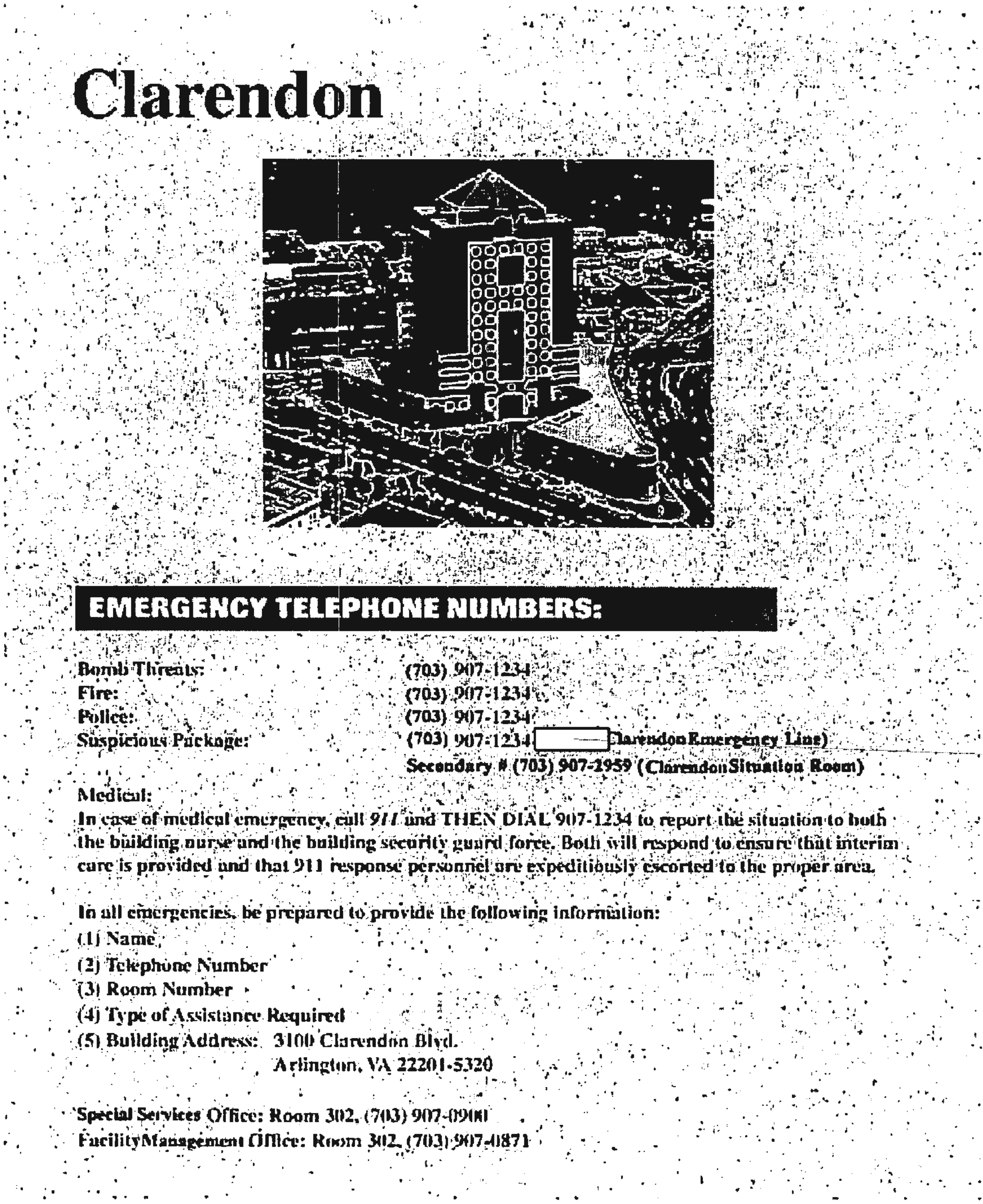
Ms. Long entered federal service with the Navy in 1978 as a Project Engineer in training with the David Taylor Research Center. Upon completion of her degree in 1982, she continued with David Taylor Research Center for six years working on various submarine acoustic sensor programs. In 1988, Ms. Long joined the staff of the Director of Naval Intelligence where she managed Intelligence Research and Development programs.

Ms. Long was selected into the Senior Intelligence Executive Service in July 1994 and was dual-hatted as the Director, Requirements, Plans, Policy, and Programs for the Navy N2 staff as well as the Director of Resource Management for the Office of Naval Intelligence (ONI). From 1994 to 1996, Ms. Long was on rotational assignment from ONI to the Defense Intelligence Agency (DIA) as Director of Military Intelligence (DMI) Staff Director. In 1996, Ms. Long joined DIA as the Deputy Director for Information Systems and Services where she directed DIA's first Chief Information Officer. worldwide information technology and communications programs.

Ms. Long earned a BS in Electrical Engineering from Virginia Tech and a MS in Mechanical Engineering from the Catholic University of America. She is the recipient of the Department of Defense Medal for Distinguished Civilian Service, the Presidential Rank Award of Distinguished Executive, the Navy Distinguished Civilian Service Award, the Presidential Rank Award of Meritorious Executive (2 awards), the National Intelligence Distinguished Service Medal and the Defense Intelligence Agency Director's Award (2 awards). Ms. Long is married to Mr. John Skibinski. They reside in Arlington, Virginia.

6. DIA Locations

Clarendon



Clarendon

EMERGENCY TELEPHONE NUMBERS:

Bomb Threats:	**(703) 907-1234**
Fire:	**(703) 907-1234**
Police:	**(703) 907-1234**
Suspicious Package:	**(703) 907-1234[redacted]larendonEmergency Line)**
	Secondary # (703) 907-2959 (ClarendonSituation Room)

(b)(3):10 USC 424

Medical:
In case of medical emergency, call *911* and THEN DIAL 907-1234 to report the situation to both the building nurse and the building security guard force. Both will respond to ensure that interim care is provided and that 911 response personnel are expeditiously escorted to the proper area.

In all emergencies, be prepared to provide the following information:
(1) Name
(2) Telephone Number
(3) Room Number
(4) Type of Assistance Required
(5) Building Address: 3100 Clarendon Blvd.
Arlington, VA 22201-5320

Special Services Office: Room 302, (703) 907-0900
FacilityManagement Office: Room 302, (703) 907-0871

The next 2 pages are withheld in full and not included.

BIOGRAPHY
DEFENSE INTELLIGENCE AGENCY
DEFENSE INTELLIGENCE SENIOR EXECUTIVE SERVICE

PHILLIP R. ROBERTS
Chief of Staff

Mr. Phillip R. Roberts was appointed as Chief of Staff in March 2007. As Chief of Staff he insures timely satisfaction of the Agency's current requirements while developing the plans, process improvements, and strategies that prepare the Agency for the future. Prior to this assignment, Mr. Roberts was the Chief of DIA Liaison - London. He was the Vice Deputy Director for Analysis prior to becoming Chief of DIALL. The Directorate for Analysis and Production (DI), composed of approximately 1,900 military and civilian personnel, provides all-source intelligence analysis to the Unified Commands and deployed U.S. and allied forces; the Chairman, Joint Chiefs of Staff; and the Secretary of Defense.

Prior to his appointment to Vice Deputy Director, Mr. Roberts served as the Chief, Operational Support Group, Directorate for Intelligence. As such, he was responsible for the production of all-source intelligence on foreign infrastructure and operational environment related issues, in support of deliberate and crisis planning requirements worldwide.

In August 1998, Mr. Roberts became a member of the Defense Intelligence Senior Executive Service (DISES). From 1998 to 1999, Mr. Roberts was the Chief, Office for Counterproliferation Support.. In this capacity, he was responsible for the production of all-source intelligence on foreign, nuclear, chemical, and biological warfare programs in support of U.S. counterproliferation efforts. From 1995 to 1998, Mr. Roberts was the Senior Intelligence Officer (SIO), Office for Counterproliferation Support and from 1993 to 1995, he served as the SIO, Office for Ground Forces.

From 1991 to 1993, Mr. Roberts served as the Deputy Functional Manager and Director, Office of General Military Intelligence Functional Management. In this capacity, he oversaw program planning and budget execution for approximately $520 million and 7,550 personnel. During this period, Mr. Roberts chaired the Council of Intelligence Producers and directed the "JIC/JAC studies" which served as the basis for the largest reallocation of Defense intelligence resources in the post-Cold War period. From 1989 to 1990, as the Special Assistant for Intelligence Production, Directorate for Research, he directed the production of finished intelligence and data base maintenance of over 800 analysts. Prior to 1989, Mr. Roberts served in other supervisory and analytical positions including Chief, North Korean Military Capabilities Branch, and Senior Intelligence Officer, Asia Division.

Mr. Roberts has received two Intelligence Community National Meritorious Unit Citations and is a recipient of the Defense Intelligence Agency Award for Exceptional Civilian Service Medal, the Defense Intelligence Agency Award for Meritorious Civilian Service Medal, the Defense Intelligence Director's Award, and the Director of Central Intelligence Diversity Management Award. From 2004 to 2007 he represented the Director, DIA at the NATO Intelligence Board.

October 2007

General Information

The Clarendon Boulevard building is a commercially leased facility. The building was constructed in 1984 and DIA occupied it in December 1987.

Directions

From Reagan National Airport

- Take George Washington Parkway to I-395 South.
- Exit I-395 at Route 110 (Rosslyn).
- Follow Route 110 to Rosslyn. Stay in left lane to Wilson Boulevard.
- Follow Wilson Boulevard approximately three miles to Highland Street.
- Turn left on Highland Street. Building is on the right.

From Dulles Airport

- Take Dulles Access Road to I-66 East.
- Exit I-66 East at Glebe Road.
- Follow Glebe Road and turn left at Wilson Boulevard.
- Follow Wilson Boulevard until it turns into Clarendon Boulevard.
- Building is on the right.

From Baltimore-Washington International Airport

- Take I-95 South to I-66 West.
- Exit I-66 West at Glebe Road.
- Follow Glebe Road and turn left at Wilson Boulevard.
- Follow Wilson Boulevard until it turns into Clarendon Boulevard.
- Building is on the right.

Attention

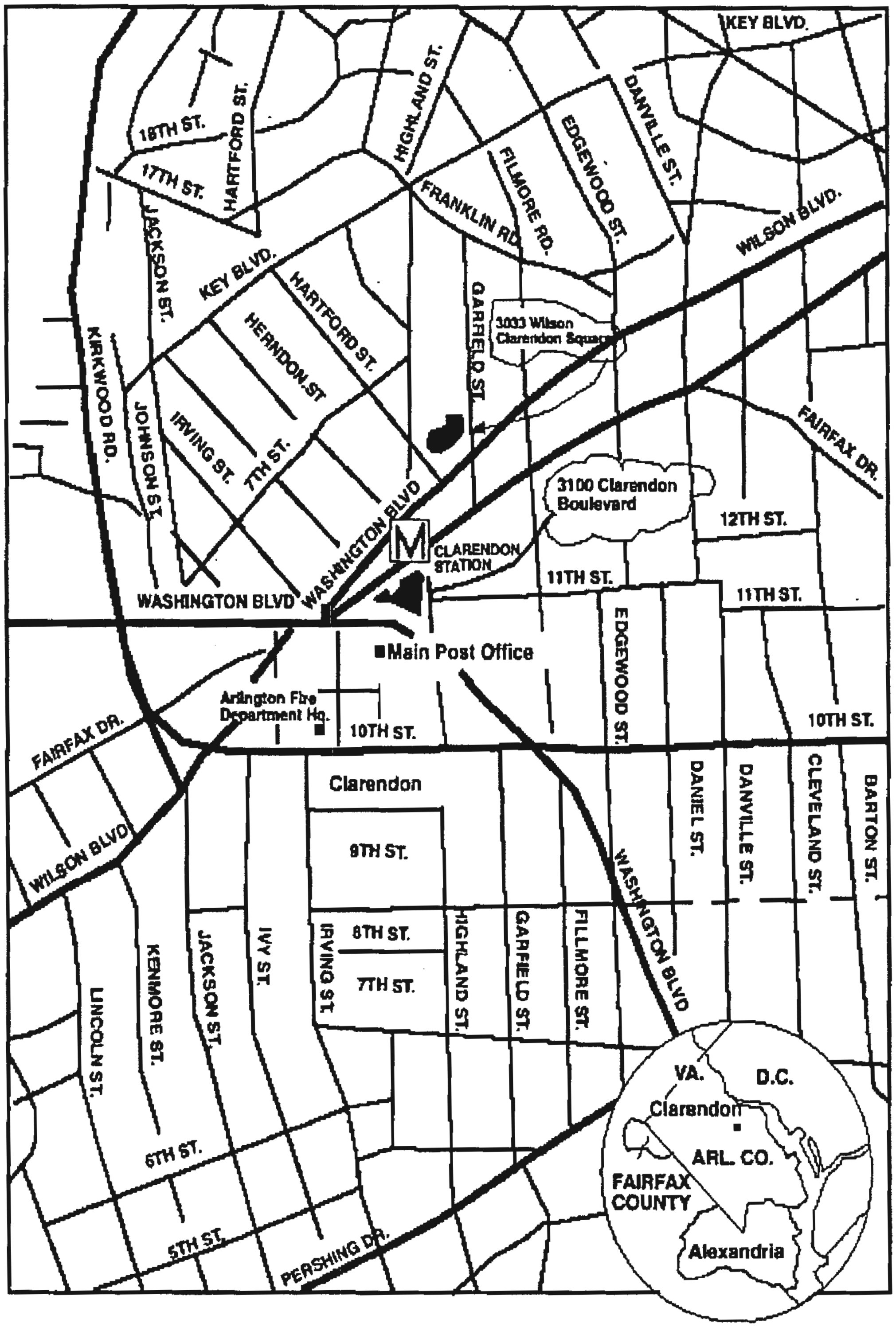
IMPORTANT PARKING INFORMATION FOR VISITORS TO

THE CLARENDON FACILITY

Garage parking is extremely limited and must be prearranged with the Clarendon Special Service Office at (703) 907-0900. Metered, street parking is available, but it is extremely limited.

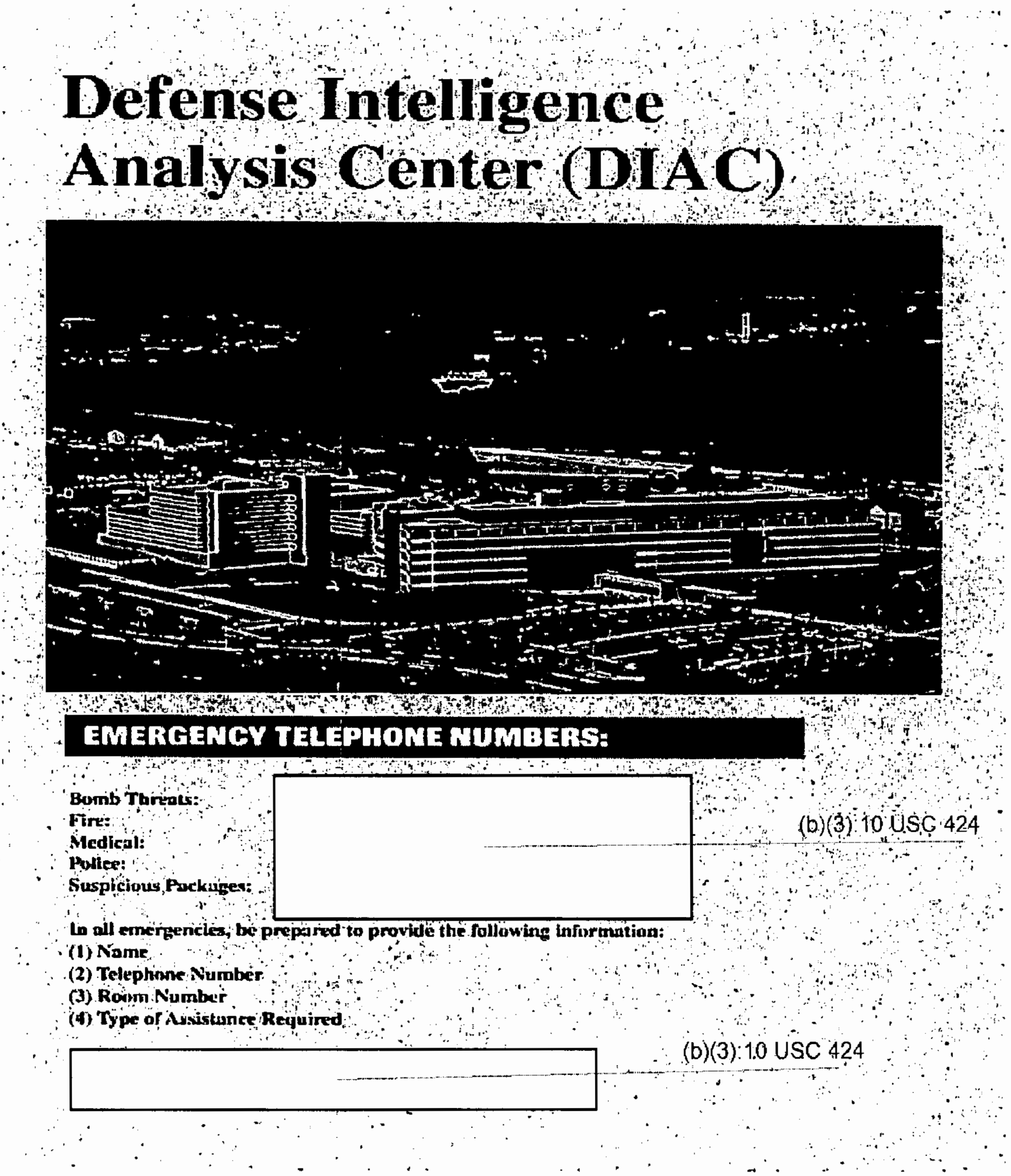
The Clarendon facility is also accessible via the metro at the Clarendon stop on the Orange Line.

The next 2 pages are withheld in full and not included.



The next 6 pages are withheld in full and not included.

DIAC



Defense Intelligence Analysis Center (DIAC)

EMERGENCY TELEPHONE NUMBERS:

Bomb Threats:
Fire:
Medical:
Police:
Suspicious Packages:

[redacted]

(b)(3): 10 USC 424

In all emergencies, be prepared to provide the following information:
(1) Name
(2) Telephone Number
(3) Room Number
(4) Type of Assistance Required

[redacted]

(b)(3): 10 USC 424

General Information

Constructed in 1984, the Defense Intelligence Analysis Center (DIAC) on Bolling Air Force Base [redacted] The construction of additional DIAC space (the DIAC Expansion) was completed in FY06 [redacted]

[redacted]

(b)(3):10 USC 424

(b)(3):10 USC 424

(b)(3):10 USC 424

Missile and Space Intelligence Center (MSIC)

EMERGENCY TELEPHONE NUMBERS:

Bomb Threats:	9-911
Fire:	9-911
Medical:	9-911
Police:	9-911
Suspicious Packages:	[redacted]

(b)(3):10 USC.424

In all emergencies, be prepared to provide the following information:

(1) Name
(2) Telephone number
(3) Room number
(4) Type of assistance required
(5) Building Address

(b)(3):10 USC 424

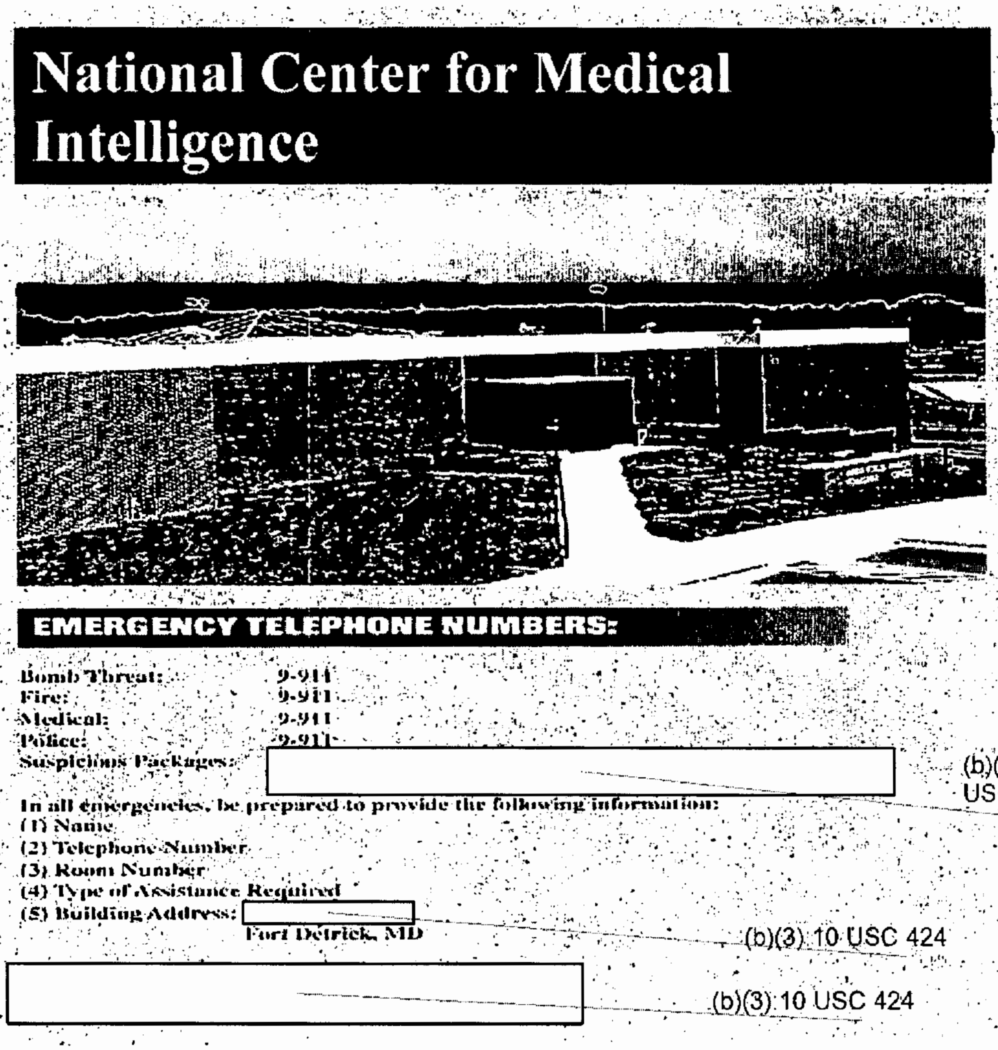
[redacted]

General Information

The MSIC is located on Redstone Arsenal, Alabama, and is a field operating agency of the Defense Intelligence Agency (DIA). Its origin is traced to the establishment of the U.S. Army Ballistic Missile Agency in 1956, which was headed by Dr. Wernher von Braun, the father of U.S. missile technology. In 1967, MSIC became one of the six major scientific and technical intelligence production elements of DIA. Since 1992, MSIC has been an integrated production activity of the Department of Defense (DoD).

The next page is withheld in full and not included.

NCMI



National Center for Medical Intelligence

EMERGENCY TELEPHONE NUMBERS:

Bomb Threat:	9-911
Fire:	9-911
Medical:	9-911
Police:	9-911
Suspicious Packages:	[redacted]

(b)(3):10 USC 424

In all emergencies, be prepared to provide the following information:
(1) Name
(2) Telephone Number
(3) Room Number
(4) Type of Assistance Required
(5) Building Address: [redacted]
Fort Detrick, MD

(b)(3):10 USC 424

[redacted]

(b)(3):10 USC 424

General Information

NCMI, located at Fort Detrick, Maryland, formerly the Armed Forces Medical Intelligence Center (AFMIC), transitioned to a national center on 2 July 2008 in recognition of its expanding role as the Intelligence Community's premier producer and coordinator of medical intelligence. AFMIC was transferred to DIA from U.S. Army on 1 January 1992.

Pentagon

Pentagon

EMERGENCY TELEPHONE NUMBERS:

DO NOT DIAL 911

Fire:
Medical:
Police:
Suspicious Packages: [redacted]

(b)(3):10 USC 424

In all emergencies, be prepared to provide the following information:

(1) Name
(2) Telephone Number
(3) Room Number
(4) Type of Assistance Required

Facility Emergencies: [redacted]
Other times: [redacted]

(b)(3):10 USC 424

Floor Plan

Room numbers are comprised of the following information:

The **first number or letter** indicates the **floor** on which the room is located: B = Basement, M = mezzanine, 1-5 = floors

The **next letter indicates** the ring on which the room is located. (Rings are designated as A,B,C,D, and E for the mezzanine and floors 1-5 plus the additional rings F and G in the basement only.)

The **next digit** or the **next two digits** indicates the corridor on which the room is located. (Corridors are designated 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10)

The **last two digits** indicate the specific bay or room number assigned to an office.

EXAMPLE, to locate room 3D326:

- Go to the **third** floor, **A** Ring
- Proceed along the A Ring to corridor 3
- Go down corridor 3 to the D Ring
- Turn right and proceed to room or bay number.

FLOOR

Proceed to floor by ramp, stair or escalator

RING

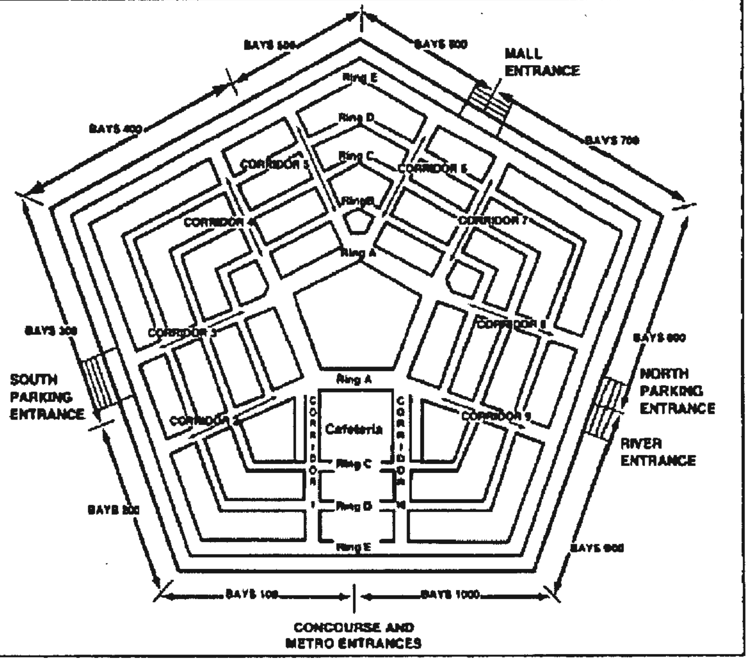
Take the main corridor (A Ring) to each numbered corridor.

CORRIDOR

Proceed along the numbered corridors (1 thru 10) to a specific ring (B thru E)

BAY

Enter ring to the left for rooms/bays numbering below 50, and to the right for rooms/bays above 50.



Directions

From Reagan National Airport

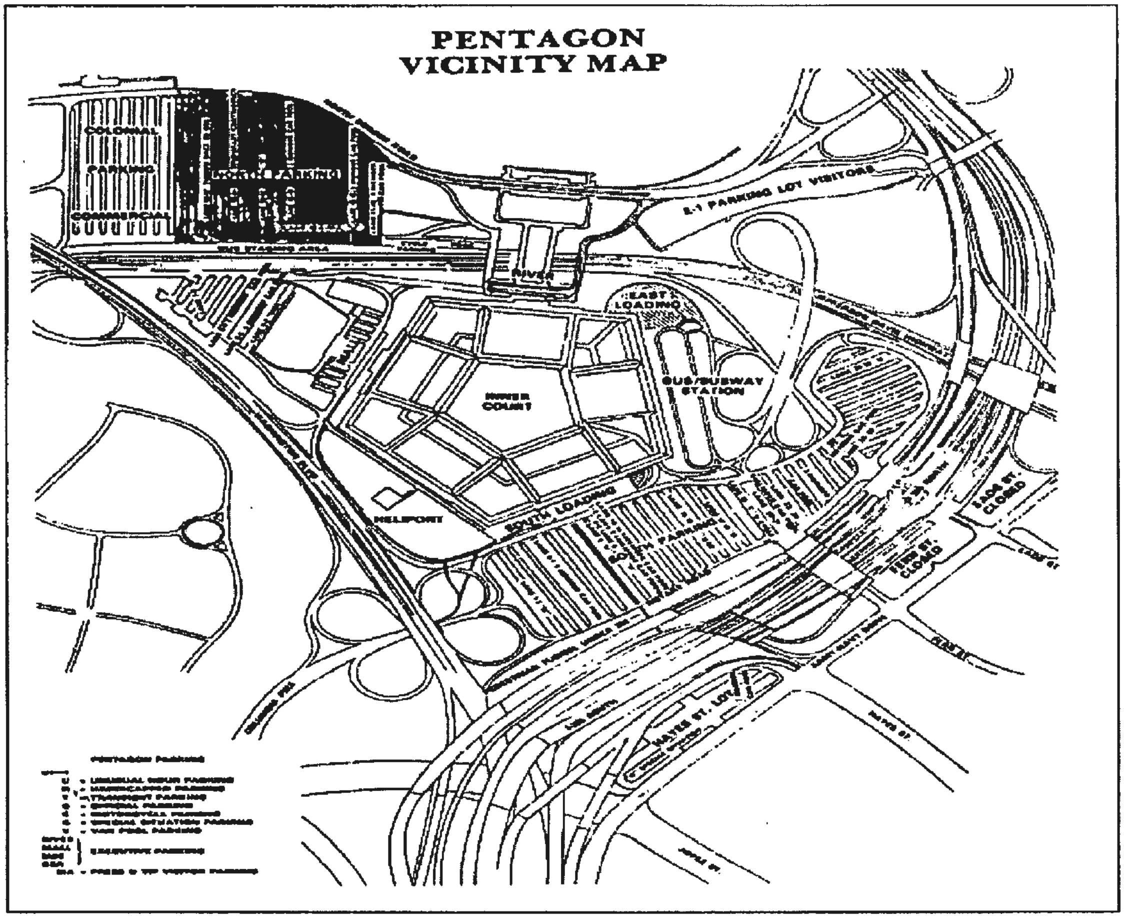
- George Washington Parkway South to I-395 South
- I-395 South to Pentagon/Washington Boulevard (Route 29) Exit
- Take Pentagon Exit on left.

From Dulles Airport

- Dulles Access Road to I-66 East (Washington)
- I-66 East to Pentagon Exit 24

From Baltimore Washington International Airports

- I-95/495 South to I-395 North
- I-395 to Pentagon Exit



7. Frequently Used Acronyms

(b)(3):10 USC 424

ABB	Agency Bonus Boards
ACT	Accelerated Career Transfer Program
AE	Acquisition Executive
AFB	Air Force Base
AHB	Agency Hiring Board
AO	Administrative Officer
AWS	Alternative Work Schedules
C	Confidential
CAC	Civilian Awards Committee
CD	Collateral Duty
CE	Command Element
CI	Chief of Investigations
CI	Counter Intelligence
COMINT	Communications Intelligence
CONUS	Continental US
CP	Office for Congressional and Public Affairs
CS	Chief of Staff
CSO	Chief of Special Office
CSP	Career Service Plan
CSRS	Civil Service Retirement System
CWF	Civilian Welfare Fund
CWS	Compressed work schedule
DA	Directorate for Administration
[redacted]	[redacted]
DACT	Degree Assisted Career Transition Program
[redacted]	[redacted]
DAS	Defense Attaché System
DCEM	DIA Civilian Expeditionary Medal
DCI	Director of Central Intelligence
DCS	Defense Courier Service
DD	Deputy Director
DDFor	Deputy Director For
DH	Directorate for Human Intelligence
DI	Directorate for Analysis
DIAC	Defense Intelligence Analysis Center
DISES	Defense Intelligence Senior Executive Service
DISL	Defense Intelligence Senior Level
DLPT	Defense Language Proficiency Test
DNI	Director for National Intelligence
DR	Director
DS	Directorate for Information Management & Chief Information Officer
DT	Directorate for MASINT and Technical Collection
EAP	Employee Assistance Program
EEO	Equal Employment Opportunity

EO	Equal Employment Office
FE	Office of the Chief Financial Executive
FECA	Federal Employees Compensation Act
FEGLI	Federal Employees Group Life Insurance
FEHB	Federal Employees Health Benefits Program
FERS	Federal Employees Retirement System
FFLA	Family Friendly Leave Act
FLPP	Foreign Language Proficiency Pay
FLTCIP	Federal Long-Term Care Insurance Plan
FMLA	Family and Medical Leave Act
FOUO	For Official Use Only
FPCON	Force Protection Conditions
FSA	Flexible Spending Account (Health Savings Plan)
FWS	Flexible Work Schedule
GC	General Counsel
GG	General Grade
GS	General Schedule
HC	Directorate for Human Capital

[redacted]

(b)(3):10 USC 424

HMO	Health Maintenance Organization
HRM	Human Resources Manager
HRMS	Human Resources Management System
HUMINT	Human Intelligence
IA	Information Assurance
IC	Intelligence Community
ICA	Intelligence Community Award
ICARP	Intelligence Community Award Review Panel
IE	Office of International Engagement
IG	Office of the Inspector General
IMINT	Imagery Intelligence
INSCOM	US Army Intelligence and Security Command
IO	Intelligence Officer
J2	Directorate for Intelligence
JAG	Judge Advocate General
JMIC	Joint Military Intelligence College
JMITC	Joint Military Intelligence Training Center
JWICS	Joint Worldwide Intelligence Communication System
LES	Leave and Earnings Statement
LWOP	Leave Without Pay
MASINT	Measurement and Signature Intelligence

MD	Office of Diversity Management
MSIC	Missile and Space Intelligence Center
MWF	Morale Welfare Fund
NIPRNET	Non-secure Internet Protocol Router Network-Unclassified
NCMI	National Center for Medical Intelligence
NOFORN	No Foreign Nationals
NSA	National Security Agency
NTE	Not to Exceed
OASDI	Old Age Survivors Disability Insurance (Social Security)
OCONUS	Outside the Continental US
OPF	Official Personnel Folder
OPI	Oral Proficiency Interview
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
OSHE	Occupational Safety, Health, and Environment Program
OSINT	Open Source Intelligence
PAR	Personnel Action Request
PARB	Performance Appraisal Review Board
POC	Point of Contact
PPO	Preferred Provider Organization
QC	Quality Control
QSI	Quality Step Increase
R	Restricted
RDO	Regular Day Off
RIF	Reduction-In-Force
RMP	Response Management System
S	Secret
SAA	Special Act Award
SCD	Service Computation Date
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SES	Senior Executive Service
SI	Special Intelligence
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network-Classified
SSCO	Special Security Contact Officer
SSO	Special Security Office
SSP	Sustained Superior Performance
SSS	Staff Summary Sheet
T&A	Time and Attendance
TDY	Temporary Duty
TEC	Training and Education Committee
TIP	Tomorrow's Intelligence Professionals
TK	Talent Keyhole
TS	Top Secret
TSP	Thrift Savings Plan
U	Unclassified
UMP	Upward Mobility Program
USO	Unit Security Office

The next 2 pages are withheld in full and not included.

WG	Wage Grade
WIGI	Within-Grade Increase
WHS	Washington Headquarter Service

9. Frequently Used Phone Numbers

NCMI Frequently Used Phone Numbers and Facilities

(b)(3):10 USC 424

SSO/Badge Office, [redacted] [redacted]
Building Management,
Emergency/
Mailroom,
Operations

(b)(3):10 USC 424

Barber Shop

Fort Detrick Barbershop is located in [redacted] Business hours are Monday 0900-1600; Tuesday, Wednesday, and Friday 0900-1700; Thursday 0900-1900; and Saturday 0900-1600. (b)(3):10 USC 424

Building Trouble Calls

Report electrical, heating, air conditioning, and ventilation problems to the NCMI Building Manager's Office at [redacted] (b)(3):10 USC 424

Conference Rooms

The NCMI operations staff manages the scheduling of the facility's conference room [redacted] (b)(3):10 USC 424

Health and Medical

The occupational health office is located in [redacted] and is available and open Monday-Friday from 0745-1630. (b)(3):10 USC 424

Lost and Found

Lost or found items can be retrieved or deposited at the Building Manager's Office, [redacted] (b)(3):10 USC 424

Locker Rooms and Shower Facilities

Locker rooms for men and women are equipped with showers. They are located on the lower level of the NCMI facility. A limited number of lockers are available for daily use.

Mail

Official mail may be deposited and/or picked up in the NCMI building at the (b)(3):10 USC 424 Program & Security Branch [redacted] A U.S. Postal Service mailbox is located in the parking lot across the street from the facility.

Parking

Parking on base at Fort Detrick is open to all personnel unless specifically identified for exclusive use by an individual, special permit, visitor, or organization.

Clarendon Frequently Used Phone Numbers and Facilities

SSO/Badge Office, Room 427	(703) 907-1639
Building Management, Room 302	(703) 907-0900
Emergency	**(703) 907-1234**
Mailroom, Room 440	(703) 907-0858

Barber Shop

Refer to the retail and service booklets in the Building Manager's Office, (703) 907-0900.

Building Construction and Alterations

Minor construction, alterations, or maintenance and repair in Clarendon will be handled in accordance with ***DIAR 12-3.*** Requests shall be submitted through the element's space and engineering coordinator to the facility engineer, Room 302, (703) 907-0871.

Building Trouble Calls

Report building problems to the facility manager's office at (703) 907-0871, Room 302. If the building maintenance staff is unavailable; call the Building Manager's Office at (703) 907-0900, Room 302.

Bus Service

The DoD Bus provides bus service between Clarendon, the Pentagon, the DIAC, and CIA. The bus stops in front of the building on Clarendon Boulevard. Bus schedules are posted throughout the Clarendon building and in the DoD telephone directory.

Equipment Repairs

Equipment repairs (typewriters, desk calculators, etc.) are arranged through the Operations Management Branch, (703) 617-3880. Computer repairs are arranged through the ADP Command Center, Room B1-209 in the DIAC, (202) 231-8000.

Food Service

Clarendon does not have contract food services. However, a café is located on level M. In addition, numerous restaurants are within easy walking distance of the building. The café on level M can assist with limited luncheon catering requirements.

Lost and Found

Lost or found items can be retrieved or deposited at the Building Manager's Office.

Locker Rooms and Shower Facilities

Men and women's lockers and shower facilities are located on the third level.

Mail

Official mail may be deposited and/or picked up in Clarendon mailroom, Room 440.

Parking

A professional parking concessionaire manages the parking garage at Clarendon for the building owner. To procure parking in the garage, a daily or monthly fee must be paid. Visitors can obtain
a one-day parking pass.

(b)(3):10 USC 424

[redacted] *Frequently Used Phone Numbers and Facilities*

Building Management
Emergency [redacted]

(b)(3):10 USC 424

Lost and Found

Lost and Found items can be retrieved or deposited at the Building Manager's Office.

Locker Rooms and Shower Facilities

There is no gym, locker room, and shower facility.

Food Services

Food vendors are located close to the lobby in the adjacent building.

Smoking

The designated smoking area is located by the building loading dock.

Visitor Access After Hours

If a visitor is expected after normal working hours, on Saturday, Sunday, or holidays, arrangements must be made through [redacted] to have the visitor admitted in the building. [redacted] requires the full name of the visitor and their approximate time of arrival. [redacted] can be reached at [redacted] [redacted]

(b)(3):10 USC 424

(b)(3):10 USC 424

(b)(3):10 USC 424

DIAC Frequently Used Phone Numbers and Facilities

ADP Command (Help Desk-Computer Issues)
SSO/Badge Office, [redacted]
Barber Shop
Pentagon Federal Credit Union (Bolling AFB)
Building Management [redacted]
Building Maintenance & Repair
Clinic
DIA Store, [redacted]
Emergency
Emergency TTY
Employee Assistance Program
Dry Cleaners
Facts and Snacks
Library (Unclassified) [redacted]
Library (Classified),
Mailroom,
Security,
Travel and Passport Services

[redacted]

(b)(3):10
USC 424

Barber Shop

The Barber Shop is located in the main lobby of the DIAC and is open from Monday-Friday from 0700-1600.

Laundry and Dry Cleaners

The DIAC Laundry and Dry Cleaners are located in [redacted] and provide dry cleaning, laundry, alteration, and shoe repair services.

(b)(3):10
USC 424

Food Services

(b)(3):10
USC 424

The DIAC cafeteria is located in the [redacted] Breakfast and lunch are served Monday-Friday, except for U.S. government holidays. Breakfast is served from 0600-0930 and lunch is served from 1000-1400, [redacted] Catering service is available

(b)(3):10
USC 424

Facts and Snacks

(b)(3):10
USC 424

The Facts and Snacks shop is located in the main lobby of the DIAC, [redacted] The shop sells a variety of items ranging from snack foods, sodas, magazines, greeting cards, etc.

Health and Medical

The DIAC health unit is open Monday-Friday from 0630-1630. In addition to providing first aid and walk-in care, the unit also provides nursing services, referrals, and immunizations to civilian employees.

Fitness

Civilian employees may utilize the cardio center across the hallway from the supply store, first floor under the escalators leading down to the cafeteria. Bolling Air Force Base also operates two gyms that civilian employees may use. These gyms include cardio and weight machines, as well as locker rooms and shower facilities.

Lost and Found

Lost and found items can be retrieved or deposited in the Building Manager's Office.

The DIA Store

The DIA store sells a variety of DIA memorabilia. Showcases of the merchandise are in the main lobby.

MISIC Frequently Used Phone Numbers and Facilities

(b)(3):10 USC 424 SSO/Badge Office, [redacted]
Building Management,
Emergency [redacted] (b)(3):10 USC 424
(b)(3):10 USC 424 Mailroom, [redacted]
Operations,

Pentagon Frequently Used Phone Numbers and Facilities

SSO/Badge Office (DIA), [redacted]
Badge Office (DoD)
Building Management
Emergency [redacted]
Emergency TTY
Mailroom [redacted]
Building Operations Command Center
Ceremonies and Special Events
Deliveries and Clearances (Dock Master)
Pentagon Police Force
Safety Issues
Pentagon LSA (Reporting computer related problems) [redacted]

(b)(3):10
USC 424

Being that DIA is headquartered at the Pentagon and it is one of the larger locations, there are a variety of facilities and services offered here. Food services range from a sushi bar to Taco Bell and McDonalds. Other services include an athletic center, CVS Drugstore, GNC Nutrition Center, Hair Care Center, Pentagon Dry Cleaners, Pentagon Vision Center, Book Store, Beauty Shop, and Library.

10. Employee Benefits

Introduction

We know you work hard every day supporting DIA's mission. We also understand your interest in learning more about all of the benefits that are available to DIA employees.

In this section, we lay out key features of DIA's pay, benefits, and support services, and we describe our commitment to making DIA the best possible employer.

In this section you will find useful information on:

- Foreign language proficiency pay (FLPP)
- Leave and Earnings Statement (LES)
- Premium pay, bonuses, and allowances
- Work schedules
- Employee tiers (emergency designation)
- Bad Weather and Emergencies
- Time and attendance
- Holidays
- Leave
- Employee benefits and insurance
- Retirement
- Employee Assistance Program

Foreign Language Proficiency Pay

As a DIA employee, you should know that you may be eligible for Foreign Language Proficiency Pay (FLPP).

If you demonstrate proficiency in a foreign language, you can request FLPP pay in the following manner:

(b)(3):10 USC 424

Step One — Contact the DIA [redacted] to schedule either a Defense Language Proficiency Test (DLPT) or an Oral Proficiency Interview.

Step Two — Submit a copy of your DLPT or oral proficiency score to [redacted]

(b)(3):10 USC 424

Step Three — If you are deemed eligible for FLPP, [redacted] will forward your certification to payroll.

Step Four — Test annually to retain your FLPP eligibility.

Attention

FLPP pay may be terminated or reduced at any time, especially if the language is removed from the **DIA Critical Language List**, or the employee has not completed their annual retest.

(b)(3):10 USC 424,.

(b)(3):10 USC 424

[redacted] is your resource for foreign language related issues at DIA. Their [redacted] website [redacted] has an abundance of information on such issues as FLPP pay, testing, eligibility, and language priorities.

(b)(3):10 USC 424

How much can FLPP pay impact your total compensation? The amount of FLPP awarded ranges from $75.00-$500.00 per pay period, depending upon your language(s) and proficiency level(s).

Premiums, Bonuses, and Allowances

We've covered how you get paid for working hard and how you get paid for working a lot, now we're going to explain how you get paid for working at odd times and in odd places. In addition to regular pay, overtime, or comp time, DIA offers its employees other premium pay, including:

- Sunday pay
- Holiday pay
- Night differential

? *How much does work on a Sunday or holiday pay?*

Sundays pay 25% more than your base pay. Holidays pay 100% more than your base pay.

DIA employees can receive still more pay, depending on assignment-specific circumstances:

- Incentives
- Allowances
- Differentials

Premium pay procedures for working late at night or in hazardous conditions are detailed in DIAI 1400.002, "Civilian Pay Administration."

[redacted]

(b)(3):10 USC 424

Work Schedules

At DIA, the standard work schedule is 8 ½-hours per day, forty hours per week, with a standard 30-minute meal period.

In keeping with the non-standard demands of the Agency mission and dependent on mission requirements, DIA permits employees to arrange accommodating work schedules with their supervisors. Several pragmatic work-life balance options are detailed below.

Flexible Work Schedule

Require employees to complete 40 hours of work each week. A regular schedule for each employee must be established and approved in advance by the supervisor. With supervisory approval, employees may be permitted to vary their arrival and departure times while still completing the 8 ½ hour workday; or employees may be permitted to vary the number of hours worked on a given day, as long as the hours worked are within established office hours and the employee is present for duty for primary business hours.

The next page is withheld in full and not included.

Compressed Work Schedule

CWS allows employees to fulfill their 80 hour bi-weekly work requirement in less than 10 workdays. There are two types of CWS schedules: 5-4/9 and 4/10.

5-4/9 CWS. The 5-4/9 schedule features the following biweekly pay period breakout:

- Eight 9-hour workdays
- One 8-hour workday
- One Regular Day Off (RDO)

The 4-10 CWS option features the following biweekly pay period breakout:

- Four 10-hour work days
- One RDO each week

⚠ CWS must be approved by the three letter Office Chief. The 5-4/9 configuration is the preferred CWS for use within DIA.

Compressed Work Schedules are always fixed and no credit hours are permitted.

Overtime

Overtime consists of all hours worked in excess of the standard work schedule, which are officially ordered in advance by the supervisor.

Comp Time

Supervisors may grant Compensatory Time in lieu of overtime pay, which is time off (paid leave) equal to the time spent on unscheduled or scheduled overtime work.

Attention

Flexible work schedules, compensatory work schedules, overtime, credit hours, and Flexiplace are **all subject to manager approval** and not all jobs at DIA support these work options.

Credit Hours

Credit hours are hours within a flexible work schedule that an employee requests to work in excess of the basic work day in order to vary the length of a future work day. A maximum of 24 credit hours can be accepted for later use.

⚠ Employees can accumulate a credit hour balance and use those hours in place of annual or sick leave. Credit hour balance cannot exceed 24 hours.

Flexiplace (Telework)

Certain DIA employees can take advantage of Flexiplace (DIA's Telework Program) and work from home. **If you can perform at least 10% of your job in an unclassified location, you may qualify for Flexiplace.** Sit down with your supervisor and review the criteria for participation (detailed in DIA Form 158), if you are interested in learning more about Flexiplace.

Bad Weather & Emergencies

In the event of an emergency or inclement weather, please call [redacted] or [redacted] to determine if you must come to work. (b)(3):10 USC 424

?

- *How do I interpret the OPM closure, delay, or early release announcements?*

☑ ***Option One: Unscheduled Leave***
If employees can't make it to work, they can request unscheduled leave for the entire work day. Supervisors must be notified.

☑ ***Option Two: Delayed Arrival*** *Employees may arrive to work no more than XX hours later than their normal arrival time. (XX = delayed time announced by OPM)*

☑ ***Option Three: Delayed Arrival/Unscheduled Leave***
Employees may show up XX hours later than normal or request unscheduled leave if unable to report to work.

☒ ***Option Four: Closed***
Non-emergency employees will not report to work and will receive an excused absence for the number of hours they were scheduled to work.

Time & Attendance

Supervisor T&A Responsibilities

☑ Learn time and attendance policies then sign the "Time and Attendance Certifying Officer Appointment Letter", confirming your responsibilities in the T&A process

☑ Approve work schedules and work schedule changes for all your employees

☑ Return approved schedules to the timekeeper prior to the start of the pay period

☑ Provide timekeepers with documentation of all time and attendance actions

Attention

Employees, when you submit your time sheet you are certifying that it is accurate and true.

Holidays

DIA generally observes 10 legal holidays annually.

When a legal holiday falls on a Saturday, then the prior Friday is treated as a holiday; if the holiday falls on a Sunday, then the following Monday is treated as a holiday.

Working on holidays that fall between Monday-Friday will not be required unless justified by unusual circumstances.

Leave

Leave is a benefit for employees. Below are the most common types of leave:

- ❖ Annual leave
- ❖ Sick leave
- ❖ Family friendly leave (FFLA)
- ❖ Family and medical leave (FMLA)

- ▫ Providing supervisors with a tentative leave schedule helps supervisors plan workload so everyone can enjoy their vacations!
- ▫ Employees occupying critical positions are expected to report for duty on legal holidays and should see their supervisor for more details.
- ▫ Supervisors are responsible for ensuring all employees are given an opportunity for a vacation.

More details on these leave programs can be found in DIAI 1424.001.

Attention

Employees, may now leverage 3 hours of "fitness" leave each week to work out for general well being. Contact EAP to learn more about the civilian fitness leave program and to request the program enrollment form that must be turned into your supervisor.

Annual Leave

As an employee, you accrue annual leave based on the amount of time you have been a federal employee. The table below details the amount of annual leave employees accrue, by pay period and year, based on tenure.

Years of Service	Hours per Pay Period	Total Leave Days per Year
Up to 3 Years	4 Hours	13 Days
3 to 15 Years	6 Hours	20 Days
15 Years and Up	8 Hours	26 Days

Attention

Supervisors, if an employee does not show up for work or call within one hour after his/her scheduled start time it is your duty to inform [redacted]

(b)(3):10 USC 424

Accumulated annual leave remaining at the end of a calendar year can be added onto the next year's leave balance, up to 240 hours.

Except in cases of emergency, approval of annual leave should be obtained in advance from your supervisor.

> **Supervisors may advance annual leave,** but only up to the amount that an employee would earn during the remainder of the leave year.

Sick Leave

As an employee, you accrue 4 hours of sick leave per pay period. **There is no limit to the amount of sick leave you can accumulate and carry-over in later leave years.**

In the case of serious disability or ailment, you may be advanced up to 30 days of sick leave.

You can view your leave balance in eZHR.

Leave is requested and approved on an OPM Form 71 *Request for Leave or Approved Absence*. The same form is also used for requesting and approving sick leave and family friendly leave.

You must apply for sick leave as soon as possible after the beginning of your illness. If you cannot make it to work, you must call your supervisor within 1 hour after the beginning of your shift and request sick leave.

Family Friendly Leave

Family Friendly Leave is another form of leave in which DIA employees may use 40-80 hours of sick leave to:

- Provide care for a family member with physical or mental illness, injury, pregnancy, childbirth, or medical, dental or optical examination or treatment
- Make funeral arrangements for a family member or attend a funeral of a family member

Family Medical and Leave Act

This act covers an employee's son, daughter, parent or spouse; it provides employees a total of 12 administrative work weeks of leave during any 12-month period to take care of certain family medical needs.

More Leave Definitions

Leave Without Pay (LWOP) – approved leave without pay must be requested by the employee and approved by the employee's supervisor

Absence Without Leave (AWOL) – unauthorized absence from work; supervisors are advised to notify [redacted] if they believe an employee is AWOL

(b)(3):10 USC 424

Home Leave – earned during an overseas tour of duty and may be used during travel from an overseas duty station. Home leave must be taken in the United States or its territories. For each year of service abroad, DIA employees will accrue 15 days of home leave.

Court Leave – granted to employees performing jury duty or when serving as a witness.

?

- *Using your leave to travel to a foreign country?*

Make sure to call [redacted] before you leave, you have some forms to fill out.

(b)(3):10 USC 424

You must also attend an overseas security briefing and submit foreign travel request to be approved by your supervisor. The correct forms can be found on the DIA website – CI security link.

Leave Sharing Programs

Leave Transfer

Leave Transfer enables employees to donate leave on a case-by-case basis to other employees experiencing a personal or family medical emergency.

To donate leave to DIA employees you must submit OPM Form 630-A. There are some restrictions:

- ❖ You may not donate leave to your supervisor.
- ❖ You may not donate leave that has not been earned.
- ❖ Donated leave can only come from your earned "annual" leave accounts.
- ❖ Sick leave may **NOT** be donated.

?

- *Can I donate my leave to federal employees outside DIA?*

Yes! If you wish to donate leave to an employee in another federal agency, you must provide all of the necessary information about the receiving agency (recipient name, phone number, and fax number) and submit OPM Form 630-B to [redacted]

(b)(3):10 USC 424

Leave Bank

Leave Bank consists of annual leave donated by employees to a leave bank established by the Agency for use by DIA employees.

To become a leave bank member (e.g., potential recipient), you must enroll through eZHR during open season.

To participate in DIA Leave Sharing Programs as a donor or recipient, contact your directorate [redacted] who will explain any qualifying criteria and direct you to the correct OPM forms, as needed. By participating in/donating to the leave bank, DIA employees are eligible to use leave in the bank as well. DIA employees may donate accrued annual leave to the Leave Bank Program and the Leave Transfer Program in 4, 6, or 8 hour increments. **Sick leave hours cannot be donated.**

(b)(3):10 USC 424

Attention

All leave (sick leave, annual leave, etc.) must be exhausted before DIA employees can receive leave from either the leave transfer program or the leave bank.

Employee Benefits & Insurance

DIA manages a vast portfolio of employee health benefits, insurance options, and retirement plans including:

- **Health Benefits**
- **Life Insurance**
- **Long Term Care Insurance**
- **Workers Compensation**
- **Health Savings Account**
- **Retirement** Federal Employee Retirement System (FERS), Thrift Savings Plan (TSP), Civil Service Retirement System (CSRS), Social Security, and Annuity

Health Benefits

? *When can I change my enrollment?*

You can change most types of benefits during open season or when you experience a major life change, such as marriage, birth of a child, or deployment overseas.

? *When is open season?*

Open season is during November and December annually, however; changes to retirement plans may be made at any time.

? *When do changes take effect?*

Changes take effect in January.

Federal Employee Health Benefits (FEHB)

All DIA employees are eligible to enroll in the Federal Employee Health Benefits Program (FEHB).

? *What are the advantages of FEHB?*

Advantages include:

☑ Better rates than private insurance
☑ Guaranteed protection for employees and their family
☑ No examinations or restrictions
☑ A choice of plans to fit individual needs
☑ Your portion of the insurance cost is not subject to taxes
☑ Payments can be made easily through payroll
☑ Continued protection after retirement

eZHR

FEHB information is available in eZHR.

Federal Employee Group Life Insurance (FEGLI)

All DIA employees are eligible to enroll in the Federal Employees Group Life Insurance Program (FEGLI).

?
- *What are the advantages of FEGLI?*

Advantages include:

☑ Low-cost life insurance

☑ Convenient payroll deductions

☑ Protection for your family in the event of an untimely death

Once you enroll in FEGLI, you can view your life insurance information in eZHR.

Flexible Spending Accounts (FSAs)

DIA employees are eligible to participate in FSAFEDS – a Flexible Spending Account (FSA) that can save you money by allowing you to set aside **pre-tax funds to pay for a wide range of common, out-of-pocket health and dependent care expenses.**

There are two types of FSA's:

1. Health Care FSA
2. Dependent Care FSA

You can apply your Health Care FSA to many expenses not typically paid by insurance, such as:

- Co-payments and deductibles
- Acupuncture, chiropractic, and other alternative care
- Expenses that exceed your plan limits
- Home medical equipment

You can apply your Dependent Care FSA to dependent expenses that allow you and your spouse to work.

Retirement

As a DIA employee, you fall under one of three retirement plans, the **Civil Service Retirement System (CSRS), CSRS Offset, or the Federal Employee Retirement System (FERS).**

> CSRS Offset applies to employees who returned to federal service after 1983 after a break in CSRS coverage of more than one year. Employees in CSRS Offset pay into Social Security and pay a reduced amount into CSRS.

Federal Employee Retirement System (FERS)

DIA employees who began working after 1985 fall under FERS and the systems three main components:

☑ Social security benefits
☑ Basic pension benefit annuity
☑ Thrift Savings Plan (TSP)

Under this plan, you pay full social security taxes and a small contribution to the FERS Basic Benefit Plan.

Thrift Savings Plan (TSP)

The purpose of TSP is to **provide you with retirement income.** The retirement income you receive from TSP depends on how much you and your agency have contributed to the account during your working years, as well as the earnings on those contributions.

Saving money for retirement:

□ **Contribute to your TSP as soon as you are eligible.** You want to receive as much of your DIA matching contribution as possible

□ **Start saving early in your career.** Your money will grow through interest and compounding the longer it is working for you.

You may make changes to your TSP contribution at anytime. **Changes must be made in eZHR unless you do not have access to JWICS.**

?

- *FERS employees do you know how to receive FREE retirement money?*

DIA will match your TSP contribution $1 for $1 for the first 3% of salary and $.50 for $1 for the second 2% of salary.* That means if you contribute 5% of your annual income to your TSP, DIA will also contribute up to 5% to your TSP account to your retirement. You can't beat free money!

**After opening a TSP account and waiting a short period, DIA will deposit the equivalent of 1% of your basic pay to your TSP account irrespective of your contributions.*

Learn about TSP investment options at www.tsp.gov.

To receive your FREE matching contributions, you must complete and initial 6-12 months of federal service.

U.S. Savings Bonds

Did you know that as a DIA employee you can purchase U.S. savings bonds year-round by having money taken directly out of your paycheck or through paperless Treasury Direct?

www.savingsbonds.gov

The DoD Savings Bonds Program enables you to purchase bonds in the following amounts:

- $50
- $75
- $100
- $200
- $500
- $1,000

Savings bonds are not subject to the ups and downs of the stock market and always increase in value above the rate of inflation.

To participate in the DoD Savings Bonds Program complete the payroll election forms available from [redacted]

(b)(3):10 USC 424

Employee Assistance Program (EAP)

Through a suite of service offerings, EAP is available to help DIA employees reach their full performance potential. It's there to assist you through problems outside of work that might affect your health, happiness, and your interaction with others.

EAP can assist employees with issues such as:

- Work performance
- Management challenges
- Health and wellness
- Stress reduction
- Interpersonal effectiveness
- Grief and loss
- Marriage and divorce
- Legal
- Anger
- Addiction
- Motivation
- Depression
- Adjusting to changes in life
- Relaxation methods
- Time management
- Finances
- Midlife and retirement
- Caregiving
- Everyday issues
- Work and life
- Parenting and childcare
- Education
- Older adults
- Disability
- Managing people

EAP OneSource programs provide confidential counseling and referral services to all DIA employees. **EAP is available in-person, online, or by phone.**

How to Contact EAP

☎

CONUS: [redacted]

OCONUS:

Internet: www.eaponesource.com

(b)(3):10 USC 424

? ● *Is EAP confidential?*

Yes. All of EAP services, both on-site and off-site, are confidential.

? ● *When should I call EAP?*

Call anytime. Our on-site specialists provide custom assistance. Or your supervisor may refer you to EAP for a specific need.

? ● *Questions about something not listed?*

Call anyway!

Defense Civilian Intelligence Personnel System (DCIPS)

What is DCIPS?

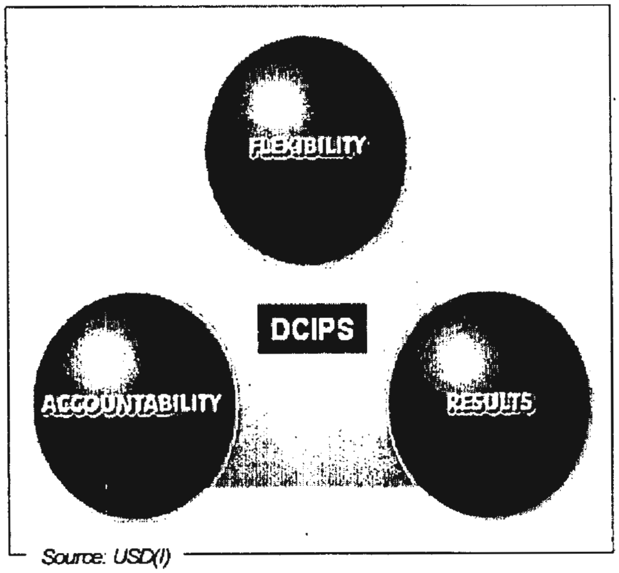
The Defense Civilian Intelligence Personnel System (DCIPS) is an enterprise-wide management system that streamlines personnel management functions and activities. It aligns the Intelligence Community (IC) under a consistent occupational framework as determined by the Under Secretary of Defense for Intelligence (USD[I]).

The DCIPS Design:

- □ **Enterprise perspective** – Reflects the principle that there is one Defense Intelligence Community (IC). Agencies and Components must function as part of the Defense Intelligence enterprise.
- □ **Consistency across the Intelligence Community** – Allows for the most effective and efficient use of available personnel and resources.
- □ **Foundation of performance** – Focuses on driving individual and organizational performance by basing compensation on performance and contributions toward meeting the mission.
- □ **Pay for performance** – Rewards individual performance through base salary increases and bonuses.
- □ **Move toward market-based pay** – Creates a competitive compensation system that makes IC organizations a more attractive option for potential candidates.

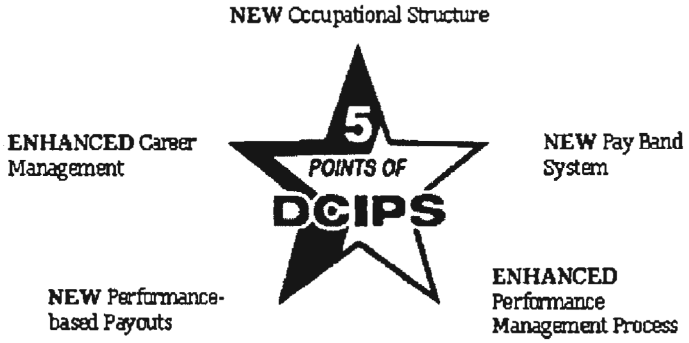
DCIPS has three (3) core goals:

- □ **Accountability:** Hold managers/supervisors accountable for properly managing their employees, and hold employees accountable for achieving results.
- □ **Flexibility:** Create a system that is flexible enough to meet the needs of the DIA workforce.
- □ **Results:** Drive individual and organizational performance towards mission accomplishment.



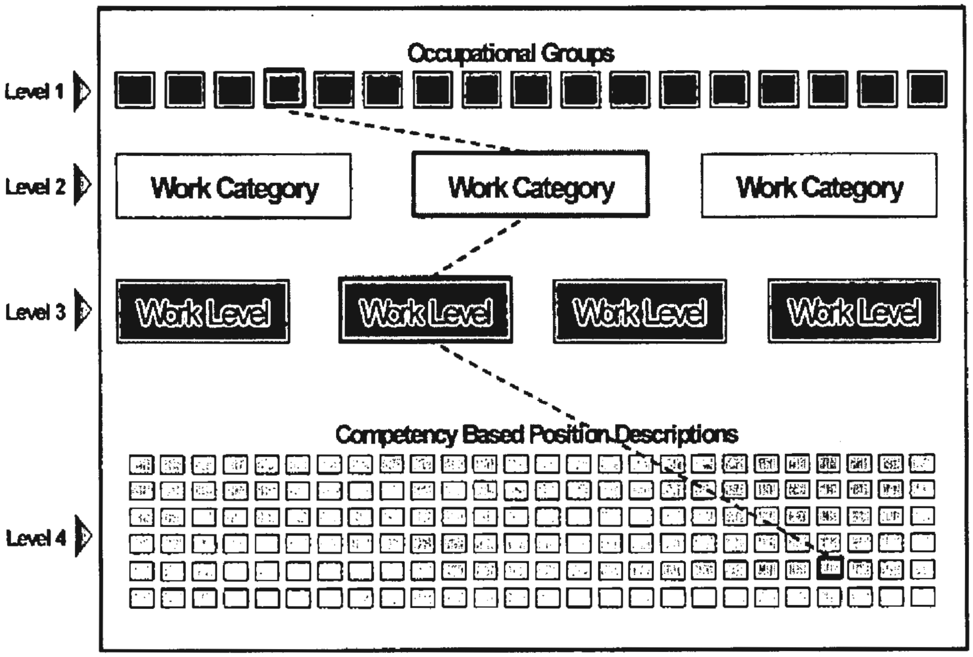
Source: USD(I)

The Five Points of DCIPS


NEW Occupational Structure
5
POINTS OF
DCIPS
ENHANCED Career Management
NEW Pay Band System
NEW Performance-based Payouts
ENHANCED Performance Management Process

New Occupational Structure

A common structure aligns the DoD IC which facilitates agility, mobility and information sharing. It includes 17 occupational groups, three work categories and 4 work levels through which all competency based position descriptions are mapped.



Occupational Groups include positions that have similar qualifications and career patterns.

DIA has 17 occupational groups identified in the table below:

Acquisition (AE)	**Human Capital (HC)**
Administration (AD)	**Information Technology (IT)**
Analysis (IA)	**Intelligence Operations (IP)**
Collection (IC)	**Legal (LG)**
Communications and Media (CO)	**Oversight and Compliance (OC)**
Education (EC)	**Science and Technology (ST)**
Facilities and Logistics (FL)	**Security (OC)**
Financial Services (FS)	**Technicians (TE)**
Health Services (HS)	

Work Categories define broad sets of work that cross related occupational series and are characterized by common qualifications and types of work. There are three categories:

Technician/Administrative Support – Work primarily involves support for the operations and functions of a particular type of work or organizational unit. Such support activities are technical or administrative in nature. Generally, qualifications are acquired through practical experience and supplemented by on-the-job or skill-specific training.

Such work tends to have fewer career progression stages and work levels.

Professional – Work that requires the interpretation and application of concepts, theories, and judgment.

□ All groups in this category require either a bachelor's degree or equivalent experience for entry.
□ Some occupations in this category have positive education requirements (that is, a requirement for a particular type or level of academic degree).

This work category features multiple career progression stages and work levels.

Supervision/Management – Work primarily involves planning, directing, and coordinating the operation of units within components; developing or executing strategy; formulating or implementing policies; overseeing daily operations; and managing material, financial, or human resources.

Work Levels define work in terms of complexity; span of authority and responsibility; level of supervision; scope and impact of decisions; and work relationships associated with a particular work category. There are four work levels:

Entry/Developmental – Work at this level in both the Professional and the Technician/Administrative Support Work Categories includes learning and applying basic procedures and acquiring competencies through training or on –the –job experience.

At this level, positions in the Technician/Administrative Support work category may involve independent performance of duties. Technician/Administrative Support positions at this work level involve positions whose primary function is the execution of established office procedures and standard program practices, and whose typical career patterns do not extend to the complexity, variety, and scope of Full Performance.

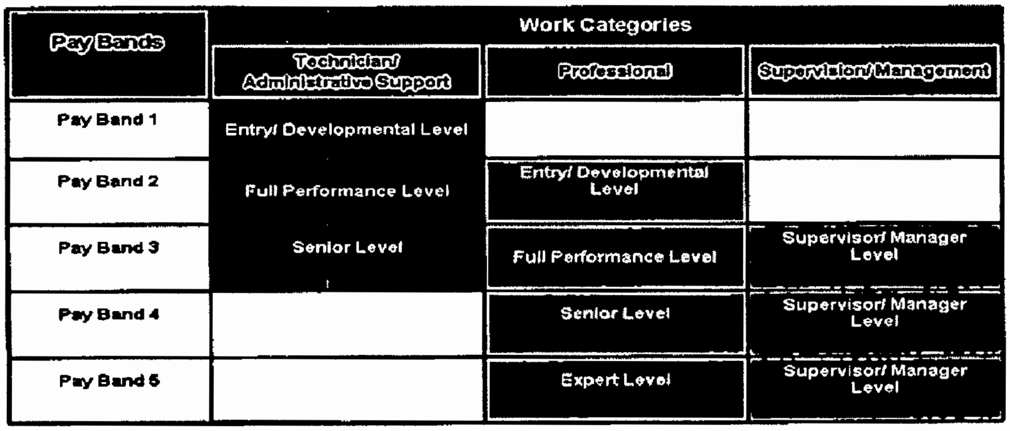
Full Performance – Involves independently performing the full range of non-supervisory duties. Employees at this level have successfully completed required entry level training or development activities, have a full understanding of the technical or specialty field, independently handle situations or assignments with minimal day-to-day instruction or supervision, and receive general guidance and direction on new projects or assignments. In short, anyone who performs his or her assignment as required without significant technical oversight.

Senior – Involves a wide range of complex assignments and non-routine situations that require extensive knowledge and experience in a technical or specialty field. Receiving broad objectives and guidelines from the manager/supervisor, senior employees independently handle a variety of complex assignments and non-routine situations and exercise independent judgment to identify and take alternative courses of action.

Expert – Involves an extraordinary degree of specialized knowledge or expertise to perform highly complex and ambiguous assignments that normally require integration and synthesis of a number of unrelated disciplines and disparate concepts. Employees at this level set priorities, goals, and deadlines, and make final determinations on how to plan and accomplish their work.

New Pay Band System

Pay is setting and administered by using five (5) pay bands; three (3) work categories (e.g., technician/administrative support, professional, supervision/management); and four (4) work levels (e.g., entry/developmental, full performance, senior, and expert) to meet the unique needs of the IC.



Pay Bands	Work Categories		
	Technician/ Administrative Support	Professional	Supervision/Management
Pay Band 1	Entry/ Developmental Level		
Pay Band 2	Full Performance Level	Entry/ Developmental Level	
Pay Band 3	Senior Level	Full Performance Level	Supervisor/ Manager Level
Pay Band 4		Senior Level	Supervisor/ Manager Level
Pay Band 5		Expert Level	Supervisor/ Manager Level

Enhanced Performance Management Process

Results-driven performance objectives and performance elements address what and how achievements are accomplished.

New Performance-based Payouts

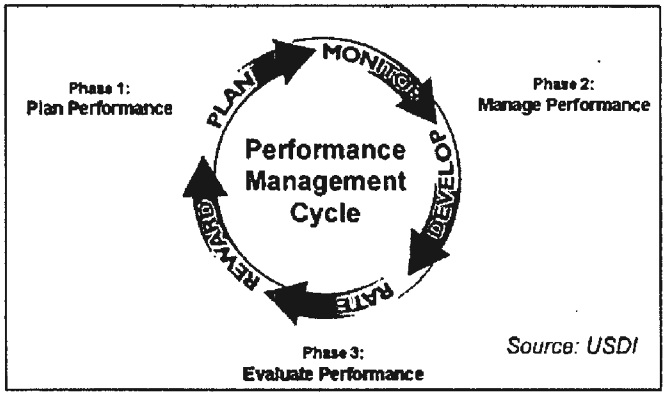
Salary and/or bonuses are directly tied to performance and results towards achieving Agency mission.

Enhanced Career Management

Enterprise-wide career development roadmaps identify developmental milestones, relevant skills and training associated with occupational specialties in support of each occupational career path.

The Performance Management Cycle

Performance management is a cyclical and ongoing process comprised of three (3) distinct phases: (1) Plan, (2) Manage, (3) Evaluate. Within the phases, there are five (5) primary activities: (1) Plan (2) Monitor (3) Develop (4) Rate (5) Reward.



Source: USDI

Phase 1: Plan Performance

Activity 1: Plan — In this phase, employees collaborate with their supervisors to develop 3 to 6 performance objectives and an individual development plan (IDP) that outlines their developmental goals for the performance appraisal period. The IDP is completed on DIA Form 200. Employees and their supervisors also discuss performance elements and how they relate to their performance objectives.

SMART Performance Objectives

Writing performance objectives is a collaborative effort between a supervisor and employee. Effective objectives:

Focus on Performance – Performance objectives should be created to bring out the best in individual and team performance.
Align with your Organization – Performance objectives must make sense in the context of the organization. Individual objectives must align with the organization's mission and goals.
Serve as an Appraisal/Management Tool – Performance objectives serve as a basis to assess accomplishments.

Well-written performance objectives enable continuous evaluation by monitoring progress, resources, and effort and allowing for corrections on the path to accomplishment. Employees and their supervisors rely on the SMART framework to help them write clear, concise, measurable statements that describe the specifics of what the employee needs to accomplish:

- □ **Specific** describes an observable action, accomplishment, or achievement.
- □ **Measurable** (or observable or verifiable) describes a method or procedure that must exist to assess and record the quality of the outcomes.
- □ **Achievable** examines capacity and conditions required to accomplish an objective.
- □ **Relevant** examines significance, value and applicability.
- □ **Time-bound** describes the performance objective start and end points.

Performance Elements

Performance elements are attributes and behaviors significant to the accomplishment of performance objectives. They explain how the performance objectives should be accomplished. There are six (6) performance elements; four (4) of which are the same for both non-supervisors and supervisors. These elements are consistent across the IC. During the planning phase, employees should consider these performance elements in developing their individual development plans (IDPs).

Non-Supervisory	Supervisory
Accountability for Results	Accountability for Results
Communication	Communication
Critical Thinking	Critical Thinking
Engagement & Collaboration	Engagement & Collaboration
Personal Leadership & Integrity	Leadership & Integrity
Technical Expertise	Managerial Proficiency

Phase 2: Manage Performance

This phase consists of monitoring and development activities. During this phase, employees engage in frequent performance discussions with the individual responsible for their performance appraisal, usually their supervisor. Employees also complete a self assessment of their performance at the midpoint of the appraisal period, and they receive a formal midpoint review from their supervisor. Throughout the year, employees and supervisors should discuss performance. In fact, it is a good idea to keep a record of accomplishments throughout the cycle.

Activity 2: Monitor — Monitoring employee performance throughout the performance year is a responsibility for both the employee and the supervisor. The midpoint review is a good opportunity for both employees and supervisors to:

- ❑ Discuss progress towards achieving performance objectives and identify ways to achieve them.
- ❑ Verify the performance objectives are still appropriate.
- ❑ Modify performance objectives if work priorities have changed since the start of the year.

At the midpoint of the performance period, both employees and rating officials complete the Midpoint Performance Review Form (DIA-Form 241). The following actions take place:

- ❑ Employees assess their accomplishments against each performance objective and performance element to date.
- ❑ Rating officials provide their assessment of employee performance for each performance objective and performance element on the same form in the relevant area.
- ❑ Rating officials specifically address areas where the employee needs improvement and documents areas for development.

Activity 3: Develop — Developing and enhancing skills is a critical component of employee success. Employees should:

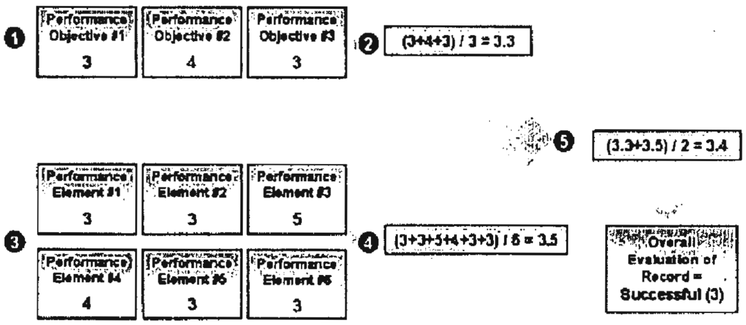
- ❑ Review their IDP to identify if there are additional areas they would like to develop.
- ❑ Discuss available training and development opportunities with their supervisor and how those opportunities would enhance their skills and their value to the organization.
- ❑ Discuss mentoring and coaching programs and professional and technical development opportunities.

Phase 3: Evaluate Performance

During this phase, employees complete a self assessment, are rated on their performance and receive an overall performance rating.

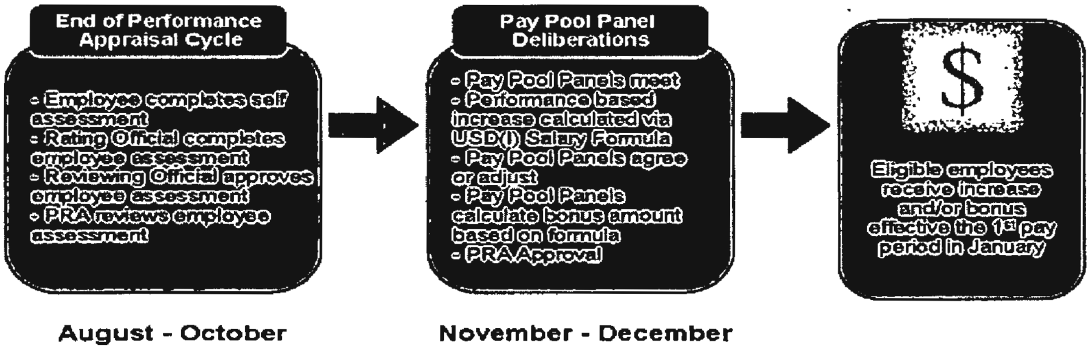
Activity 4: Rate — Rating activity begins at the end of the appraisal period. Supervisors rate employee performance based on what the employee accomplished and how they accomplished it. Employees continue to document their achievements using an Employee Self-Assessment Form (DIA Form 242).

As depicted below, the overall rating on the performance appraisal is calculated as an average of the performance objective rating and the performance element rating.



Activity 5: Reward — Rewarding employee performance is the final step in the performance management cycle and enables organizations to recognize and reward individual and team accomplishments. During this phase employees receive salary increases and bonuses based on their performance rating. Proposed salary increases and bonus decisions are reviewed at several levels of the agency to ensure consistent standards are applied in an equitable manner.

The performance management reward process is illustrated below.



End of Performance Appraisal Cycle

- Employee completes self assessment
- Rating Official completes employee assessment
- Reviewing Official approves employee assessment
- PRA reviews employee assessment

Pay Pool Panel Deliberations

- Pay Pool Panels meet
- Performance based increase calculated via USD(I) Salary Formula
- Pay Pool Panels agree or adjust
- Pay Pool Panels calculate bonus amount based on formula
- PRA Approval

Eligible employees receive increase and/or bonus effective the 1st pay period in January

August - October

November - December

DCIPS is a management system that compensates and rewards employees based on performance and contribution to the mission. DCIPS provides flexibility to move more freely across a range of work opportunities. DCIPS gives DoD the tools to foster a culture that values and recognizes talent. The entire DoD Intelligence Community is implementing a common performance management system which standardizes evaluation processes and rewards for all employees.

For questions contact the Human Capital Customer Service Hotline: [redacted] Toll (b)(3):10 USC 424
(b)(3):10 USC 424 Free [redacted] between the hours of 0700-1700

Or e-mail:
(b)(3):10 USC 424 [redacted] (JWICS) Or, type **Human Capital Customer Service** in your Outlook To: field

(b)(3):10 USC 424 [redacted] (SIPRNet) Or, type **Human Capital Customer Service** in your Outlook To: field.

11. Employees' Guide to the Standards of Conduct

Whom to Call for Advice

(b)(3):10 USC 424 The **DIA General Counsel,** [redacted] is the Designated Agency Ethics Official (DAEO) for DIA employees, both civilian and military, who serve in the Defense Intelligence Agency. The Alternate Designated Agency Ethics Officials are: [redacted] (b)(3):10 USC 424 [redacted] is the POC for ethics issues. However, all of the attorneys in the General Counsel's office are all Ethics Counselors.

Please direct your ethics and standards of conduct questions to:
DIA General Counsel
(b)(3):10 USC 424 [redacted]

Telephone
Fax [redacted] (b)(3):10 USC 424

Important Advice

If you're not positive that what you're about to do is appropriate, ask your ethics official. One mission of our office is to advise DIA personnel and assist them to accomplish their goals without violating the standards of conduct.

In fact, disciplinary action for violating the standards of conduct will **not** be taken against you if you act in good faith reliance upon the advice of your ethics official, if you have made full disclosure of the relevant circumstances.

This guide provides a general summary of the rules. It does not include every exception, every requirement, or all the factors that must be considered in making certain decisions. If you are unsure of your actions, call your ethics official before you act.

General Principles of Public Service

Don'ts	Do's
Don't use nonpublic information to benefit yourself or anyone else	Place loyalty to the Constitution, the laws, and ethical principles above private gain
Don't solicit or accept gifts from persons or parties that do business with or seek official action from DoD (unless permitted by an exception)	Act impartially to all groups, persons, and organizations
Don't make unauthorized commitments or promises that bind the Government	Give an honest effort in the performance of your duties
Don't use Federal property for unauthorized purposes	Protect and conserve Federal property
Don't take jobs or hold financial interests that conflict with your Government responsibilities	Disclose waste, fraud, abuse, and corruption to appropriate authorities
Don't take actions that give the appearance that they are illegal or unethical	Fulfill in good faith your obligations as a citizen, and pay your Federal, State, and local taxes
	Comply with all laws providing equal opportunity to all persons, regardless of their race, color, religion, sex, national origin, age, or handicap

Remember: Violating ethics principles may result in disciplinary or corrective action, including criminal prosecution. Protect yourself from disciplinary action by seeking the advice of your agency ethics official.

Gifts

Gifts From Outside Sources

Rule: You may not accept a gift given:

- Because of your **official position**, or
- By a **prohibited source**

Regardless of any exceptions that allow accepting gifts, it is **always impermissible** to:

- Accept a gift in return for being influenced in the performance of an official act. This is a bribe!
- Solicit or coerce the offering of a gift
- Accept gifts from the same or different sources so frequently that a reasonable person would think you're using your office for private gain
- Accept a gift in violation of a statute

> Patty, a DoD employee, meets informally every week with representatives of defense contractors, who customarily treat her to a small breakfast. Although an exception might permit acceptance of these small breakfasts, Patty's recurring practice of accepting them is improper.

What's a Prohibited Source?

A prohibited source is any person who is, or any organization a majority of whose members are:

- Seeking official action by DoD
- Doing or seeking to do business with DoD
- Regulated by DoD, or
- Substantially affected by the performance of <u>your</u> official duties

> Joe, a Computer.Com representative, is seeking to do business with DoD. He invites members of the acquisition dept. to a golf tournament, which his company will pay for. DoD acquisitions personnel cannot accept the gift of free golf greens fees unless an exception to the gift rule applies, because Computer.Com, by seeking to do business with DoD, is a prohibited source.

What's a Gift?

Anything of monetary value.

What's Not a Gift?

Here are examples of items that are not defined as "gifts":

- Modest items of food and refreshments (like coffee and donuts) when not served as a meal
- Prizes in contests open to the public
- Greeting cards and items with little intrinsic value, such as plaques, certificates, and trophies, intended only for presentation
- Commercial discounts available to the public or to all Government civilian or military personnel
- Anything the Government acquires by contract or otherwise legally accepts
- Anything for which you pay market value

Gifts That You May Keep

Remember, you don't have to accept a gift. It may be smart, depending on the circumstances, to decline a gift, even when it is allowed by the exceptions below.

- Gifts valued at $20 or less, **but**
  - not cash or investment interests
  - not more than $50 in total from one source in a year
- Gifts motivated by personal relationships
- Certain discounts and similar benefits offered
  - by professional organizations
  - to groups unrelated to Government employment (such as AARP)
  - to groups in which membership is related to Government employment, if the same benefits are available to other, similar organizations. (e.g.: discounted loans to Gov't. credit union members.)
  - by a *non*-prohibited source to any group as long as not discriminatory on basis of rank, type of responsibility, or pay.
- Gifts resulting from your or your spouse's outside business activities

You may accept cups of coffee offered by a contractor at no charge.

If you enter your business card in a drawing sponsored by a DoD contractor that is open to the public, you may keep the prize.

On each of his quarterly visits, a sales representative of Overpriced Computers Inc. gave Bonnie, a DoD employee, a company T-shirt, valued at $10 each. During that period, Bonnie's brother Steve, who also works for Overpriced Computers Inc., purchased for her a birthday present valued at $60. Bonnie may keep all of the gifts given to her. The T-shirts don't exceed the $50 annual limit from one source, and the gift from her brother Steve is the result of a personal, not business, relationship.

Tom was offered two tickets valued at $30 a piece to a baseball game from an employee of a defense contractor. Since the price of each ticket exceeds the $20 limit, Tom may only accept the tickets if he pays the contractor $60, the full market value of the tickets. (Paying only $40 is not permissible.)

- Free attendance provided by a state, local government, or tax exempt civic organization when there is a community relations interest
- Gifts accepted under specific statutory authority, such as certain gifts from a foreign government
- Certain educational scholarships and grants (consult a DoD ethics official)
- Free attendance, food, and entertainment (not travel) *when provided by a sponsor:*
  - of an event on the day that you are speaking or presenting information, or
  - of a widely attended gathering, provided that your supervisor determines that your attendance is in the agency's interest. (If the sponsor has interests that may be affected by you, an additional conflict of interest determination is required.)
- Free attendance, food, and entertainment (not travel) *provided by a person other than the sponsor* of a widely attended gathering, if:
  - the market value of the gift of free attendance is $285 or less and more than 100 persons are expected to attend, and
  - your supervisor determines that your attendance is in the agency's interest. (If the person has interests that may be affected by the employee, an additional conflict of interest determination is required.)
- Meals, lodging, transportation, and other benefits in connection with employment discussions
- Awards for meritorious public service or achievement, and honorary degrees – see your ethics counselor
- Travel benefits and free attendance from political organizations in connection with certain political activities
- Food and entertainment (not travel and lodging), at social events, if: (1) the invitation is not from a prohibited source, and (2) the event is free to all attendees.

On account of his DoD position, an arms trade association invites Jared, a DoD officer, to an industry-wide, one-day seminar sponsored by the association, a $200 value. He is also invited to dinner, which costs $100, at a restaurant after the seminar with several industry executives. Jared may accept the seminar invitation, provided that his supervisor determines that his attendance furthers DoD's interests. Jared may not accept the free dinner invitation, which is not part of the seminar and is closed to other interested participants.

An annual dinner is held by a veterans' service organization that costs $125 per person. Representatives from veterans' groups, Congress, and the media will attend. Several DoD employees are given free tickets by Big Guns, Inc. At the dinner, a veteran will be honored. Since it is a widely attended gathering, the DoD employee may be able to accept the free tickets if his or her ethics official determines more than 100 persons are expected to attend the event, and there is an agency interest in the DoD employee's attendance.

- Gifts of food and entertainment (not to exceed the per diem rate) at meetings or events attended in an official capacity in foreign areas, when (1) *not* provided by a foreign government **and** (2) non-U.S. citizens participate in the meeting or event

Foreign Gifts

Rule: Federal employees may accept gifts from foreign governments if the gift is below the "minimal value" which, in October 2002, is $285. Check with your ethics counselor about appraising the gift or what the current threshold is.

Disposition of Improper Gifts

Rule: If you are offered a gift that you cannot accept, you should:

- Decline the gift
- Return the gift, or
- Pay the donor the gift's market value

Attention

Subsequent reciprocity is not a solution

Under certain circumstances, perishable items may be:

- donated to charity
- destroyed
- shared within the office

(check with your ethics official)

Gifts Between Employees

Rule: You may not accept a gift from an employee who earns less than you (unless you have a personal relationship with the employee, and you are not in the chain of command)

Rule: You may not give, make a donation toward, or solicit a gift for someone superior to you in the chain of command.

Exceptions to the Rule

1. On an occasional basis, such as holidays or birthdays, you may give to a superior or receive from a subordinate:
   - Non-monetary gifts of up to $10
   - Personal hospitality provided at a residence (or an appropriate host/hostess gift),
   - Food or refreshments shared in the office
2. On special, infrequent occasions,

Bill asks his 4 coworkers each to pitch in $20 to purchase a $100 golf putter for Doreen, their boss, for Christmas. Doreen invites the office to a New Year's party, serving meals valued at $25. Bill brings a $20 bottle of wine.

- Bill may not solicit, and he and his coworkers may not give, their boss a group gift or individual gifts at Christmas that exceed $10.
- The dinner and the wine are both appropriate.

- of personal significance, such as marriage, illness, or birth or adoption of a child
- that terminate the chain of command, such as retirement, resignation, or transfer you may
- solicit voluntary contributions up to $10/person for a group gift
- give an appropriate gift to a superior
- accept appropriate gifts and group gifts that do not exceed $300 from subordinates (See your ethics counselor for exceptions.)

> Doreen decides to retire. Bill, who works for Doreen, gives her a $20 book and again solicits for a going-away gift. He would like to get her a golf-related desk set that costs about $50.
>
> - Bill may give the $20 book, as it is an appropriate gift
> - Bill may also solicit for a gift and contribute toward the group gift
> - Bill has learned his lesson and does not suggest an amount to contribute

Conflicts of Interest

Conflicting Financial Interests

Criminal Rule: You may not do government work on a particular matter that will affect the financial interest of:

- You
- Your spouse
- Your minor children
- Your general partner
- Organizations with which you're negotiating or have arrangements for future employment, **or**
- Any organization for which you serve as an employee, officer, director, trustee, or general partner

> Bryan, a DoD procurement officer, is about to award a contract for new computers. His wife, Deanna, owns a computer sales business, which has bid on the contract. Bryan may not participate in the contract award decision, since the decision will affect his wife's financial interests.

If you think you may have a conflicting financial interest, consult your DoD ethics official immediately to determine the appropriate remedy.

Bribery and Graft

Rule: You may not seek or accept anything of value, other than your salary, for being influenced in your official duties.

Commercial Dealings Between DoD Employees

Rule: You may not knowingly solicit or make solicited sales to personnel who are junior in rank, grade, or position (or their families). This includes insurance, stocks, real estate, cosmetics, household supplies, and other such goods and services.

Sue operates a cosmetics sales business out of her home after hours. During the day she is a supervisor at DoD. She may not make solicited sales to her DoD subordinates or the job or after work by calling them at home.

Representation of Others in Matters Affecting Government

Rule: You generally may not represent anyone outside the Government before a Federal agency or court, or share in any compensation for such representations made by anybody else, if the Government is involved in the particular matter.

- There are limited exceptions.
- There are special exceptions for consultants.
- Check with your ethics official.

Supplementation of Federal Salary

Rule: You may not accept compensation from any source except the Government for your services as a Government employee.

This rule does not apply, if:

- you are a "special Government employee" – *i.e.*, a consultant, or
- you serve without compensation, or
- your supplementation is a result of a public service award

Impartiality in Performing Official Duties

Rule: Maintain your impartiality. Don't participate in any particular DoD matter if:

- the matter is likely to affect the financial interest of a member of your household, or a person with whom you have a "covered relationship" is involved in the matter, and
- a reasonable person with knowledge of the relevant facts could question your impartiality.

A senior VP from Blatz Corp. recently resigned from Blatz to become a senior official in DoD. Shortly after his arrival, the official's office is tasked to decide whether or not to renew Blatz's contract with DoD. Because the senior official was employed by Blatz within the last year, he may not make the decision

Who may be in a "covered relationship?"

- A member of your household or a relative with whom you're close,
- Someone with whom you have or seek to have a business relationship, other than a routine consumer transaction,
- An organization (other than a political party) in which you actively participate,
- Someone with whom you had, within the last year, a close business relationship, such as partnership or employment, or
- Someone with whom your spouse, parent, or dependent child has (or seeks to have) a close business relationship, such as partnership or employment.

Misuse of Position

Rule: You may not use, or permit the use of, your Government position, title, or any authority associated with your office:

- To induce or coerce another person to provide any benefit to you or anyone with whom you are affiliated to imply that DoD or the Government endorses personal activities
- To imply that DoD or the Government endorses personal activities
- To endorse any product, service, or enterprise, except as provided by statute or regulation

> The General Counsel has been asked by his college to serve on the Alumni Association. He may serve in his personal capacity, but may not allow his position as General Counsel to be used on the college letterhead or other promotional literature.

Use of Government Resources

Rule: Use Federal Government equipment and property, including communications systems, only for official purposes or authorized purposes as approved by your supervisor.

Rule: Use official time in an honest effort to perform official duties, and don't ask subordinates to perform tasks outside their official duties.

> Oscar, who is the deputy director of a DoD office, is in charge of raising funds for his son's Little League team. Oscar may not ask his subordinates to contribute.

Fundraising

Rule: You may raise funds for organizations in your personal capacity, but you may not use your official title, position, or authority to fundraise, nor may you solicit subordinates or prohibited sources.

> Stu, an ethics attorney at DoD, has been offered $1500 to teach a 1-day course on Federal ethics to employees at Big Contractor, Inc. Because the topic relates to his official duties, he may not accept the compensation.

Teaching, Speaking, and Writing

Rule: You may accept payment for teaching, speaking, or writing that is unrelated to your official duties and that was not prepared on official time.

- If your employment by DoD is identified, you must make a disclaimer.

Outside Activities

Rule: If you file a financial disclosure report, you need your supervisor's prior written approval before you engage in business activity or employment with a DoD "prohibited source" (see page 2). Presidential appointees and certain non-career employees have additional restrictions – consult your ethics counselor.

Rule: You may not have outside employment or activities that would materially impair your ability to perform your duties.

Jill, who tests new computers for the office, wants to work on weekends for the vendor of those computers. Since her outside employment would cause a conflict of interest with her Government duties, she should not accept the job.

Political Activities

DIA civilian employees may NOT actively participate in political campaigns and other partisan activities. While the Hatch Act loosened restrictions on political activity for most Federal civilian employees, Federal laws still limit the political activities of military personnel, law enforcement, **national security**, and career SES employees. If you plan to engage in any partisan political activity, you should consult your ethics counselor.

Prohibited Political Activity – DIA employees *may not*:

- Participate in a permitted political activity while on duty, while in a Government office or building, or while using a Government vehicle.
- Use their official authority or influence to interfere with or affect the result of an election.
- Participate in the following political organization activities:
  - o Serving as officers of a political party or partisan group;
  - o Serving as delegates, alternates or proxies to a political party convention; and
  - o Addressing a political convention, caucus, or rally in support of or in opposition to a candidate, if done in concert with a candidate, political party, or partisan group.
- Participate in the following political fundraising activities:
  - o Soliciting or receiving political contributions;
  - o Hosting, sponsoring, managing, organizing, selling tickets to, promoting, addressing, or being a featured guest at a political fundraiser.

- Take an active part in a political campaign:
  - o Endorse or oppose a candidate in a political advertisement, broadcast, or campaign literature, in concert with a candidate, political party, or partisan group;
  - o Distribute campaign literature printed by or in concert with a candidate, political party, or partisan group; and
  - o Provide volunteer services to a political campaign.
- Run for partisan office.

Permitted Political Activities – DIA employees *may*:

- Express their political opinions publicly (but not in concert with a candidate, political party, or partisan group), which includes:
  - o Display a political sign, sticker, button, or similar material (but not while on duty, in a Government office, or using a Government vehicle.
  - o Sign a political petition.
- Be politically active in connection with a question that is not specifically identified with a political party (such as a municipal ordinance.)
- Participate in the following election-related activities:
  - o Voting;
  - o Running for non-partisan office (where political parties may not designate candidates);
  - o Serve as election judges or clerks when the law requires them to perform non-partisan duties.
- Participate in the following political organization activities:
  - o Be a member of a political party or partisan group; and
  - o Attend a political convention, caucus, or rally solely as spectators.
- Participate in the following political fundraising activities:
  - o Make a financial political contribution; and
  - o Be present at a political fundraiser solely as an attendee.

> Helen, a DIA employee, would like to place a political sticker on her POV. She drives her POV to the DIAC each day and parks in the gravel parking lot. Helen may put the sticker on her car because she is expressing her political opinion publicly, she is not on duty, and she is not in a Government building or office.

Employment Issues

Seeking Employment

Rule: If you are seeking non-Federal employment (e.g., sending resumes to select employers), you may not do Government work on a particular matter that will affect the financial interests of any of your prospective employers. You must give a written disqualification statement to your supervisor.

> Janelle, a procurement specialist, is doing work as a Government employee on a contract worth $500,000. She is offered an interview for a job by the contractor. Janelle must disqualify or recuse herself and inform her supervisor and ethics official.

Post-Government Employment

Rule: Always consult your ethics counselor before separating from the Government. He or she will advise you on the restrictions that will apply to your activities in the private sector in light of your specific duties and level of responsibility as a Government employee.

Official Travel Benefits

You may keep promotional items such as frequent flyer miles that are awarded for official travel that is funded by the Government. If Government travel is funded by a non-Federal entity, you may keep promotional items that are awarded for that travel if the non-Federal entity does not object.

You may also keep promotional items given to compensate you for being voluntarily bumped from a flight. You may voluntarily surrender your seat ONLY if doing so does not adversely affect the performance of your official duties and does not result in additional cost to the Government.

You may not keep promotional items given to compensate you for being involuntarily bumped from a flight.

Sources of Further Information

If you have further questions, consult a DIA ethics counselor in the General Counsel's office described on page ii.

Additional information is available in:

1. **Standards of Conduct for Employees of the Executive Branch**

   The U.S. Office of Government Ethics has developed a comprehensive set of regulations to assist Federal employees with their ethics questions. This is a primary source of guidance on ethics and standards of conduct. It may be found on the Office of Government Ethics website: www.usoge.gov.

2. **DoD 5500.7-R, the Joint Ethics Regulation ("JER")**

   The JER contains supplemental regulations for DoD employees.

UNCLASSIFIED

memorandum

U-733-08/GC

DATE: May 5, 2009

REPLY TO
ATTN OF: GC

SUBJECT: Initial Ethics Training

TO: New DIA Employees

REF: DoD Directive 5500.7-R, Joint Ethics Regulation

1. As a new employee of the Defense Intelligence Agency (DIA), you are required to complete initial ethics training. To satisfy this training requirement, you must read the enclosed "Employees' Guide to the Standards of Conduct." If you cannot find this document in your in-processing package, please contact [redacted]

(b)(3):10 USC 424

2. You are authorized one hour of official time to read this material. This training must be completed within **30** days of coming on board to DIA. When completed, please notify [redacted] [redacted] by either mailing or faxing the printed, legibly signed, and dated copy of this memo to Defense Intelligence Agency [redacted] Office of General Counsel, [redacted] [redacted] with your completion data.

(b)(3):10 USC 424

(b)(3):10 USC 424

3. You may wish to review additional guidance on standards of conduct issues. Additional ethics material is located on General Counsel's Homepage: [redacted]

(b)(3):10 USC 424

4. The Designated Agency Ethics Official for DIA is [redacted] General Counsel. The DIA Agency Ethics Program Manager is [redacted] Assistant General Counsel. Additional ethics counselors are available in DIA General Counsel's Office.

(b)(3):10 USC 424

(b)(3):10 USC 424

5. If you have any questions about standards of conduct issues, please feel free to contact me at [redacted] I am located in the Pentagon [redacted] I welcome you to DIA and thank you for your time and attention.

(b)(3):10 USC 424

[redacted]

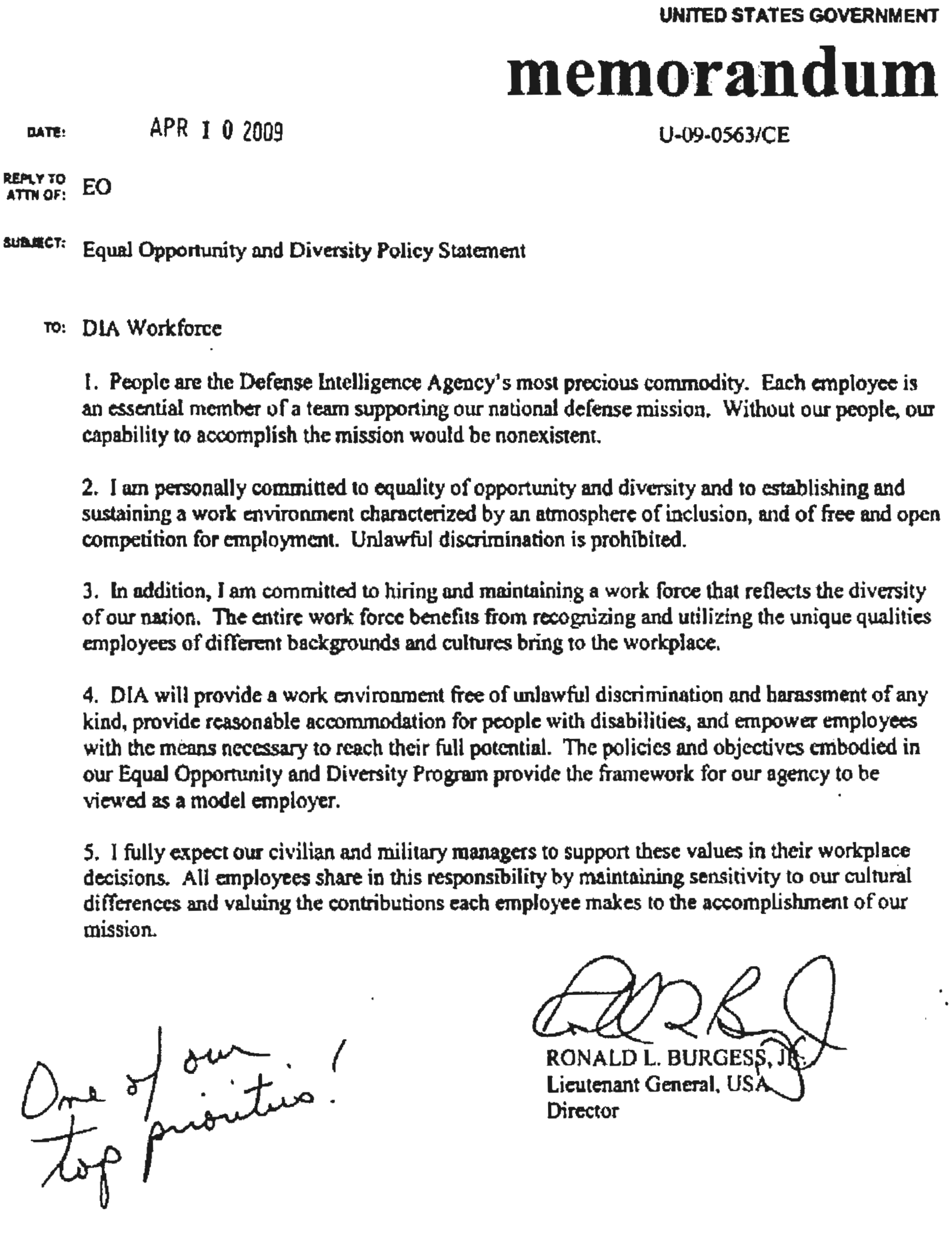
(b)(3):10 USC 424

Assistant General Counsel

I certify that I have read the "Employee's Guide to the Standards of Conduct."

Printed Name ____________________ Signature ____________________ Date ________

12. Equal Opportunity and Diversity Policy Memorandum



UNITED STATES GOVERNMENT

memorandum

DATE: APR 1 0 2009

U-09-0563/CE

REPLY TO ATTN OF: EO

SUBJECT: Equal Opportunity and Diversity Policy Statement

TO: DIA Workforce

1. People are the Defense Intelligence Agency's most precious commodity. Each employee is an essential member of a team supporting our national defense mission. Without our people, our capability to accomplish the mission would be nonexistent.

2. I am personally committed to equality of opportunity and diversity and to establishing and sustaining a work environment characterized by an atmosphere of inclusion, and of free and open competition for employment. Unlawful discrimination is prohibited.

3. In addition, I am committed to hiring and maintaining a work force that reflects the diversity of our nation. The entire work force benefits from recognizing and utilizing the unique qualities employees of different backgrounds and cultures bring to the workplace.

4. DIA will provide a work environment free of unlawful discrimination and harassment of any kind, provide reasonable accommodation for people with disabilities, and empower employees with the means necessary to reach their full potential. The policies and objectives embodied in our Equal Opportunity and Diversity Program provide the framework for our agency to be viewed as a model employer.

5. I fully expect our civilian and military managers to support these values in their workplace decisions. All employees share in this responsibility by maintaining sensitivity to our cultural differences and valuing the contributions each employee makes to the accomplishment of our mission.

RONALD L. BURGESS, JR.
Lieutenant General, USA
Director

One of our top priorities!

13. Drug Testing

General Notice of Random Drug Testing in DIA
POC: [redacted] (b)(3):10 USC 424

Memorandum

U-9387/[redacted] (b)(3):10 USC 424

REPLY TO ATTN OF: DR

SUBJECT: General Notice of Random Drug Testing in DIA

REFERENCES:

a. Executive Order 12564, 15 September 1986.

b. DIA Manual 22-17, "Drug-Free Federal Work Place Program."

TO: Distribution F

1. The purpose of this notice is to remind the work force of the Department of Defense (DoD) guidance that has effected the number of civilian random drug tests conducted at DIA.

2. In 1986, the President issued Executive Order 12564, which mandated specific actions to assure the objective of a drug-free Federal workplace. Since then, DoD has been in the forefront in developing and implementing effective drug testing programs for its work force. DIA, based on its sensitive intelligence mission, has an especially compelling obligation to continue taking the necessary steps to eliminate illegal drug use from its workplace.

3. DIA civilians have been subject to random drug tests since 1989. However, until now, there has never been an annual requirement to test a specified percentage of the civilian work force. DoD guidance now calls for each organization to randomly test 50 percent of its civilian work force.

4. To meet this requirement, the [redacted] has increased the frequency of testing, and the number of DIA civilian employees to be tested each month. Therefore, there is a very good possibility that an employee may be selected for testing more than once. If selected for random testing, an employee will be notified through his/her supervisor of the date, time, and place of the test on the same

(b)(3):10 USC 424

day that the test is scheduled. Selection for random testing in no way implies that an employee is under suspicion of using drugs.

5. All DIA employees have a mandatory obligation to be tested when contacted. They are required to participate, regardless of whether or not they were previously tested. Managers must treat this requirement as a **priority** and ensure their employees take the test when notified.

6. Employees who are found to use illegal drugs or refuse to take a scheduled drug test will be subject to the full range of disciplinary actions authorized under DIA regulations. Disciplinary action may be mitigated when an employee voluntarily admits to illegal drug use, obtains required counseling and/or rehabilitation, and thereafter refrains from using illegal drugs.

7. DIA's drug free environment continues to be a testimonial to the integrity of our employees and the overall success of a multifaceted approach to monitoring employee welfare.

14. Hand Carrying Classified Documents

Do

Plan well in advance so that the material will be waiting for you at your destination. Make every effort to send material via secure means (i.e., registered U.S. mail, the Defense Courier Service (DCS)). Consider hand carrying as your last resort. Let courier professionals do the job.

Prior to Leaving

☑ Obtain written authorization
☑ Travel orders/theatre clearance
☑ Courier card (regardless of mode of travel)
☑ Courier Letter of Authorization (if traveling by commercial aircraft)
☑ Get a travel briefing (within 6 months of travel)
☑ Make arrangements for any overnight storage. Obtain a receipt for any temporary storage. Classified material must be stored only at an accredited facility.
☑ Make a list of materials you will carry and leave the list at your office
☑ Double wrap materials
☑ Arrange to have the classified material shipped back via a normal secure means (registered U.S. mail or DCS)
☑ Use secure FAX machines to send materials that do not require original signatures

While Hand Carrying

☑ Keep materials in your possession at all times
☑ Report security incidents immediately upon arrival at an accredited facility or your destination (whichever comes first)

If Traveling by Commercial Aircraft

☑ Ensure all airlines are U.S. carriers, or that no U.S. carrier is available before using a foreign carrier
☑ Arrange with destination's point of contact for passage through non-U.S. Customs checkpoints **and** have in your possession:
  - Courier Authorization Card
  - Courier Letter of Authorization (original, signed copy)

DO NOT

☒ Read, display, or use materials in public
☒ Leave materials unattended
☒ Wait until the last minute to decide what classified material should be taken

- ☒ Take the material home with you before, or after your trip, or store it in your hotel room
- ☒ Think that because you hand carried the material to your destination, that you have to hand carry it back
- ☒ Hand carry unless there is no other way to get it there

Attention

(b)(3):10 USC 424

[redacted] **for additional assistance or to report problems encountered during couriering**

References

DIAR 50-2, "Information Security Program," Chapter 5, Appendix C.
DoD S-5105.21.-M-1, "Sensitive Compartmented Information Administrative Security Manual," Chapter 3.

15. Information Systems Security (INFOSEC) Guidelines

System Protection/Antiviral Practices

Passwords

Passwords are issued to individuals for their use only. Giving your password to another person is in violation of DIAR 50-23. Protect passwords, when combined with user account names, at the highest classification level of the system to which the passwords allow access.

Individual Account Protection

To ensure individual account and system protection, users must use the screen lock function or log-off the system each time they leave their workstation. For the purposes of the workday, activating a password-protected screen locking mechanism is considered secure. Users are required to logoff when departing for the day. Failure to secure the workstation by using screen lock or logging off is a practice dangerous to security and may result in adverse administrative action.

Non-DIA Software

Requests for approval to use non-standard DIA software, including free and unsolicited demonstration software, must be signed by a division chief or higher official before submitting to the DIA [redacted] Approval to use and install non-DIA software can be requested through the [redacted]

(b)(3):10 USC 424

Personally-Owned Software

Personally-owned software, regardless of source, may not be introduced into DIA computers.

Modems

Use of modems in DIA is controlled and managed. Modem connection to computers may be approved as outlined in DIAM 50-24. A division chief or higher official must submit a request for modem connection to [redacted] Approval is site and configuration specific.

(b)(3):10 USC 424

Escort Responsibility

The individual providing escort duty is responsible for ensuring the person being escorted does not gain access to a DIA automated information system. Failure to do so may result in a security incident and adverse administrative action.

Classification Markings

Media Labels

All removable magnetic media must bear a label indicating the classification level of information to which the media contains. A color-coded security classification label, for example an SF-712 for SCI, must be affixed to media and computer processors such as CPUs, laser printers, and external drives.

Place the labels in a conspicuous place on the media and processors where they will not adversely affect operation of the equipment.

Marking

Users will ensure that all output contains proper classification and control markings and is adequately protected. This includes all messages and correspondence generated on electronic mail systems. Automatic classification marking systems or macros are encouraged.

Media Control & Accountability

Copying Files

When copying or moving files between systems with differing classifications, users must follow INFOSEC SOP 1 to ensure the proper data are copied or moved. Each LSA cell has software utilities to assist in the execution of secure copy procedures.

Processing Restrictions

(b)(3):10 USC 424

Information systems connected to DIA LANs can process, store, and transmit Top Secret SCI information. Processing of Top Secret [redacted] Limited Distribution (LIMDIS), and Special Access Program (SAP) information is restricted to accredited, stand-alone computers.

Processing Violations

(b)(3):50 USC 3024(i)

(b)(3):10 USC 424

If information other than TS SI/[redacted] is inadvertently processed on the DIA LAN, report the incident immediately to the [redacted] [redacted] The contaminated workstations(s) will be disconnected from the network and sanitized. User LAN and workstations will be isolated until all media, workstations, and the file server are scanned and cleaned.

Destruction

Removable Media

Destroy removable media as non-pulpable classified waste. It is not necessary to cut diskettes into pieces or remove the ribbon from the cartridge. However, removal of the hard plastic is required.

Laser Toner Cartridges

Laser printer toner cartridges will be recycled rather than disposed of as waste. Prior to recycling, the cartridges must be desensitized by running at least five **full** pages of unclassified, randomly generated text through the machine before the cartridge is removed. These pages should not include any blank spaces or solid black areas. Used laser printer toner cartridges should be placed in the cardboard box that the new cartridge was shipped in, or any cardboard box. The exhausted toner cartridges should be turned into the local supply store on a one-for-one exchange basis for new laser toner cartridges.

16. Deployment

DIA employees may be required to deploy overseas during their careers. After reading this section, employees will better understand management expectations and responsibilities surrounding each of the main phases of a DIA deployment.

Curious about what deployment might mean for you? In this section you'll find useful information and examples in the following areas:

(b)(3):10 USC 424 [redacted]

- ❖ Employee responsibilities
- ❖ Deployment prep and training
- ❖ Benefits
- ❖ Time and attendance
- ❖ Redeployment

Deployment and Deployment Prep

From your official selection to your return to station, [redacted] (b)(3):10 USC 424 will coordinate command and control.

Attention

Supervisors: You are required to excuse the selected employee from normal duties as necessary to facilitate completion of pre-deployment requirements.

Deployment Key Players

Directorates and Special Offices are responsible for:

☑ **Identifying** personnel with the skills and abilities that match mission requirements

☑ **Nominating** personnel for deployment by completing the nomination form

☑ **Notifying** the supervisor and employee of a deployment selection

(b)(3):10 USC 424 ☑ **Coordinating** [redacted]

(b)(3):10 USC 424 **The** [redacted] **is responsible for:**

☑ **Conducting** pre and post administrative processing and providing logistical support

(b)(3):10 USC 424 ☑ **Appointing** [redacted] for deployment preparation and administration

☑ **Scheduling** and administering required training and country briefings; coordinating with the [redacted] to notify employees of training (b)(3):10 USC 424

☑ **Identifying** requirements for region, country, and security clearances

☑ **Providing** date and time of the pre-deployment briefings

The employee's supervisor is responsible for:

☑ Ensuring that deployed personnel are considered for special recognition, promotion, and other awards, with input from in-theater supervisors
☑ Confirming that performance appraisals are finalized for the period of time that their employee was deployed, with input from in-theatre supervisor
☑ Creating and communicating new performance expectations for recently returned employees within 30 days from return to duty
☑ Ensuring that returning employees are fully and meaningfully reintegrated into the organization

While preparing for your deployment EAP offers assistance with the preparation, transition and support for you and your family. **Let EAP work for you!**

Pre Deployment

(b)(3):10 USC 424

At the [redacted] you will have the opportunity to:

- ❖ Receive immunizations
- ❖ Participate in deployment training
- ❖ Attend deployment briefings

Medical Requirements

(b)(3):10 USC 424

All employees are required to obtain a pre-deployment health assessment prior to visiting [redacted]

(b)(3):10 USC 424

[redacted] will provide you with immunizations appropriate to your deployment destination.

Training

(b)(3):10 USC 424

[redacted]

(b)(3):10 USC 424

[redacted]

Here's what else you can expect to receive from your pre-deployment experience:

☑ Common Access Card with Geneva Convention Category and overseas use authorization

☑ Legal documentation (wills) and identification tags

☑ Military equipment

☑ Medical and dental screening records and a record of required immunizations received

☑ Weapons qualification sheet

Pre Deployment Briefing

(b)(3):10 USC 424

Your [redacted] will brief you one final time prior to your deployment into the theater of operations on:

☑ Weather, seasonal changes, and recommended attire in your theater of operations

☑ Local customs and traditions

☑ Communications and correspondence, including mailing addresses and telecommunication information

☑ Personnel and security issues

☑ Flight information and pre-flight meeting time/place

Deployment Benefits

Health Insurance

While deployed, your regular health care benefits are covered under the Federal Employees Health Benefits Program, which has a number of worldwide options.

Life Insurance

Deployment to a combat zone does not cancel your FEGLI coverage.

While deployed, you are eligible for coverage under the Federal Employees Group Life Insurance Program (FEGLI).

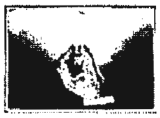
Civilian employees sent to a war/combat zone in a support role will keep FEGLI coverage as well as Accidental Death and Dismemberment (AD&D) coverage.

Federal Employee's Compensation Act

The Federal Employee's Compensation Act (FECA) provides benefits to you if you are injured during the performance of duty while on deployment, or if you acquire an employment-related disease while on deployment. FECA also enables your dependents to collect benefits in the event you are injured or succumb to disease or death.

Expect a **Benefits Briefing** from HCH that will guide you through specifics on:

- Pay and allowances
- Life insurance
- Workers' compensation
- Disability benefits
- Beneficiary forms



- If you previously waived basic life insurance under FEGLI, you may sign up for FEGLI prior to your deployment.

T&A Reporting During Employment

While deployed, make sure your deployment supervisor submits your timesheets via fax or email to your DIA supervisor.

DIA supervisors: You must ensure that you receive your employees' T&A sheets with the signature (or originating email address) of the on-scene temporary supervisors.

Deployment Pay

Your compensation may vary while on deployment. Due to long/irregular hours, physical hardships, and dangerous conditions, your salary may be impacted in the following ways:

☑ **Premium Pay** - paid to a civilian employee during deployment while working on holidays, weekends, or late at night.

☑ **Incentive for Voluntary Deployment** – voluntary employees may receive **$8,000 for 179 day** deployment and **$16,000 for 365 day** deployment.

Attention

The voluntary deployment incentive payment is separate from annual directorate and agency bonuses. Deployed personnel must still be considered for annual directorate and agency bonuses.

☑ **Post Differential Pay** – variable percentage of basic compensation granted to employees at posts with very difficult living conditions, excessive physical hardship, or notably unhealthy conditions.

You must serve at least 42 days at the post authorized to receive post differential pay.

☑ **Danger Pay** - Up to 35% of basic pay (established by the Secretary of State) granted to employees when civil insurrection, civil war, terrorism or wartime conditions threaten physical harm or imminent danger to the health or well-being of a majority of employees officially stationed at a post in a foreign area.

To receive payment of, the deployment incentive, post differential, and danger pay, you must submit a copy of your travel orders and vouchers to [redacted] once you return from deployment.

(b)(3):10 USC 424

Redeployment – Coming Home

While on deployment, a DIA in-theater point of contact is available to help you coordinate your redeployment. You should contact your POC at least 30 to 60 days prior to your scheduled return date.

Redeployment Briefing

(b)(3):10 USC 424

Upon return, you are required to contact [redacted] to schedule a redeployment briefing and to return your military equipment (when provided).

The in-theater POC will inform you of your:

- ❖ Passenger flight information
- ❖ Departure date
- ❖ Arrival date
- ❖ Arrival location
- ❖ Special needs

Redeployment Administrative Leave

Upon return, supervisors are required to grant employees up to 5 days of administrative leave **in addition to approved liberal use of annual leave.** This allows employees to reunite with family and friends and receive some much needed rest and relaxation. After this administrative leave period, supervisors typically assign returning DIA employees to half-time duty days during the first full week back to their respective directorate or special office.

Here are some leave guidelines on reintegrating employees:

If deployed for 1 to 2 months	☑ 1 duty day of admin leave for civilians ☑ 24-hour pass for military personnel
If deployed for 2 to 4 months	☑ 3 duty days of admin leave for civilians ☑ 72-hour pass for military personnel
If deployed for 4 to 12 months	☑ 5 duty days of admin leave for civilians ☑ 96-hour pass and one duty day for military personnel

(b)(3):10 USC 424

Upon your return, you will be contacted by [redacted] to schedule reintegration briefings, which will cover:

- ☑ Amendments to travel orders/arrangements
- ☑ Reimbursements for travel expenses
- ☑ Payment of danger and foreign post-differential pay
- ☑ Return of equipment including weapons
- ☑ Return of atropine and 2-pam chloride auto-injectors
- ☑ Mandatory medical screenings
- ☑ Reasonable accommodation information
- ☑ Reintegration seminar

?

- *How can employees better prepare their families for their deployment?*

EAP conducts educational seminars for deployed personnel, which identify the emotional cycle of deployment return and preparation for returning.

Deployment Appraisal

Deployments of 90 days or more

If you are going to deploy for 90 days or more, your DIA supervisor will render a close-out appraisal prior to your departure.

Once you deploy to your new duty location, your in-theatre/rater will document your performance expectations for the period of your deployment.

⚠ You may receive more than one performance appraisal, which will be kept on file by DIA.

Deployments of Less than 90 days

If you will be deployed for less than 90 days, performance expectations will not be required. Your in-theater supervisor will document your significant accomplishments and report these accomplishments back to your DIA supervisor

Attention

Supervisors

Get in touch with your employee's in-theater supervisor to determine whether your employee should be nominated for an award. Have the in-theater supervisor fill out the nomination form.

Recognizing Employees

Supervisors are encouraged to recognize the performance of employees returning from deployed assignments.

Awards available include:

- **The DIA Civilian Expeditionary Medal (DCEM)**
- **The DIA Civilian Combat Support Award**
- **The DIA Civilian Mission Support Certificate**
- **The Armed Forces Civilian Service Medal (AFCSM)**
- **The Defense of Freedom Medal**

17. Awards

Supervisors, civilian employees, and military personnel should read this chapter to find out information on:

- Supervisor award responsibilities
- Civilian and military awards comparison chart
- Awards ceremony overview

Supervisors, you should learn as much as possible about available awards to ensure your top performers receive the recognition and decoration they deserve.
Awards **help improve employee retention and raise morale.**

Attention

Awards should only be given out to deserving employees. Supervisors, you should only use awards to recognize exceptional performance and on-the-job achievement.

When nominating and preparing military awards, contact your directorate's senior Service Advisor (SSA) or Senior Enlisted Advisor (SEA) for assistance.

Attention

You are not guaranteed an award!
Supervisors should only use awards to recognize exceptional performance and on-the-job achievement.

Award Responsibilities

Office Chiefs & Division Level Supervisors Role:

- Identify exceptional performance and make appropriate award recommendations
- Ensure that supervisors review suggestions and constructive ideas for their organization's rewards needs
- Ensure that supervisors comply with EEO policies
- Approve on-the-spot awards for $100-$450 and time-off awards up to 40 hours
- Ensure that employees are only recognized once per act of exceptional performance

Supervisors Role:

- Initiate award recommendations and process them through your chain of command
- Identify exceptional performance and make appropriate recommendations
- Compile an award justification memo noting the recommended type of award and other supplemental information

- Encourage employees to nominate their peers for awards and to also call out exceptional performance
- Approve on-the-spot awards for $100-$450 and time-off awards for up to 8 hours

Attention

Nomination procedures differ for almost every type of award. Initiate award nominations through your directorate's [redacted] or Awards POC.

(b)(3):10 USC 424

For a complete list of awards, checklists, and nomination procedures please see the HC Awards Website [redacted]

(b)(3):10 USC 424

Awards Comparison Table

Civilian Awards	Military Awards
Presidents Award for Distinguished Federal Civilian Employees (*Equal to DSSM when the employee is at a lower level than the Director)	Defense Distinguished Service Medal or *Defense Superior Service Medal (DSSM)
DoD Medal for Distinguished Civilian Service (Highest DoD Award)	Defense Superior Service Medal
Secretary of Defense Meritorious Civilian Service Medal (DoD 2nd highest Award)	Legion of Merit
Defense of Freedom Medal	Purple Heart
Office of the Secretary Defense Medal for Exceptional Civilian Service	Defense Meritorious Service Medal
Office of the Secretary of Defense Medal for Valor	Joint Service Commendation Medal with Valor
Joint Civilian Service Commendation Award	Joint Service Commendation Medal
Joint Civilian Service Achievement Award	Joint Service Achievement Medal
SecDef Medal for the Global War on Terrorism	Global War on Terrorism Expeditionary Medal
Armed Forces Civilian Service Medal	Armed Forces Service Medal
DIA Specific Awards	
DIA Award for Exceptional Civilian Service	Defense Superior Service Medal
DIA Award for Meritorious Civilian Service (New)	Defense Meritorious Service Medal
DIA Civilian Combat Support Award	Joint Service Commendation Medal with Valor
Defense Intelligence Director's Award	Joint Service Commendation Medal
DIA Civilian Mission Support Certificate	Joint Service Achievement Medal
DIA Civilian Achievement Medal (New)	Joint Service Achievement Medal
DIA Director's Award for Humanitarian Service	Humanitarian Service Medal
DIA Public Service Award (non-career federal only)	Military Outstanding Volunteer Service Medal
DIA Directorate and Special Office Level Bonus DIA Award for Excellence (New)	DIA Annual Military Officer/Enlisted Person of the Year
DIA Certificate of Commendation	Letter of Commendation
DIA Certificate of Appreciation	Letter of Appreciation or Certificate of Achievement
DIA Special Act Award	Certificate of Achievement
DIA On-the-Spot Award	Certificate of Achievement or Coin
DIA Time Off Award	Military Pass
Suggestions, Inventions, and Scientific Achievement	Military Suggestion Award
National Intelligence Cross (IC Award)	Military Also Eligible
National Intelligence Medal for Valor (IC Award)	Military Also Eligible
National Intelligence Distinguished Service Medal (IC Award)	Military Also Eligible
National Intelligence Superior Service Medal (IC Award)	Military Also Eligible
National Intelligence Reform Medal (IC Award)	Military Also Eligible
Exceptional Achievement Medal (IC Award)	Military Also Eligible
National Intelligence Meritorious Unit Citation (IC Award)	Military Also Eligible

National Intelligence Medallion (IC Award)	Military Also Eligible
National Intelligence Certificate of Distinction (IC Award)	Military Also Eligible
The Director of National Intelligence's Award for Collaboration Leadership (IC Award)	Military Also Eligible
Galileo Award (IC Award)	Military Also Eligible
Intelligence Community EEO and Diversity Exemplary Leadership Award (IC Award)	Military Also Eligible
Intelligence Community EEO and Diversity Outstanding Achievement Award (IC Award)	Military Also Eligible
Distinguished Public Service Medal (IC Award)	N/A
Superior Public Service Medal (IC Award)	N/A
IC Expeditionary Service Medal	Military Also Eligible
Joint Duty Service Device	N/A
DIA Director's Annual Agency Team Award	Military Also Eligible
DIA Teamwork Award	Military Also Eligible
DIA Diversity Management Award	Military Also Eligible
DIA Outstanding Employee with a Disability Award	Military Also Eligible

Awards Ceremony

All awards should be presented in an informal or formal ceremony so the employee knows the value of their service, and others may appreciate their contributions. A ceremony will emphasize the award is recognizing a significant achievement.

Tips on Conducting an Awards Ceremony

If you plan to conduct a formal awards ceremony, consult the Civilian Awards Program Policy found on the Civilian Awards and Recognition website [redacted] Another great resource for preparing and conducting an award ceremony are your directorate Senior Service Advisor or Senior Enlisted Advisor.

(b)(3):10 USC 424

18. eZHR

eZHR is the application employees and supervisors use to view, update, and maintain personnel and training records. You will find eZHR from the DIA Internal Communications Page – under Important Links – click "eZHR." You will sign-in to eZHR using your DIA-issued DoDIIS user ID and password.

What You Can View in eZHR

- DIA personnel actions
- Pay information
- Leave balance
- Administrative information
- Life and health insurance
- Retirement plan
- TSP
- Military service
- Foreign language proficiency pay
- Position description
- Rating chain information
- Performance appraisal information
- Passport and Visa Information
- Position Description

⚠The most common eZHR tasks will be found under "My Civilian eZHR Self-Service."

What You Can Do in eZHR

☑ Enroll to receive your Leave and Earnings Statement (LES) electronically
☑ Update diversity information
☑ Self-certify education
☑ Certify completed training
☑ Learn about available training and enroll in courses
☑ Add honors and awards
☑ Update your work experience
☑ Record a name change
☑ Enter address changes
☑ Update emergency contact information
☑ Enroll in or change your TSP allocations
☑ Enroll in Telework
☑ Sign up for Leave Bank
☑ Self-certify your foreign language skills
☑ Self-certify licenses and certificates
☑ Check on emergency designation
☑ Enroll employees in training
☑ Submit employees for awards

☑ Complete trial-period assessments
☑ Document record of counseling
☑ Access analyst resource catalog and competencies
☑ Apply for civilian jobs at DIA
☑ Create your civilian resume

eZHR Forms

eZHR Forms

eZHR Forms allows supervisors and employees to complete, track, and print civilian performance appraisal documentation.

What Supervisors Do in eZHR Forms

☑ Document employee performance objectives for the upcoming rating period
☑ Conduct a mid-point review of employee performance
☑ Supply supplemental appraisal input for short-duration assignments
☑ Record rater assessments, including narrative comments and numerical ratings

What Employees Do in eZHR Forms

☑ Document employee self assessment of progress during the rating period
☑ Review and acknowledge the receipt of performance objectives, mid-point review, supplemental appraisals and the annual close-out appraisal

What Reviewers Do in eZHR Forms

☑ Review and approval of employee objectives
☑ Provide narrative comments to support the overall rating

eZHR Training On-Demand

Training On-Demand shows employees and supervisors how to do anything and everything in eZHR and eZHR Forms.

Training On-Demand is an interactive online learning tool. On-Demand gives you a choice of how you would like your question answered.

?

● *How do I access eZHR Training On-Demand?*

Select the eZHR Training On-Demand, or eZHR Forms Training On-Demand from the eZHR (or eZHR Forms) homepage.

See It

In the **"see it"** mode, you sit back and watch the computer show you how a task is completed. The training uses screen shots from eZHR.

Try It

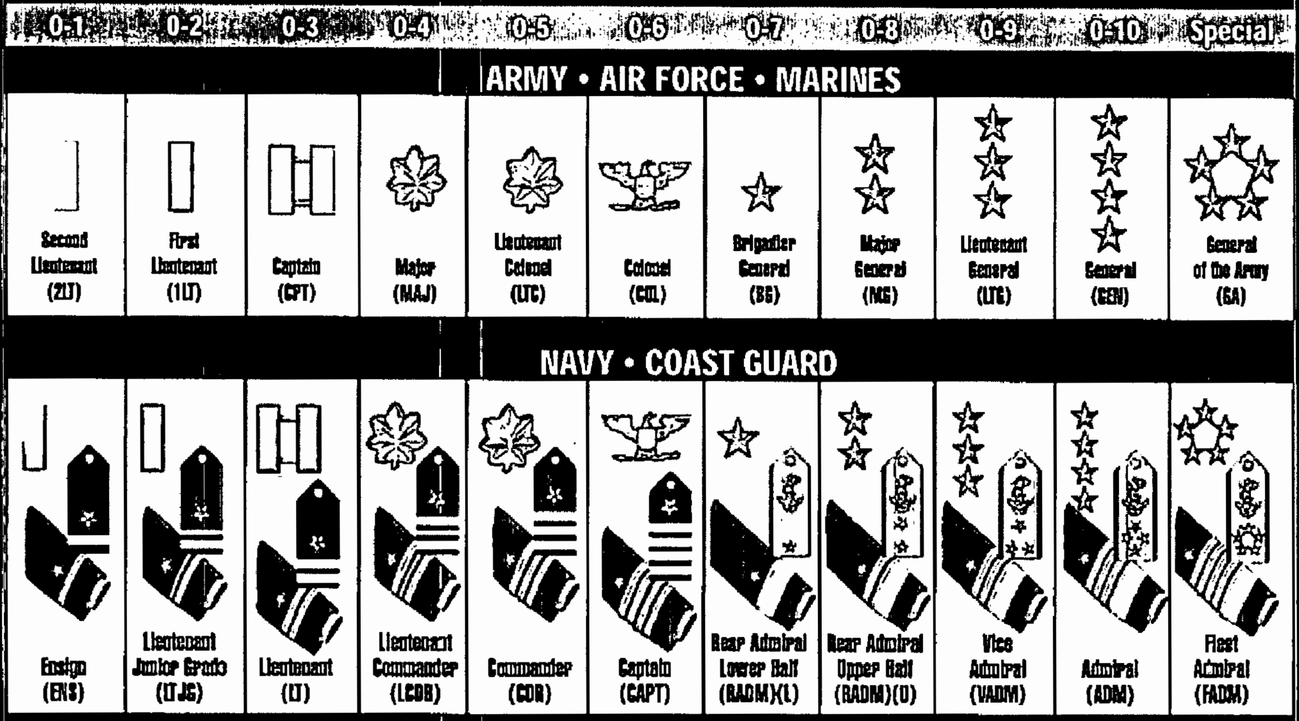
In the **"try it"** mode, you are asked to click through screenshots in order to practice clicking where appropriate to complete the task.

Do It

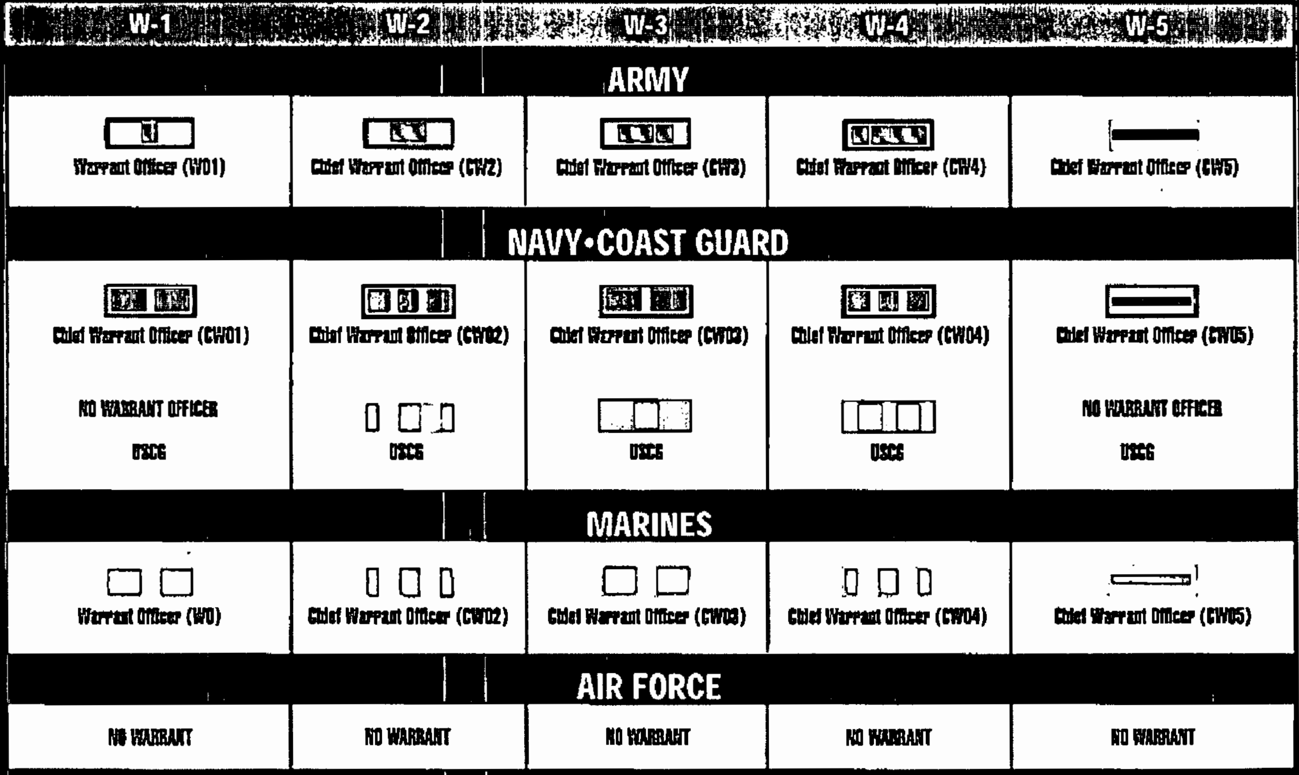
In the **"do it"** mode, a separate screen opens with text and pictures telling you how to accomplish the task. **The benefit of the "do it" mode is that you can actually use eZHR and have the "do it" window open to show you how to use eZHR at the same time.**

> ⚠ In the **"see it"** and **"try it"** modes eZHR will not be affected. In the **"do it"** mode eZHR will only be affected if you choose to use eZHR while using the training screen.

Insignia of the United States Armed Forces – OFFICERS

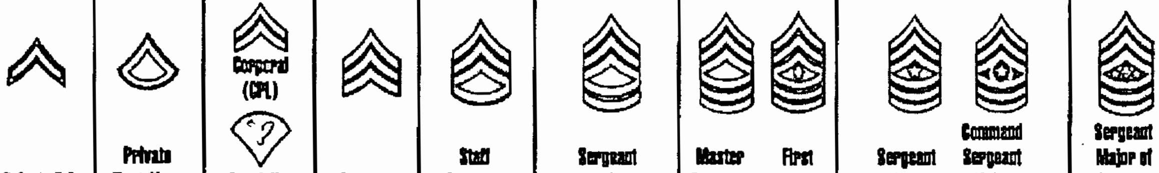


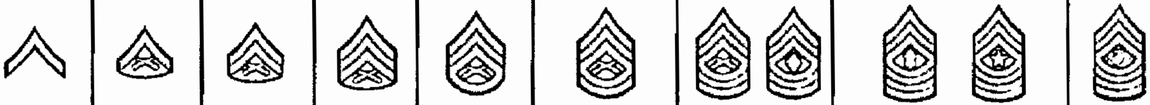
O-1	O-2	O-3	O-4	O-5	O-6	O-7	O-8	O-9	O-10	Special
ARMY • AIR FORCE • MARINES										
Second Lieutenant (2LT)	First Lieutenant (1LT)	Captain (CPT)	Major (MAJ)	Lieutenant Colonel (LTC)	Colonel (COL)	Brigadier General (BG)	Major General (MG)	Lieutenant General (LTG)	General (GEN)	General of the Army (GA)
NAVY • COAST GUARD										
Ensign (ENS)	Lieutenant Junior Grade (LTJG)	Lieutenant (LT)	Lieutenant Commander (LCDR)	Commander (CDR)	Captain (CAPT)	Rear Admiral Lower Half (RADM)(L)	Rear Admiral Upper Half (RADM)(U)	Vice Admiral (VADM)	Admiral (ADM)	Fleet Admiral (FADM)

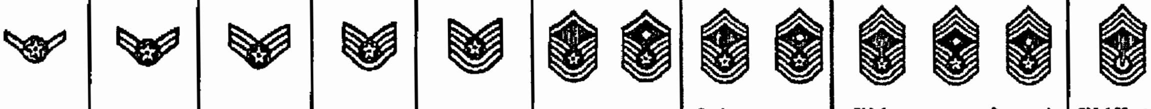


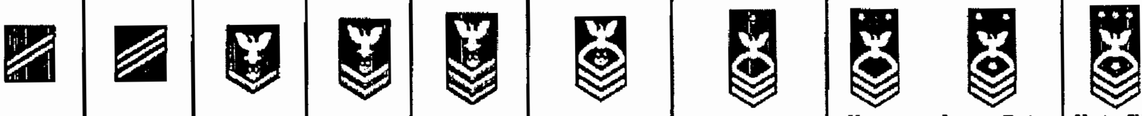
W-1	W-2	W-3	W-4	W-5
ARMY				
Warrant Officer (WO1)	Chief Warrant Officer (CW2)	Chief Warrant Officer (CW3)	Chief Warrant Officer (CW4)	Chief Warrant Officer (CW5)
NAVY•COAST GUARD				
Chief Warrant Officer (CWO1) NO WARRANT OFFICER USCG	Chief Warrant Officer (CWO2) USCG	Chief Warrant Officer (CWO3) USCG	Chief Warrant Officer (CWO4) USCG	Chief Warrant Officer (CWO5) NO WARRANT OFFICER USCG
MARINES				
Warrant Officer (WO)	Chief Warrant Officer (CWO2)	Chief Warrant Officer (CWO3)	Chief Warrant Officer (CWO4)	Chief Warrant Officer (CWO5)
AIR FORCE				
NO WARRANT	NO WARRANT	NO WARRANT	NO WARRANT	NO WARRANT

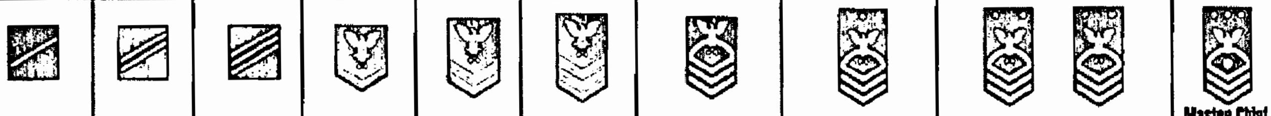
Insignia of the United States Armed Forces — ENLISTED









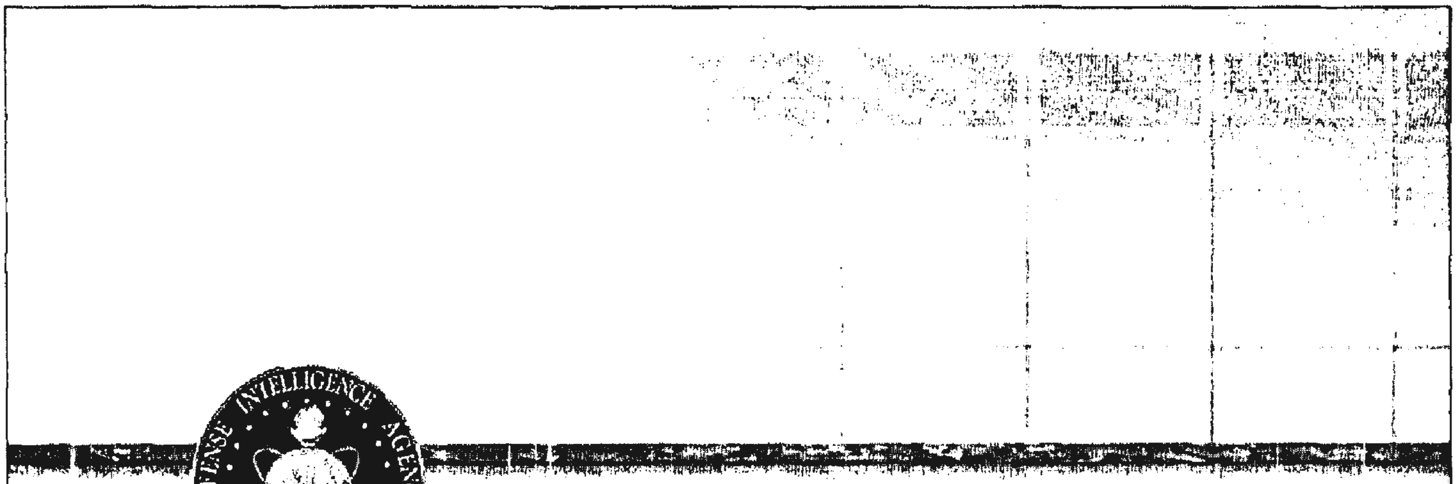


	E-1	E-2	E-3	E-4	E-5	E-6	E-7	E-8	E-9	Senior Enlisted Advisors
ARMY	no insignia Private E-1 (PV1)	Private E-2 (PV2)	Private First Class (PFC)	Corporal (CPL) Specialist (SPC)	Sergeant (SGT)	Staff Sergeant (SSG)	Sergeant First Class (SFC)	Master Sergeant (MSG) First Sergeant (1SG)	Sergeant Major (SGM) Command Sergeant Major (CSM)	Sergeant Major of the Army (SMA)
MARINES	no insignia Private (Pvt)	Private First (PFC)	Lance Corporal (LCpl)	Corporal (Cpl)	Sergeant (Sgt)	Staff Sergeant (SSgt)	Gunnery Sergeant (GySgt)	Master Sergeant (MSgt) First Sergeant (1stSgt)	Master Gunnery Sergeant (MGySgt) Sergeant Major (SgtMaj)	Sergeant Major of the Marine Corps (SgtMajMC)
AIR FORCE	no insignia Airman Basic (AB)	Airman (Amn)	Airman First Class (A1C)	Senior Airman (SrA)	Staff Sergeant (SSgt)	Technical Sergeant (TSgt)	Master Sergeant (MSgt) First Sergeant (E-7)	Senior Master Sergeant (SMSgt) First Sergeant (E-8)	Chief Master Sergeant (CMSgt) First Sergeant (E-9) Command Chief Master Sergeant (CCM)	Chief Master Sergeant of the Air Force (CMSAF)
NAVY	no insignia Seaman Recruit (SR)	Seaman Apprentice (SA)	Seaman (SN)	Petty Officer Third Class (PO3)	Petty Officer Second Class (PO2)	Petty Officer First Class (PO1)	Chief Petty Officer (CPO)	Senior Chief Petty Officer (SCPO)	Master Chief Petty Officer (MCPO) Force or Fleet Command Master Chief Petty Officer (FORMC) (FLTMC)	Master Chief Petty Officer of the Navy (MCPON)
COAST GUARD	Seaman Recruit (SR)	Seaman Apprentice (SA)	Seaman (SN)	Petty Officer Third Class (PO3)	Petty Officer Second Class (PO2)	Petty Officer First Class (PO1)	Chief Petty Officer (CPO)	Senior Chief Petty Officer (SCPO)	Master Chief Petty Officer (MCPO) Command Master Chief (CMC)	Master Chief Petty Officer of the Coast Guard (MCPO-CG)

Source: www.defenselink.mil

20. DIA Strategic Plan 2007 – 2012

“The primary focus of DIA at this time is to prevail in the Global War on Terrorism (GWOT) by providing insight, knowledge, and actionable intelligence to leaders and operations. To do so well requires the continuous renewal and adaptation of our resources and capabilities to ensure we achieve persistent penetration of the adversary.”



Strategic Plan
2007–2012

Leading the Defense Intelligence Enterprise

Defense Intelligence Agency
Committed to Excellence in Defense of the Nation

Mission

Provide timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers.

Vision

Integration of highly skilled intelligence professionals with leading edge technology to discover information and create knowledge that provides warning, identifies opportunities, and delivers overwhelming advantage to our warfighters, defense planners, and defense and national security policymakers.

Values

We are committed to...

- Service to our community and our fellow citizens.
- Dedication, strength, and urgency of purpose to provide for our nation's defense.
- Customer-focus in the products and services we provide.
- Integrity and accountability in all of our actions and activities.
- Inquiry, truth, and continuous learning.
- Creativity and innovation in solving problems, discovering facts, and creating knowledge.
- Teamwork through international and external partnerships.
- Leadership at all levels within defense intelligence and the Intelligence Community.

Table of Contents

> Our nation is engaged in a long war against terrorism and violent extremism. Providing support to our Soldiers, Sailors, Airmen, and Marines engaged in insurgencies in Iraq and Afghanistan and the Global War on Terrorism is our first priority.
>
> – Lieutenant General Michael D. Maples, US Army, DIA Director

Director's Letter

Commanders and policymakers rely on military intelligence professionals to make sense of our world — to offer depth of insight, ensure accuracy and timeliness of information, and provide warning. Irregular warfare and the Global War on Terrorism require agile operational forces and precise weaponry — both of which are highly information-centric. To succeed, our armed forces and military leaders require the right information delivered at the right time in the right form. This is no small challenge.

DIA will meet this challenge and continue to evolve as a leading intelligence combat support agency, by focusing on five major strategic actions:

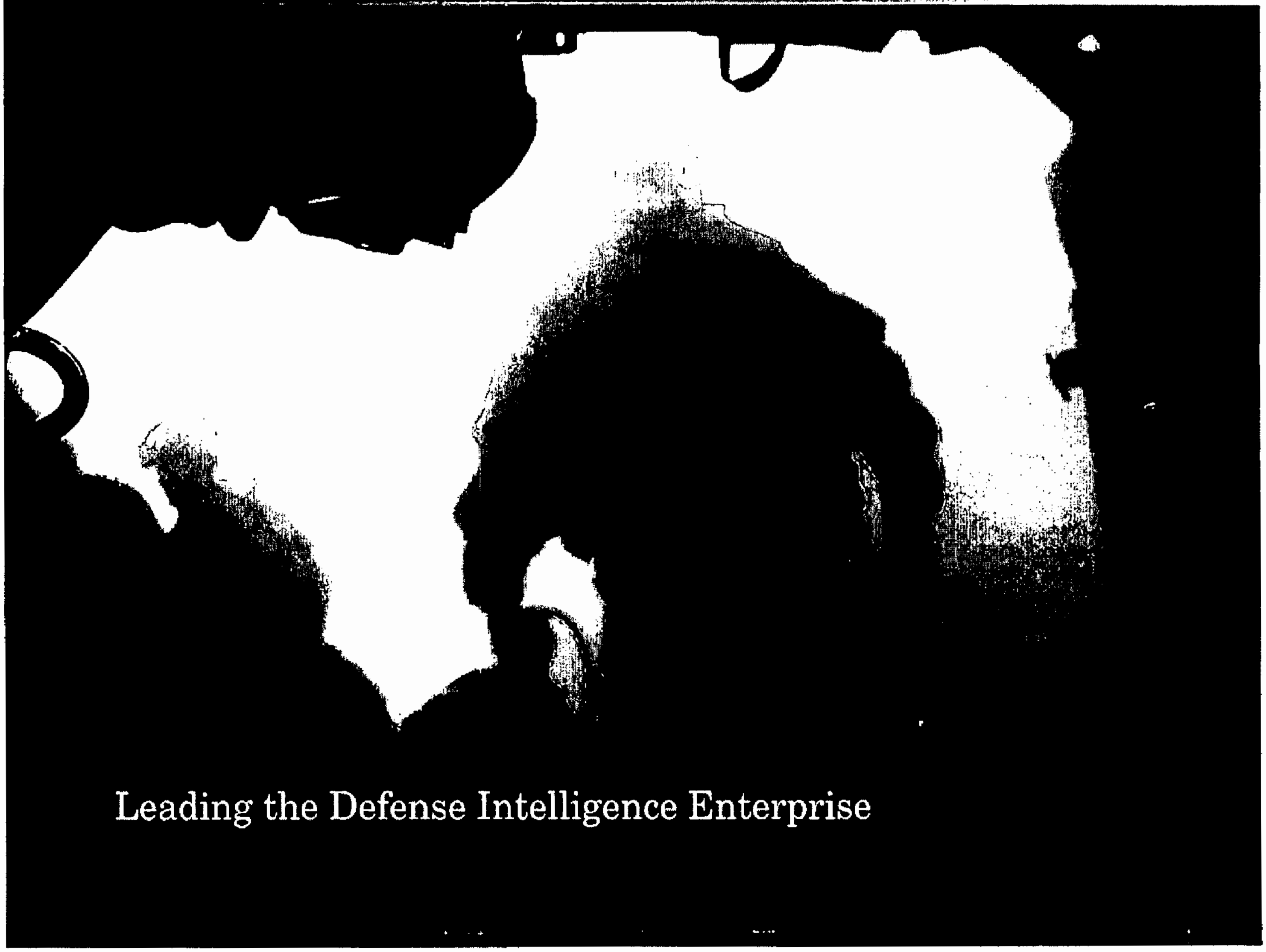
- Build an agile, forward-looking organization able to provide intelligence depth and warning integrated into US military operations.
- Strengthen human, analytic and technological capabilities to remain ahead of our adversaries through advanced collection and analysis.
- Support unification of effort across the Intelligence Community to promote horizontal integration fostering access to data and sharing of information.
- Recruit, develop, and retain a diverse, results-oriented intelligence workforce to ensure the right skills and competencies are in place.
- Establish high quality, modern and scalable human, technical and financial support systems to maximize all available resources.

This plan demonstrates DIA's commitment to continuous improvement in pursuit of defense intelligence excellence. It points to our rapid evolution as a global combat support agency in the face of changing military operations. And it speaks to our efforts to build new, more effective capabilities to advance the mission of DIA and its partners.

I am proud of the hard work and dedication of the DIA workforce. I am also proud of your contributions to our armed forces and your service to our Nation. I thank you for your shared commitment to the important initiatives and actions outlined in this Strategic Plan for DIA.

MICHAEL D. MAPLES
Lieutenant General, USA
Director

Introduction



Leading the Defense Intelligence Enterprise

The Intelligence Reform and Terrorism Prevention Act, the National Security Strategy, the National Defense Strategy, the Quadrennial Defense Review, the formation of the Office of the Director of National Intelligence (ODNI), and the National Intelligence Strategy (NIS) represent an extraordinary period of change for intelligence.

A critical outcome of this transition will be the creation of a highly integrated and interconnected Defense Intelligence Enterprise. This construct will serve as a critical link between defense and national priorities, and will horizontally integrate the people, systems and processes that comprise the individual components of intelligence.

Defense Intelligence Enterprise *— the Defense Intelligence Community (organizations within the Department of Defense (DoD) that have an intelligence mission and/or function), plus all of their stakeholders. Stakeholders — entities and interests that are involved in creating, sustaining, and enhancing the mission capacity, either voluntarily or involuntarily, of the enterprise. Enterprise — the nodal element within a network of interrelated stakeholders.*

To achieve this, DIA and its partners must work together to achieve a shared vision encompassing five fundamental imperatives:

Sustain the Fight in the Global War on Terrorism

The primary focus of DIA at this time is to prevail in the Global War on Terrorism (GWOT) by providing insight, knowledge, and actionable intelligence to leaders and operators. To do so well requires the continuous renewal and adaptation of our resources and capabilities to ensure we achieve persistent penetration of the adversary.

The GWOT, and our increased focus on irregular warfare capabilities, moves intelligence to the operational center. It requires the intelligence professional and operator to be integrated and fully engaged in collection, analysis, and production of actionable intelligence in the fight against terrorists and to prevent the proliferation of weapons of mass destruction.

Irregular Warfare *— a form of warfare that has as its objective the credibility and/or legitimacy of the relevant political authority with the goal of undermining or supporting that authority. Irregular warfare favors indirect approaches, though it may employ the full range of military and other capabilities to seek asymmetric approaches, in order to erode an adversary's power, influence, and will.*

Plan and Support Defense Operations

Achieving a new level of integration between the intelligence professional and the operator will be accomplished nationally through the Defense Joint Intelligence Operations Center (DJIOC) and regionally through combatant command (COCOM) JIOCs including all-source intelligence campaign planning (ICP) capabilities.

The JIOCs will form the basis of a collaborative, interactive relationship with national and defense intelligence agencies, COCOM JIOCs, COCOM analytical and collection elements, military service intelligence organizations, and the Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance (JFCC-ISR).

***The Defense Joint Intelligence Operations Center** — established to integrate and synchronize military and national intelligence capabilities. The DJIOC will plan, prepare, integrate, direct, manage, and synchronize continuous, full-spectrum defense intelligence operations in support of the combatant commands.*

Achieve Defense Intelligence Unity of Effort

Achievement of true unity of effort among members of the Defense Intelligence Enterprise will come through the joint creation of policies, processes, and systems that encourage and facilitate access, sharing, and interoperability. DIA will lead this effort by coordinating capabilities and resources in ways aimed at better serving the customer.

The drive towards coordination includes building new programs as needed and the integration of the defense intelligence initiatives already underway, including the DoD Intelligence Information System (DoDIIS) Way Ahead, the Defense Intelligence Analysis Program (DIAP), the Defense HUMINT Management Office (DHMO), and others.

Support the Office of the Director of National Intelligence

As a provider of all-source defense intelligence, DIA is uniquely positioned to serve as a critical link between national and defense capabilities and priorities. This strategic plan lays the groundwork for this through the development of goals and objectives aligned in support of the NIS.

In the years ahead, DIA will seek to develop and support initiatives that establish a collaborative, interactive relationship with the ODNI to ensure that defense and national priorities are managed in a coordinated and synchronized approach. The desired outcome will be the continuously more efficient use of resources.

Develop the Defense Intelligence Enterprise

DIA is committed to transforming defense intelligence into an enterprise that supports integration and synchronization of collection, analysis, planning, and management activities. The resultant Defense Intelligence Enterprise construct will enable access to the totality of intelligence resources and more effectively meet the needs of national and defense customers.

Complex global operations, transnational threats, and the evolution of an enhanced national intelligence structure will require new organizing principles. The Defense Intelligence Enterprise will take shape as a central organizing principle, particularly as the Defense and COCOM JIOC components are refined in the years ahead.

The culmination of our efforts will be to achieve human and technological platforms that can deliver faster, better, and more efficient intelligence to consumers. The purpose of this strategic plan is to identify the necessary goals and objectives central to achieving this vision for DIA and an integrated Defense Intelligence Enterprise.

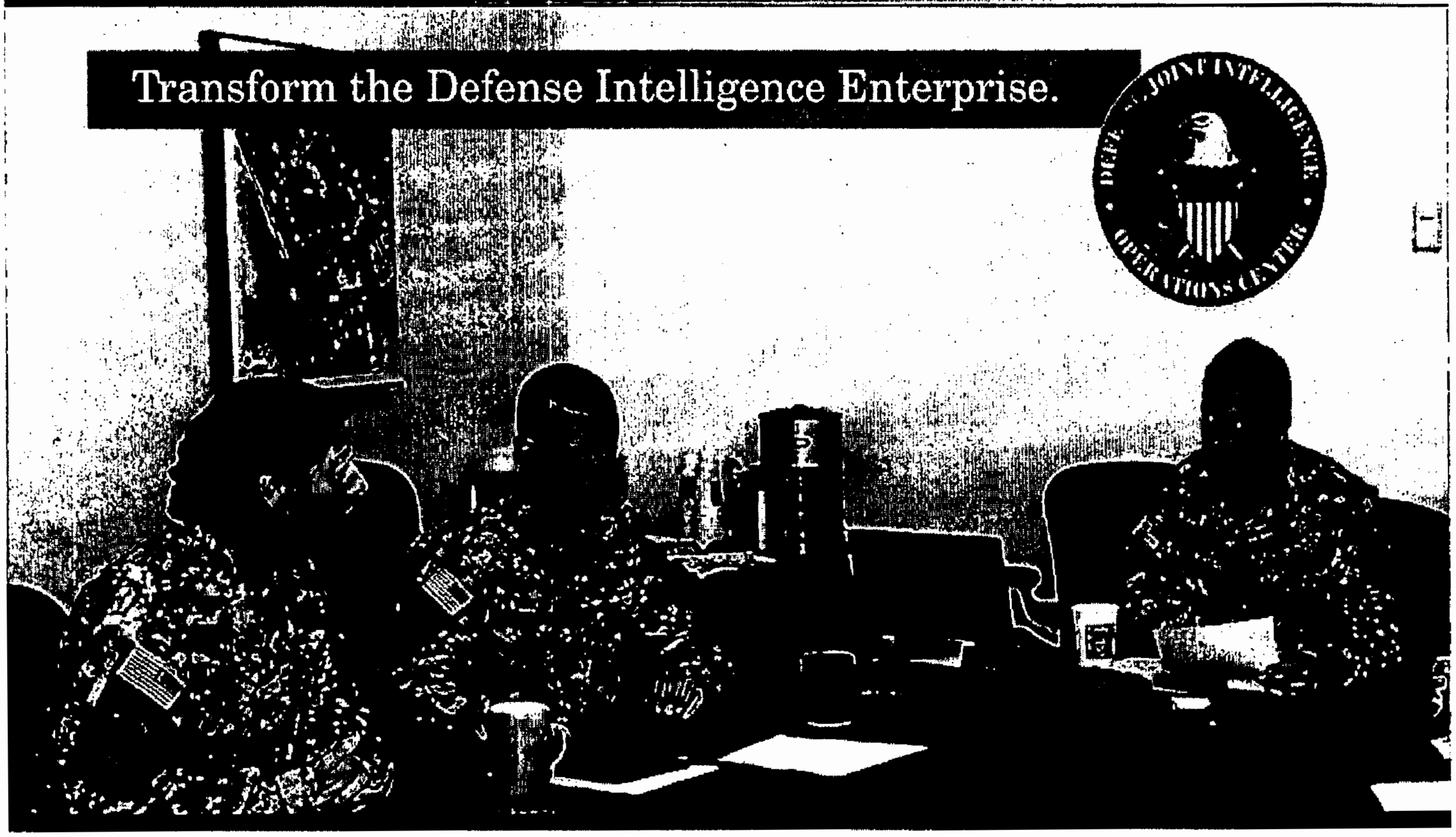
Goals

Section I:	Enhance Mission Management
Goal 1	Transform the Defense Intelligence Enterprise.
Goal 2	Achieve next generation collection capabilities.
Goal 3	Produce the right intelligence for the right customer at the right time.
Goal 4	Create a knowledge-based culture.

Section II:	Enhance Enterprise Management
Goal 5	Attract, develop, and retain a results-focused workforce.
Goal 6	Provide superior resource and organization management.
Goal 7	Sustain a culture of continuous improvement.
Goal 8	Provide the optimal work environment.

Goal 1

Transform the Defense Intelligence Enterprise.



DIA's commitment to the Nation is to prevail in the Global War on Terrorism, prevent and counter the spread of weapons of mass destruction, bolster the growth of democracy, and anticipate developments of strategic concern and opportunity. This requires a collective effort. To achieve this, the Agency is committed to transforming individual capabilities into a cohesive, integrated Defense Intelligence Enterprise.

DIA's Director will lead this effort nationally through the Defense Joint Intelligence Operations Center and regionally through the combatant command Joint Intelligence Operations Centers. The Agency will sustain integration through co-location of multi-agency resources, implementation of interoperable technology, a global force management (GFM) capability, and all-source intelligence campaign planning (ICP) at the national and theater levels.

Objective 1.1

Enable the DJIOC and COCOM JIOCs to fully implement Horizontal Integration through the Defense Intelligence Enterprise.

DIA will use the DJIOC to synchronize assessments, planning, deconfliction, and execution of intelligence activities across agencies and theaters, creating a horizontally integrated enterprise. The DJIOC will form the basis of a collaborative, interactive relationship between national and defense intelligence agencies, COCOM JIOCs, COCOM analytical and collection elements, Service intelligence organizations, and the Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance. The Agency will institutionalize a fully integrated Defense Intelligence Enterprise, networked and enabled by an enterprise Information Technology (IT) architecture. DIA will:

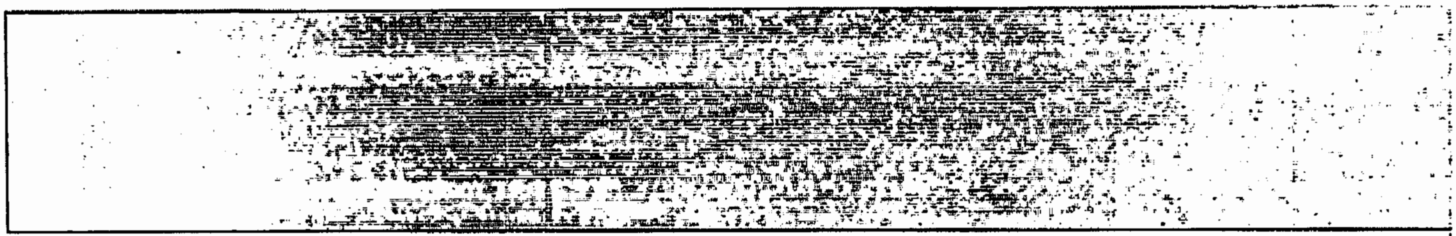
- Improve national-level operational support to the COCOMs through a centrally coordinated all-source DJIOC providing collection, processing, and planning services involving both defense and national intelligence assets.
- Improve theater-level operational support to the COCOMs through regionally focused all-source JIOCs, providing collection, processing, and planning services involving both defense and national intelligence assets.
- Achieve an integrated and interoperable IT infrastructure for the Defense Intelligence Enterprise that incorporates the Department of Defense Intelligence Information System (DoDIIS) architecture and ensures seamless integration between all strategic, operational and tactical intelligence components.
- Identify innovative practices and technologies developed in support of the DJIOC and COCOM JIOCs that can be implemented across the Defense Intelligence Enterprise to enhance integration and unity of effort.

Objective 1.2

Build a full range of Intelligence Campaign Planning capabilities to promote a cohesive, integrated approach to intelligence campaign development.

DIA will support an ICP process that will identify, plan, and apply all defense and national intelligence capabilities against policy, strategic, operational, and target objectives. An effective ICP process will yield actionable plans directing the synchronized and sequenced application of intelligence assets. This process will encompass the full range of intelligence requirements from strategic to tactical, will identify intelligence gaps and vulnerabilities, and will exploit intelligence targets to support operational objectives. DIA will:

- Develop a rigorous, integrated ICP process to produce plans for the synchronized and sequenced application of intelligence assets against objectives.
- Evaluate and monitor the effectiveness of intelligence plans, operations, and processes, and adjust as needed to achieve desired results.

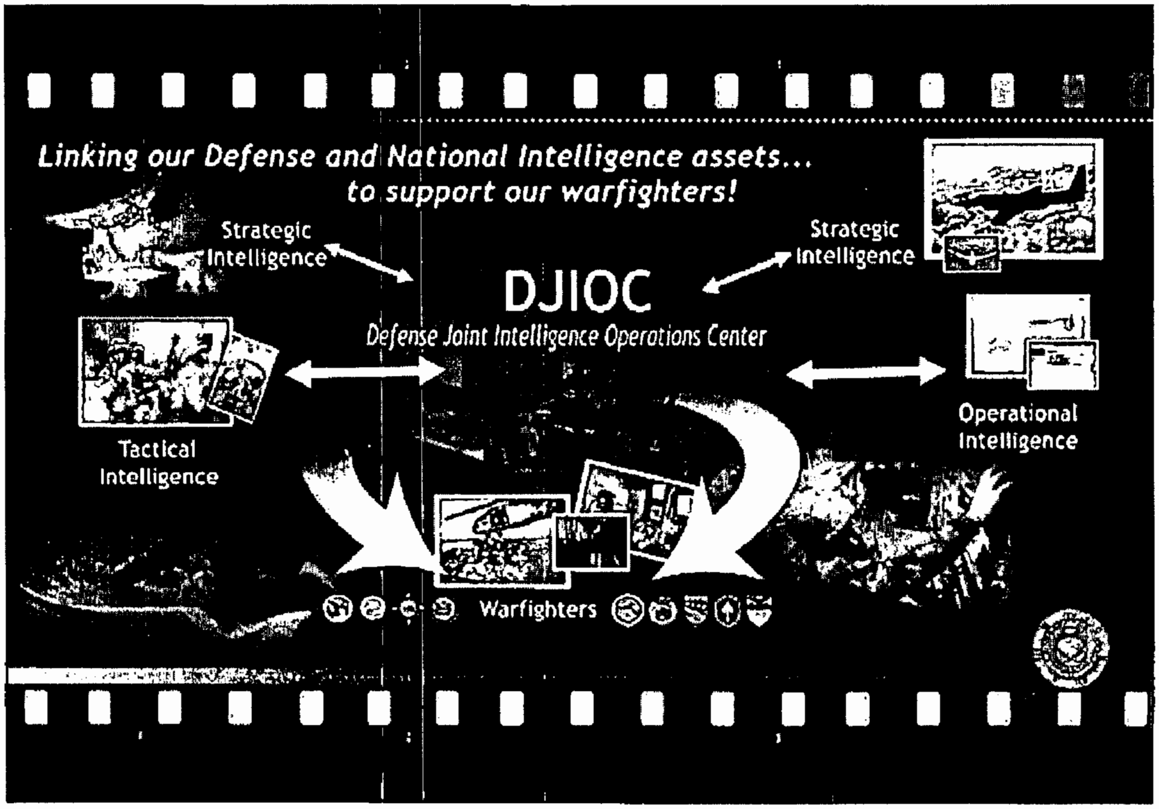


Objective 1.3

Develop and implement a comprehensive Global Force Management approach to achieve unity of effort across the Defense Intelligence Enterprise.

DIA's approach to GFM supports the DoD methodology for force and resource apportionment, assignment, and allocation. In addition, the approach will provide increased visibility into force availability and an improved mechanism for the assessment of risk. The combination will allow DIA to harness resources and capabilities better worldwide and across defense intelligence programs, resulting in a more agile and responsive decision making environment. DIA will:

- Develop a process and associated applications, data and services to provide the DJIOC with the ability to identify available Blue Force capabilities including: highlighting those that are interchangeable between theaters, allocating them against priority requirements, and providing the means to mitigate intelligence capability shortfalls.
- Through implementation of GFM, instill in the Defense Intelligence Enterprise the ability to become more efficient and effective stewards of defense intelligence assets.
- Hone our partner relationships across public and private sectors, at home and abroad, engaging our collective capabilities to address today's complex security challenges.


Linking our Defense and National Intelligence assets...
to support our warfighters!
Strategic Intelligence
Strategic Intelligence
DJIOC
Defense Joint Intelligence Operations Center
Tactical Intelligence
Operational Intelligence
Warfighters

Goal 2

Achieve next generation collection capabilities.

DIA will advance its ability to provide unique capabilities to operators and leaders by addressing collection shortfalls across the Defense Intelligence Enterprise. The Agency will increase investment in the development of innovative human intelligence (HUMINT) and technical collection capabilities to achieve a higher degree of persistent surveillance and warning capability through improved collection techniques resulting in the precise penetration of current and emerging targets.

Objective 2.1

Develop a horizontally integrated, adaptive set of collection capabilities to achieve persistent surveillance.

DIA's responsibility to develop an overarching DoD collection management architecture, plan, and process — that already includes imagery intelligence, signals intelligence, geospatial intelligence, and measurement and signature intelligence (MASINT) — will be further strengthened with the integration of HUMINT and newly-developed collection strategies. The Agency will enhance its capabilities through increasing the strength and integration of its HUMINT and technical collection assets. The GWOT and the increased focus on irregular warfare have underscored the need for HUMINT collection in order to achieve true persistent surveillance. The ability to gain and exploit battlefield awareness is critical to achieving warning and tactical advantage against the nation's adversaries. DIA will:

- Improve foreign language proficiencies and expertise to better assess, explain, and exploit the cultural landscape in which collectors operate.
- Integrate HUMINT and MASINT with other capabilities across the Defense Intelligence Enterprise to achieve persistent surveillance of the Nation's adversaries.

Objective 2.2

Leverage a federated community of defense scientific and technology intelligence (S&TI) capabilities.

DIA will serve as a hub across the Defense Intelligence Enterprise for the development of S&TI capabilities. The Agency will research, develop, and deploy new MASINT capabilities and other innovative collection technologies aimed at improving the ability to provide early warning. DIA will:

- Realize close-access technical collection operations by developing a multi-layer/multi-sensor architecture using comprehensive MASINT data archives and phenomenology, signature, and environmental effects libraries.
- Expand the ability of the Defense Intelligence Enterprise to exploit the full range of scientific research in pursuit of national security objectives.
- Exploit technological advances and develop countermeasures to mitigate the human and materiel damage caused to US and allied forces by improvised explosive devices (IEDs) and other irregular warfare weapons.

Objective 2.3

Increase the awareness, availability, and use of open source information, to ensure all-source collection and analysis.

DIA will increase open source information capabilities to advance the Defense Intelligence Enterprise's exploitation of material available from the Internet, databases, press, radio, television, video, geospatial data, photos, and commercial imagery. The Agency will improve integration of these resources enabling it to better utilize relevant open source collection and analysis to gain a more complete picture for leaders and operators. DIA will:

- Develop a coherent management construct to consolidate and clarify open source strategies, policies, training, and functional IT requirements across the Defense Intelligence Enterprise.
- Ensure properly administered unclassified holdings are available to customers.
- Integrate defense and national open source capabilities to eliminate duplication of effort and explore opportunities for collaboration among components of the Intelligence Community (IC).

Objective 2.4

Improve counterintelligence (CI) collection management and analysis to better identify, neutralize, and exploit foreign threats.

DIA personnel must be aware of the methods and intentions of foreign intelligence, subversive, or terrorist elements. To ensure the protection of the Defense Intelligence Enterprise and its forces, DIA will seek to increase capabilities in the areas of CI operations and investigations, analysis and assessments, technology development and protection, and force protection. DIA will:

- Integrate the DoD CI management role for production, collection, and operations requirements with the intelligence collection community to bring all-source information to bear against foreign intelligence threats.
- Support collectors with flexible services, customized on short notice to take advantage of unplanned opportunities.
- Integrate CI planning with available ICP processes to expand its role in joint military operations.

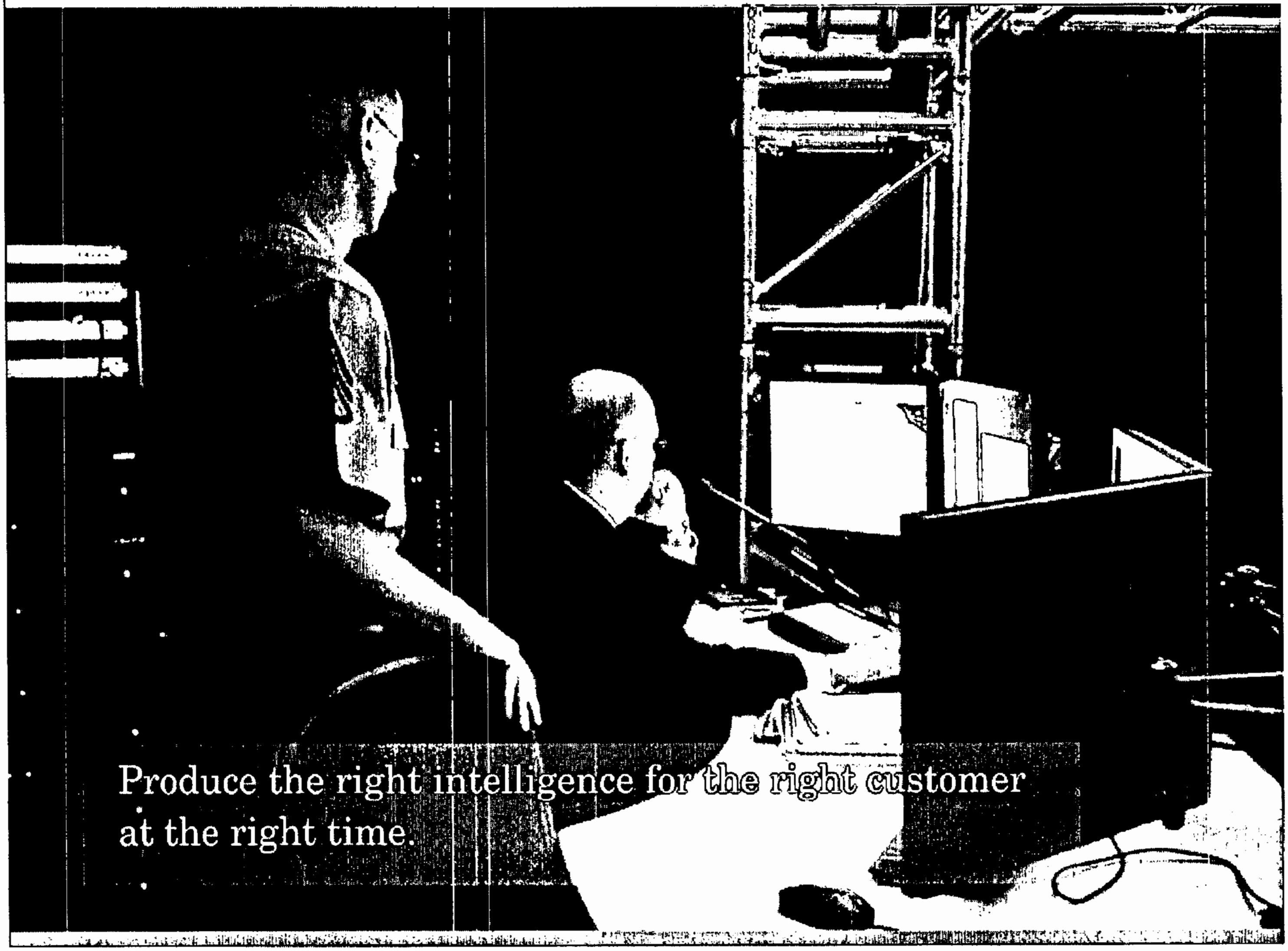
Objective 2.5

Collaborate with customers, industry, and Agency partners to discover and capture emerging intelligence concepts, processes, and technologies.

DIA is committed to leveraging relationships with partners in government and industry to rapidly discover and exploit advances in learning and technology. The Agency will seek out best practices and emerging technologies to ensure operational capabilities are more advanced and versatile than the threats confronting the nation. To this end, DIA will speed assimilation and deployment of these technologies through proactive collaboration with a range of partners to ensure continuous improvement. DIA will:

- Position DIA resources as a link between customers, industry partners, national and defense intelligence components, and non-traditional organizations to maintain awareness of emerging and future technologies, capabilities, and practices.
- Through innovative partner relationships, modernize and sustain HUMINT information operations and improve unconventional MASINT operations.
- Exploit emerging capabilities and technologies through the establishment of a formal program to speed discovery, development, and deployment.

Goal 3



Produce the right intelligence for the right customer at the right time.

DIA continually seeks better ways to support its customers by providing tailored analytic output that is precise, timely, and actionable. Proximity to the customer and the integration of the Defense Intelligence Analysis Program (DIAP) will enhance the allocation of analytic resources across the Defense Intelligence Enterprise. Risk management of analytic resources, increased analytic rigor and training, and the promotion of critical thinking and long-term strategic analysis are vital to this effort. DIA will ensure DIAP, ICPs, and defense intelligence priorities are aligned and integrated to best support military and national intelligence integration, collection strategies, and adaptive planning.

Objective 3.1

Link risk-managed all-source analysis to customer requirements.

DIA will link risk-managed all-source analysis to customer needs by providing customers tailored access to all relevant and archival data on demand via technologies that can organize, analyze, and display correlated information. DIA will:

- Develop and sustain the criteria and methodology for establishing levels of analytic effort based on guidance from key intelligence customers.
- Assign clearly defined all-source analytical responsibilities to defense intelligence analytic organizations within General Defense Intelligence Program (GDIP) and DIA Military Intelligence Program, based on capabilities, workforce characteristics, and mission requirements.
- Develop and track measures of effectiveness for analytic performance and customer satisfaction.

Objective 3.2

Strengthen analytic tradecraft training and professional development at all levels to improve the quality and rigor of defense intelligence.

DIA will improve analytic practices across the Defense Intelligence Enterprise, ensuring greater rigor through the use of creative analytic techniques and research methodologies. The Agency will acquire, maintain, and improve the analytic skills necessary to achieve aggressive all-source analysis against the full spectrum of enduring and emerging challenges. DIA will:

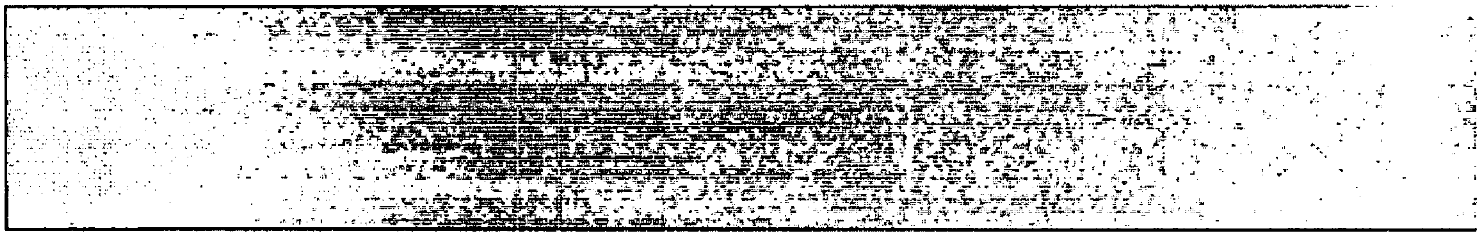
- Design and maintain a cradle-to-grave analytic development and leadership program that fosters collaboration throughout the IC to ensure the capabilities to meet defense intelligence requirements are in place.
- Develop formal analytic requirements and programs that will lead to a better understanding and application of methodologies, structured techniques, and creative and critical thinking skills.

Objective 3.3

Foster critical thinking and promote long-term strategic analysis and warning through the use of advanced research methods and techniques.

DIA will develop expertise in the use of advanced analytic methods and techniques that build on past knowledge. This includes the integration of critical thinking models and diverse perspectives in the development of analytic output. The Agency will provide customers with analytic judgments that clearly identify opportunities, vulnerabilities, and uncertainties. DIA will:

- Create an environment for analysts to use critical thinking and basic structured



analysis techniques to mitigate bias, understand mindsets, and incorporate competing views to help guide the national dialogue regarding threats to the United States and its interests.

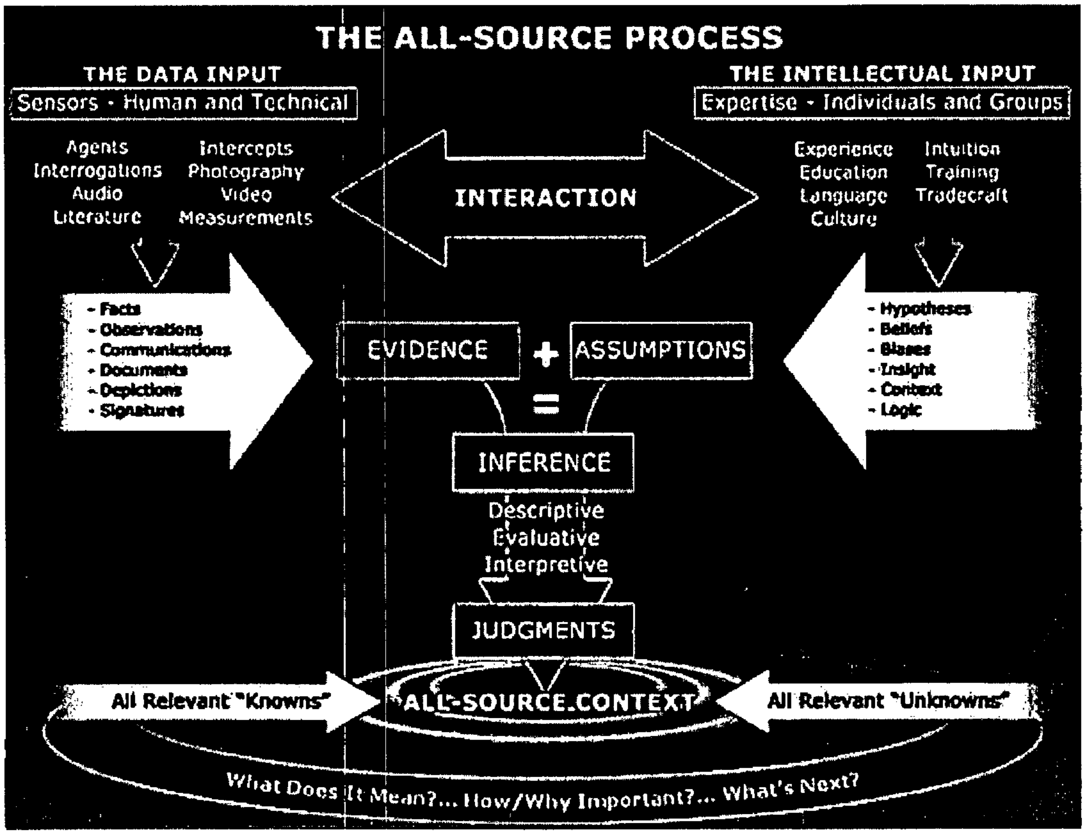
- Institutionalize forward-looking strategic analytic methods and techniques to increase long-term strategic analytic production to ensure warning of future threats.

Objective 3.4

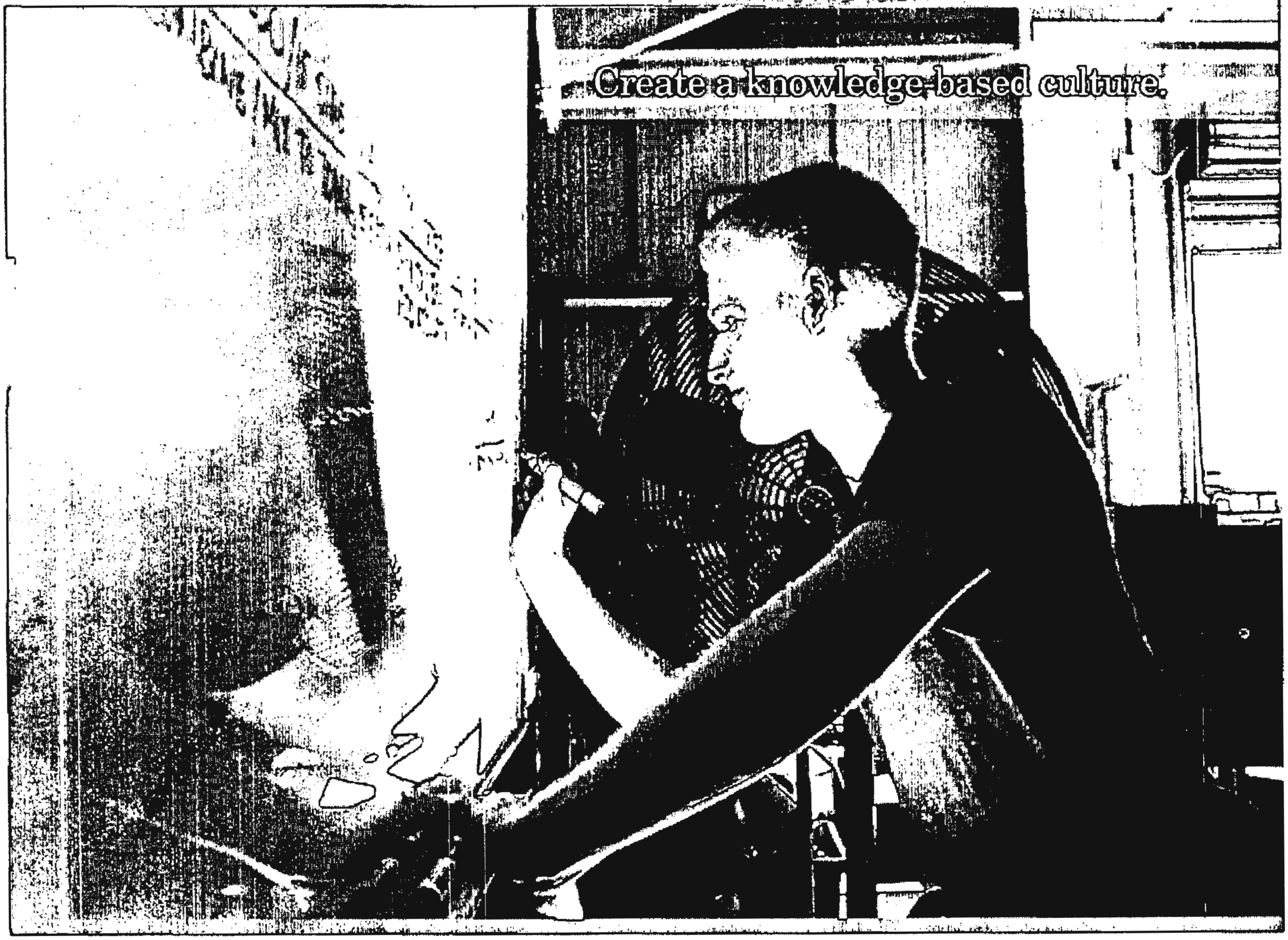
Promote all-source analysis through the integration of collectors and analysts with access to information at the earliest point of consumability.

DIA believes collaboration between collectors and analysts is critical to tearing down walls that limit the ability to collect, process, and share information quickly. DIA will accomplish enhanced collaboration through co-location and training of the collector and analyst workforce, implementation of interoperable systems, and creation of an information-sharing culture. DIA will:

- Build teams, design processes, provide collaboration tools, and develop innovative approaches to improve information sharing and timely access to data.
- Support on-demand, simultaneous access to shared data across security domains for the IC workforce through IT implementation of Horizontal Integration.
- Establish an intelligence solution repository to maintain critical data in an easily accessible structured format.



Goal 4



Create a knowledge-based culture.

DIA is committed to becoming a highly effective knowledge-based organization by establishing a culture where information is proactively shared among Agency personnel and IC partners. The Agency will implement new strategies to develop and exploit knowledge wherever it exists. This includes initiatives to strengthen cooperation with foreign partners, broaden information access through interoperable technology, and build innovative knowledge creation practices and sharing techniques.

Objective 4.1

Cooperate with foreign partners to increase global situational awareness and close critical intelligence gaps.

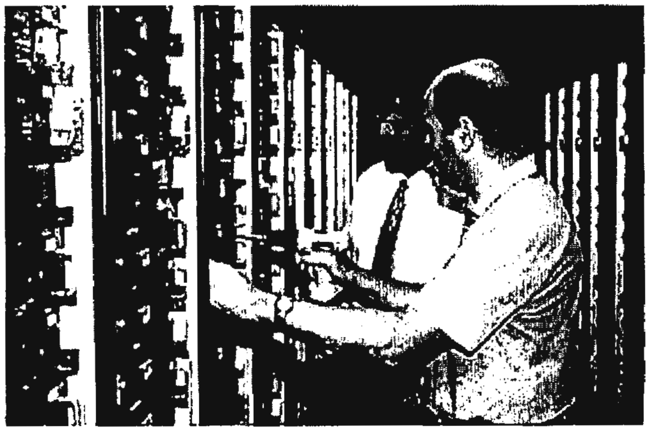
DIA will seek out and build relationships with knowledgeable and capable foreign partners to enhance access to information and perspectives otherwise unavailable to our intelligence analysts. The Agency will work with its partners to focus on the intent of foreign leaders and adversaries to provide the intelligence required to prevent—rather than respond to—potential crises around the world. DIA will:

- Coordinate with other members of the IC to leverage existing and emerging intelligence relationships to greater advantage.
- Provide timely foreign exchange and disclosure policy guidance to support improved information access for foreign partners and coalition members.
- Serve as the critical link and DoD focal point for the foreign defense attaché community, foreign embassy staffs, and the defense and national intelligence communities to leverage resources and limit intelligence shortfalls.

Objective 4.2

Implement interoperable state-of-the-practice Information Management (IM) technologies consistent with the Information Sharing Environment.

DIA believes a flexible, centrally-managed and locally-executed Defense Intelligence Enterprise will provide customers with enhanced interoperability and more cost-effective IM services. Future solutions and services will adhere to enterprise standards and IM best practices. This will support the



level of access, timeliness, quality, agility, and precision of information required for current and future missions. It will also support seamless horizontal and vertical integration of DoDIIS applications and data by leveraging multiple IM activities. DIA will:

- Promote, field, and maintain a horizontally integrated knowledge environment enabled by physical and virtual collaboration in conjunction with the intelligence and operator communities.
- Use data tagging best practices and technologies to enable more efficient search and retrieval of information, enhance access to all data sources, and refine data standards and data ownership.
- Identify and implement technologies, standards, and IM data policies that enable all-source fusion across multiple security domains in a user-friendly format.
- Incorporate Defense Intelligence Enterprise-wide systems to reduce IT costs using a widely coordinated "Service Oriented Architecture" to promote reuse and provide enterprise standards.

Objective 4.3

Implement innovative strategies to discover, share, apply, and build upon knowledge as a force multiplier across the Defense Intelligence Enterprise.

DIA recognizes that new strategies for building and communicating knowledge can have an exponential impact on the Defense Intelligence Enterprise's mission. DIA will identify innovative knowledge strategies through interaction with leaders from business, academia, partner agencies, and other disciplines. The selected concepts will be implemented by introducing changes in culture, as well as processes and technology, to create multi-dimensional and mutually supporting approaches to improving knowledge development. DIA will:

- Utilize innovative capabilities, techniques, and socialization methodologies to achieve improvement in knowledge-building and knowledge-sharing.
- Identify and apply best practices from government, industry, and academic sources to strengthen DIA's knowledge capabilities.
- Implement and manage concepts that encourage a unified, knowledge-based culture across the Defense Intelligence Enterprise.
- Increase the frequency of outcome-based collaboration among employees to facilitate knowledge-sharing.
- Implement solutions combining culture, process, and technological dimensions that will promote the ability to learn from challenges.

Goal 5

Attract, develop and retain a results-oriented workforce.

The people that constitute the DIA workforce are our most valuable resource. In light of this, DIA depends on the combined skills of its workforce to achieve the defense intelligence mission with excellence. Every member of the DIA workforce must have an equal opportunity to excel in their career through learning and performance improvement, mentoring, and access to engaging work opportunities. A results-focused workforce, possessing diverse global perspectives and a broad range of skills and capabilities is required to respond to the threats of the 21st century. DIA will ensure the requirement for diverse global perspectives and skills are met by executing thoughtful recruitment, development, and retention activities.

Objective 5.1

Recruit a highly qualified, diverse workforce with an array of backgrounds and life experiences that enhance the range and depth of Agency capabilities.

DIA's workforce must perform in an increasingly dynamic, cross-functional, and team-driven environment. The Agency will hire highly qualified, intellectually diverse candidates with a range of backgrounds and skills, including knowledge of hard target foreign languages and cultures. In addition, DIA will strive to ensure successful placement of new hires by accurately matching employee skills, competencies, and career desires to the appropriate position. DIA will:

- Ensure that all human capital support conditions and resources are in place to identify, attract, hire, staff, and retain talented professionals.
- Increase directorate engagement in staffing by building practices and communications which enable participation at all stages of the process.
- Partner with the military services to ensure that assignments to DIA are highly desired and professionally rewarding for active and reserve military personnel.
- Provide challenging developmental and experiential work opportunities to sustain passion and curiosity throughout the workforce.

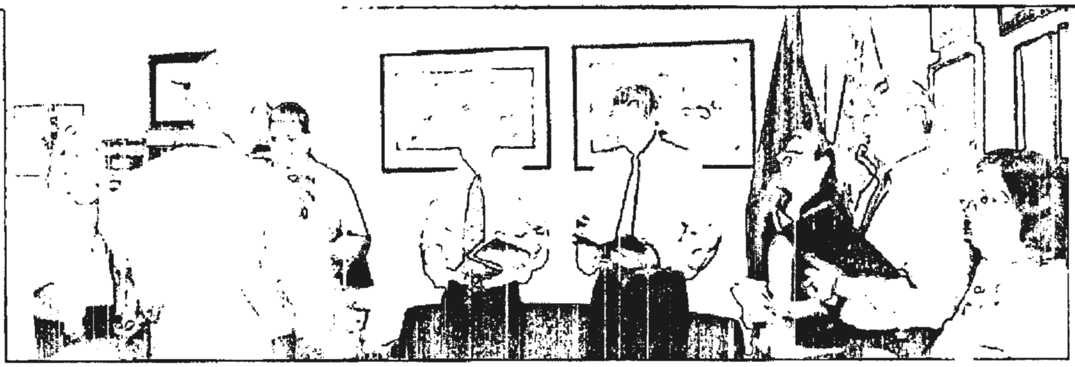
Objective 5.2

Shape the DIA workforce to ensure the critical workforce skills and competencies are in place to fulfill future mission requirements.

DIA will foster an environment where all members of the workforce can maximize their contribution to the mission. The civilian and military workforce must have access to developmental and work-related opportunities that will build attributes, skills, and capabilities in line with future expectations. This includes subject matter expertise, core management capabilities, and a well-rounded set of work experiences which position employees for promotion within the civilian or military ranks. DIA will:

- Ensure the entire DIA workforce — regardless of grade, job series, or job location — is provided the required competency-based skills, tools, learning opportunities, and resources to maximize their ability to meet the changing environment of the 21st century.
- Ensure the workforce is proficient in general, specialist, and managerial competencies to fulfill the Agency mission, and is provided a range of professional development and career opportunities to achieve this.
- Ensure all personnel understand the core mission and functions of DIA and possess the requisite technical proficiencies and communication skills necessary to fully contribute to the Agency's mission.
- Expand interagency rotational programs to develop "jointness" across the IC and

[redacted]



build deeper understanding of methods, requirements and capabilities.

- Create the conditions, relationships, practices, tools, and support to develop an effective foreign language capability across the enterprise.

Objective 5.3

Implement a comprehensive set of innovative learning strategies and performance improvement services to facilitate DIA's global workforce.

DIA will refine and expand the range of learning opportunities available to all Agency employees in both technical and non-technical disciplines. This will include development of non-traditional learning strategies in recognition of the fact that the DIA workforce is increasingly global. The Agency will design learning opportunities to support increased agility and integration in the workforce through the cross-application of skills and deployment support. DIA will:

- Increase awareness of learning, performance improvement, and deployment opportunities to enhance career and skill development.
- Partner with the National Intelligence University to expand, develop, and integrate the capabilities of all-source analysts and collectors.
- Maintain a fully incorporated, highly skilled Reserve Component to support Agency and IC mission and deployment requirements.
- Build a comprehensive global learning and performance service platform that corresponds with the needs of a virtual and deployed workforce.

Objective 5.4

Develop the next generation of leaders through creative, innovative programs that promote excellence in management practices.

DIA seeks to build a management development process that equips employees with the skills and competencies necessary to lead an integrated Defense Intelligence Enterprise. Based on industry best practices, the Agency's leadership certificate program will expose participants to a wide array of organizational and people management subjects. DIA will:

- Continue implementation of a leadership development program to build capabilities at all managerial levels, broaden the applicant pool, and increase the skill depth of those seeking promotion into leadership positions.
- Provide learning and performance improvement opportunities to supervisory personnel in order to maximize employee performance and retain high performers.

Goal 6

Provide superior resource and organization management.

DIA requires effective managerial processes and accurate measures to assess progress and shortfalls within the Agency, particularly against key strategic priorities. To ensure the proper management framework and supporting business systems are in place, the Agency will continue to develop practices and procedures designed to improve oversight and accountability at all levels.

Objective 6.1

Build, defend, and account for DIA's financial and manpower resources across a broad range of intelligence programs and capabilities.

DIA will use effective stewardship of public resources to achieve programmatic efficiency and eliminate redundancy. The Agency recognizes that effective stewardship and managerial processes require transparency and accuracy in financial data and manpower authorizations for monitoring and assessing resource decisions. Policies, procedures, and systems must ensure the reliability of management information, support regulatory compliance, demonstrate strategic alignment, and measure program effectiveness. DIA will:

- Demonstrate accountability to overseers by issuing and communicating an auditable financial statement and receiving an unqualified (clean) opinion issued by independent auditors.
- Implement an internal control program to improve accountability and compliance to support budget-performance integration efforts.
- Integrate GDIP IT budgets, capabilities, assets, and staff in a global enterprise and establish a set of DoDIIS centralized processes and methodology.
- Integrate enterprise system and reporting technologies to modernize Agency purchasing, acquisition, finance and logistics business processes.

Objective 6.2

Implement budget-performance integration by linking DIA resource allocations and performance measures to strategic objectives.

DIA's mission requires the careful allocation of investments and resources at all levels. The Agency recognizes that government resources are finite and must make hard decisions when balancing priorities and risks. Consequently, DIA will use all relevant data to evaluate and invest in those programs which are most likely to yield products and results tied to strategic objectives. DIA will:

- Assess the current program development process to evaluate how program submissions are aligned against strategic objectives and/or may be improved to further meet the mission needs of the Agency.
- Utilize the Enterprise Architecture model to align IT systems and technologies against strategic, operational, and tactical objectives, key process areas, and identified business requirements.
- Strengthen the linkages between strategic objectives, business capabilities, supporting services, and performance measures to understand business needs and program performance measures when defending or requesting resources.
- Evaluate directorate-level performance outcomes against the accomplishment of overall Agency strategic objectives and metrics.
- Eliminate programs that add little value to accomplishing strategic objectives and re-direct savings to existing and emerging strategic priorities.
- Implement a portfolio management framework to manage risks, returns, and performance of IT investments throughout their life cycle.
- Utilize a centralized investment management tool to facilitate comprehensive programming, budgeting, and reporting information on all IT investments.

Objective 6.3

Enhance acquisition planning and contracting using a portfolio approach to support program management and contract related workforce oversight.

DIA relies on the application of timely, effective, and compliant acquisition and contracting practices to ensure the flow of goods and services necessary to complete the defense intelligence mission. Effective acquisition program management practices and oversight will ensure DIA secures the latest technologies and capabilities to support strategic initiatives. The Agency will meet customer needs by ensuring that contracting staff are highly capable, use best practices, and support a culture of excellence. DIA will:

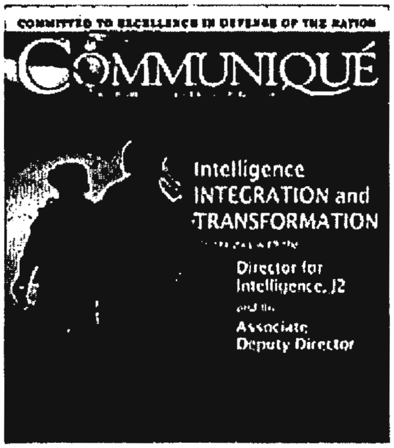
- Provide timely and sound acquisition guidance to DIA leadership, managers, and workforce to ensure effective use of contracting resources.
- Integrate initiatives to increase efficiency and effectiveness through improvement of acquisition tradecraft, management, controls and processes.
- Improve acquisition and performance management reporting to enable rapid transition of leading edge technologies from research and development phases to all-source operations.

Objective 6.4

Strengthen outreach and communications to build strategic relationships and raise awareness of the Agency's mission and contributions to national security.

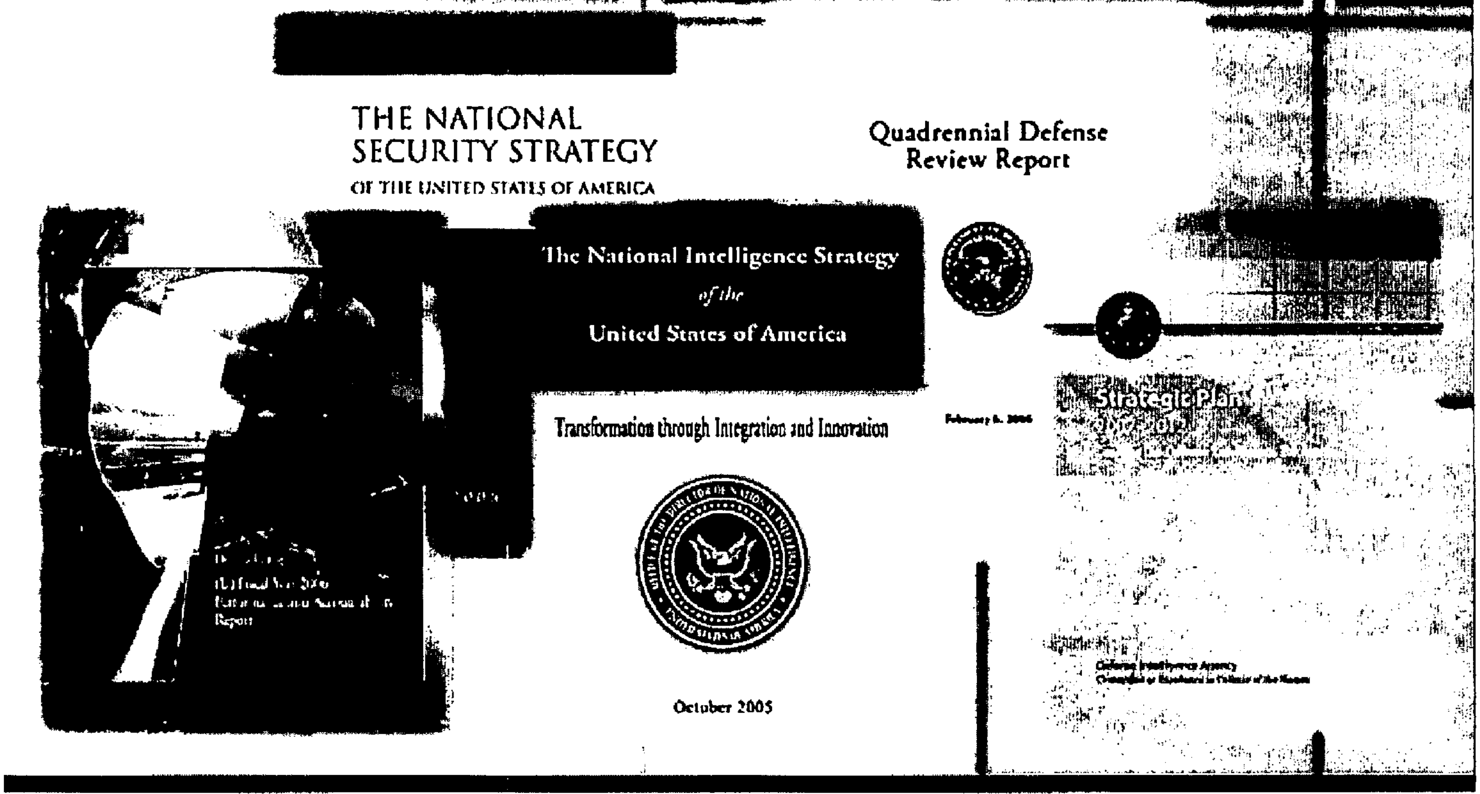
DIA places a high value on outreach and communication to provide various stakeholder audiences with insight into the wide range of Agency activities and accomplishments. DIA seeks to continuously improve the quality, content, presentation, and delivery of its communication products to ensure customers, partners, the workforce, and other stakeholders remain highly informed. In addition, the Agency will implement a proactive engagement strategy and communications plan to provide overseers with consistent insight into DIA's mission and functions. DIA will:

- Convey to external and internal Agency audiences a consistent, compelling, and tailored message allowing insight into the activities and mission of DIA.
- Inform Agency customers and stakeholders of modifications to Agency processes, including the rationale and the necessity for the proposed changes.
- Refine the corporate communications initiatives and products of DIA through feedback to ensure they meet the information needs of customers, stakeholders, and the workforce.



Goal 7

Sustain a culture of continuous improvement.


THE NATIONAL SECURITY STRATEGY
OF THE UNITED STATES OF AMERICA
Quadrennial Defense Review Report
February 6, 2006
The National Intelligence Strategy of the United States of America
Transformation through Integration and Innovation
October 2005
Strategic Plan

DIA believes that a culture of continuous improvement, urgency, and efficiency is necessary to accomplish the defense intelligence mission with excellence. The Agency will establish and institutionalize a number of performance assessment tools and processes to better inform short- and long-range resource decisions. In addition, DIA will continue to assess the threat and operating environments, as well as stakeholder priorities and requirements, to identify adjustments to plans and policies.

Objective 7.1

Centrally manage and sustain the deployment of Lean Six Sigma as a tool for continuous improvement.

The Agency supports the DoD Continuous Process Improvement Program through the implementation of Lean Six Sigma and will use this methodology to eliminate redundancy and variation in core processes. The initiative will increase overall productivity and improve support to combatant commanders and senior decision makers. Also, DIA will use established key performance indicators (KPI) to enable senior leaders to make data-driven decisions aligned with Agency strategic goals and objectives. These measures will improve the ability of DIA leadership to manage performance, execute critical initiatives and resource decisions, and enforce overall process owner accountability. DIA will:

- Manage the deployment of Lean Six Sigma as a change agent for performance excellence through training, performance evaluation, metric validation and project selection.
- Implement, refine, and manage KPIs to accurately measure DIA core processes using the DIA Performance Dashboard.
- Coordinate, manage, and track critical KPIs across directorates as a platform for performance improvement, project selection, and input to the DIA Performance Plan.

Objective 7.2

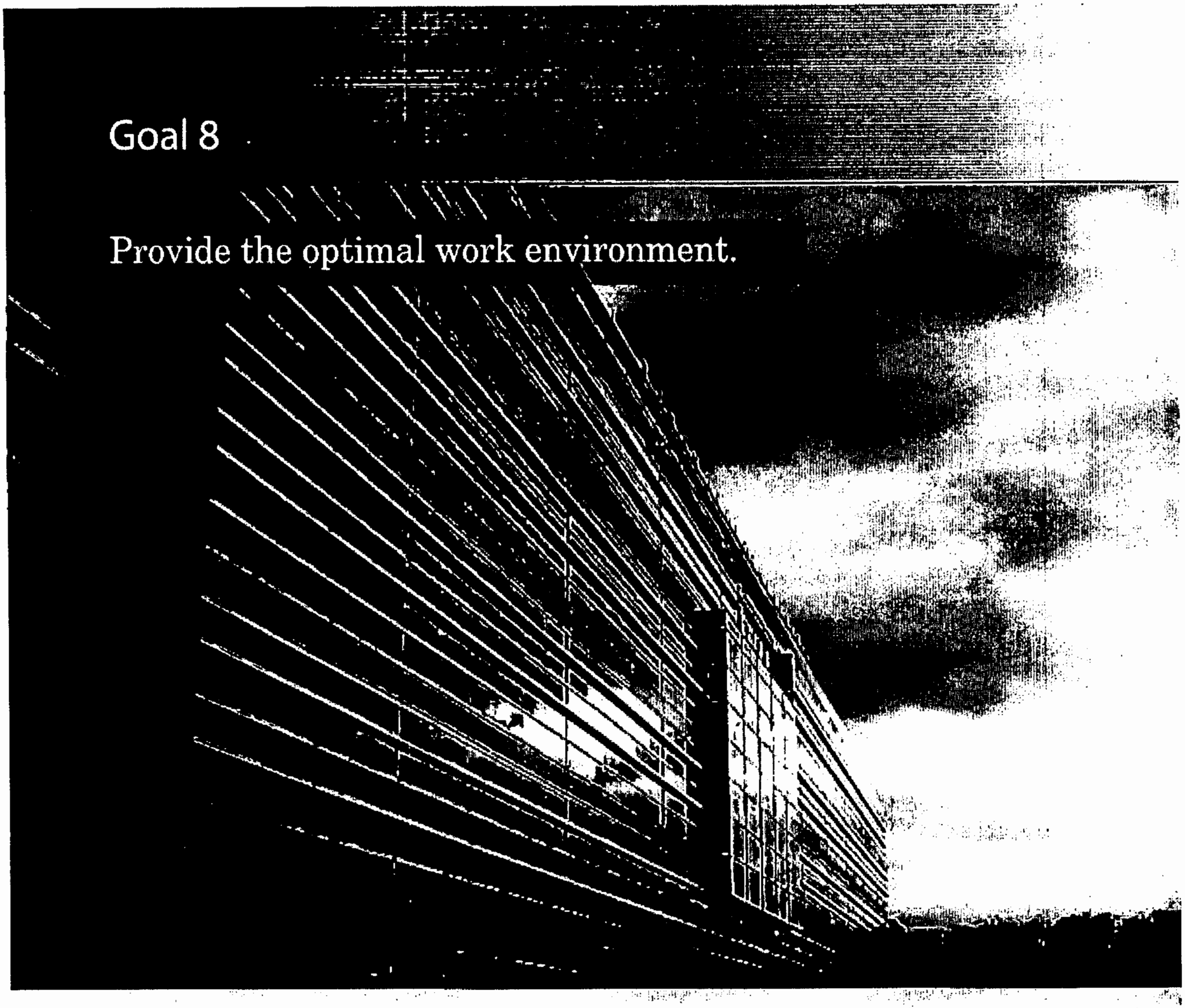
Refine DIA's strategic planning cycle to adapt to the dynamic needs of customers.

DIA will refine its Agency-wide planning construct to ensure resources are allocated and utilized effectively to address strategic priorities. The Agency will evaluate the overall operating environment, including the recommendations and mandates of stakeholders. It will assess the efficacy of on-going programs and identify emerging and future threats, required changes in operations, and potential resource or programmatic needs. DIA will manage its strategic plan as a "living document"— developing updates as warranted and demonstrating linkages to various integrated budget-performance metrics. DIA will:

- Achieve a codified, coordinated strategic planning and financial management approach across DIA at the enterprise and directorate levels.
- Institutionalize DIA's strategic plan throughout the Agency, to be reflected in directorate plans, performance assessments, and communications.

Goal 8

Provide the optimal work environment.



DIA recognizes the importance of providing a fair, modern, and secure work environment. The Agency will work to ensure all employees have an opportunity to excel in support of the mission. This is achieved through a culture that supports and leverages equality of opportunity, modernizes its facilities and infrastructure, and values constant awareness of security and CI threats.

Objective 8.1

Eliminate barriers to employment and ensure opportunities for training, upward mobility, and career growth are provided to all employees.

DIA is committed to the principle that every member of the workforce be provided an equal opportunity to excel. Equal opportunity and a workplace free of discrimination and harassment is essential to attracting, developing, and retaining a high-caliber workforce. To that end DIA will be free from prohibited discrimination through encouraging managers and supervisors to remove physical and social barriers, asking employees to use a collaborative approach to national security challenges, and valuing diverse viewpoints. DIA will:

- Design and implement a model equal employment opportunity program that meets or exceeds federal standards and achieves Federal Model Employer status.
- Provide conflict management options to prevent, intervene, and resolve disputes; improve productivity, and reduce investigation and litigation costs.

- Develop appreciation for workforce differences, support equality of opportunity for all, and recognize employee contribution to mission success.

Objective 8.2

Improve the physical infrastructure to support workforce performance, accommodation, safety, and security.

DIA employees deserve a safe and efficient physical work environment, wherever possible. The Agency's physical infrastructure must be effectively maintained and upgraded to take advantage of new technologies and processes in order to fully meet customer requirements now and in the future. DIA will:

- Establish a DIA facilities functional management capability and administer the increasing size of the DIA workforce and additional locations using improved processes and interagency cooperation.
- Develop standardized processes to conduct and manage the inspection, integration, and oversight of DIA facilities and related field sites.

Objective 8.3

Continuously improve integrated security policies, processes and practices to facilitate a secure work environment and enable aggressive CI actions.

DIA must protect the security of the work environment as well as forms of intelligence and information. This is accomplished by carefully vetting employees to ensure they meet the criteria for access and are fully cognizant of the rules governing the Agency's information and facilities. DIA must safeguard data, provide authorized access, and serve as the DoD authority on declassification and Freedom of Information Act requests. DIA will:

- Improve timeliness of DoD security clearance adjudication to ensure a fully vetted workforce able to access and process intelligence information in support of mission requirements.
- Increase the frequency of sensitive compartmented information facility inspections to reduce accreditation processing times.
- Improve Agency workforce knowledge of security policies including Special Access Programs, NATO Access Program, sensitive compartmented information and collateral policy through training and communications.
- Improve the management and operation of DIA's Information Assurance program to ensure the proper protection of the confidentiality, integrity, and availability of enterprise information assets.

Objective 8.4

Achieve a fully integrated and executable mission assurance program.

DIA will strive to achieve a fully integrated mission assurance program to mitigate risk through proactive planning and preparation. Successful execution will require coordination with the IC, DoD, host site and military base authorities as well as local governments. DIA will:

- Refine continuity crisis policy and leadership succession plan and implement a multi-year strategic management plan for resources in support of mission assurance.
- Improve the crisis management framework to execute a single, streamlined crisis action plan and provide hazard reduction, risk assessment, and impact mitigation.
- Provide training to ensure full organizational readiness and program evaluation with implementation of corrective actions.

Summary

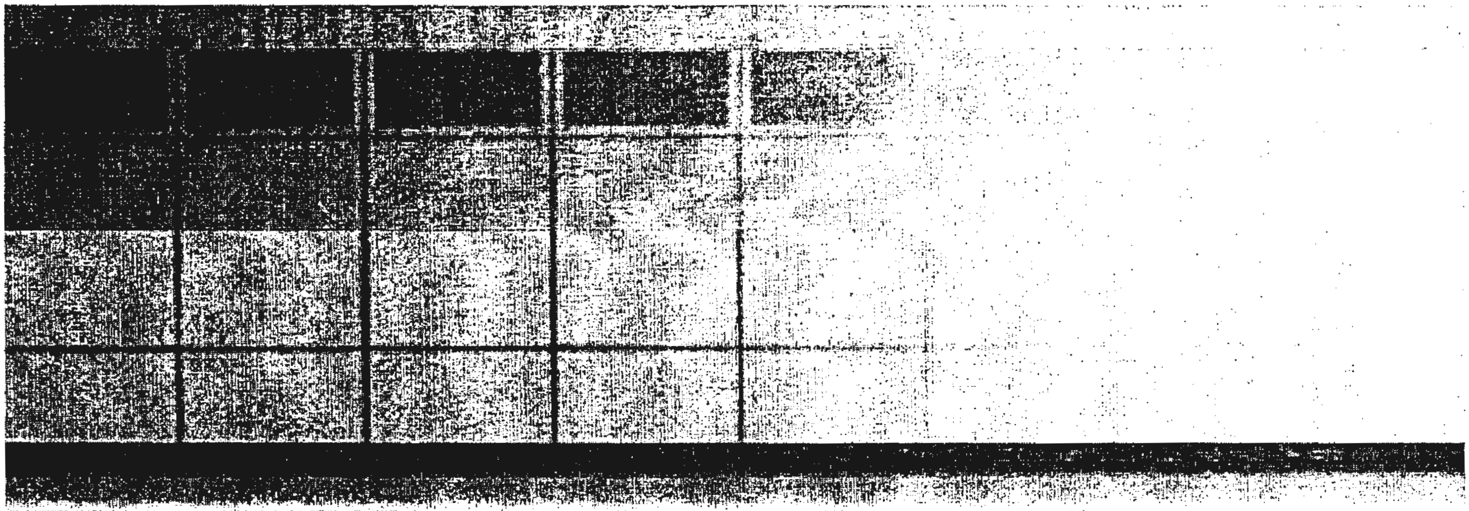
The national security threats we face, among them insurgency, terrorism and weapons of mass destruction, are complex and multi-dimensional. They are steeped in perceptions of history and ideology, and intensified by the competition for scarce political and economic resources. Their global nature requires us to think and act with a diversity of mindset but with unity of purpose and vigilance towards the future.

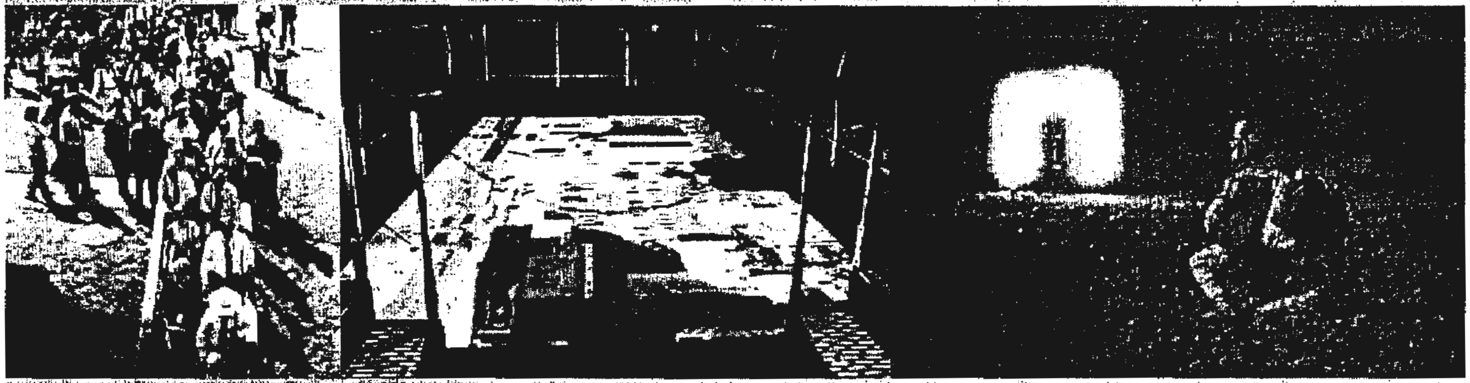
This strategic plan lays the groundwork for achieving an integrated, synchronized portfolio of highly capable individual components. All areas of defense intelligence, including collection, analysis, counterintelligence, technology, human capital, and management must be strong for the collective whole to achieve excellence. There can be no weak link in the chain — lest our adversaries find it.

In the years ahead, we can expect an environment marked by the unexpected and the unpredictable. We must be ready. We must prepare for the rapid changes ahead by working in unison, shaping agile intelligence professionals, and building processes, and technologies that can anticipate and respond at will. Our mission requires it, the protection of the United States and its allies demand it.

Defense Intelligence Agency Desired Endstate

Integration of highly skilled intelligence professionals with leading edge technology to discover information and create knowledge that provides warning, identifies opportunities, and delivers overwhelming advantage to our warfighters, defense planners, and national security policymakers.





DEFENSE INTELLIGENCE AGENCY
UNITED STATES OF AMERICA

http://www.dia.mil

PCN 2622

21. Vision 2015: A Globally Networked and Integrated Intelligence Enterprise

> "The purpose of this Vision document is to chart a new path forward for a globally networked and integrated Intelligence Enterprise for the 21st Century based on the principles of integration, collaboration, and innovation."

VISION 2015

A Globally Networked and Integrated Intelligence Enterprise

Mission

Create Decision Advantage

Vision

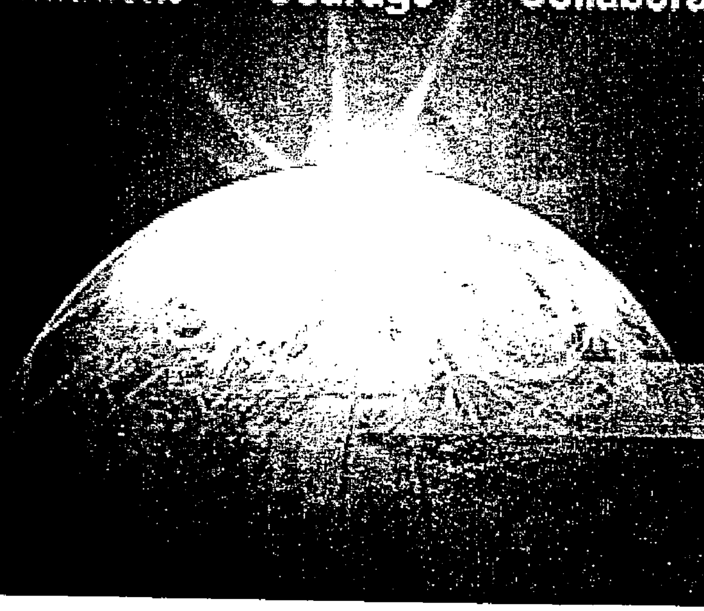
A Globally Networked and
Integrated Intelligence Enterprise

Strategy

Integrate foreign, military, and domestic intelligence capabilities through policy, personnel and technology actions to provide decision advantage to policy makers, warfighters, homeland security officials and law enforcement personnel

Values

Commitment • Courage • Collaboration



DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Fellow Intelligence Professionals:

We are engaged in a dynamic global environment, in which the pace, scale, and complexity of change are unprecedented. It is a networked world where what happens in Peshawar affects Peoria — and vice versa. Risks are often unforeseen and threats are hidden and agile, making the job of intelligence professionals more critical and more challenging. Our national security depends on anticipating risks and out-maneuvering our adversaries, not just out-muscling them. Therefore, intelligence is more critical than ever. We must address these risks and threats by integrating all elements of national power — defense, homeland security, diplomacy, development, and intelligence. However, the Intelligence Community is still largely structured, staffed and operated around a design optimized for a different era. Adapting the Community to this new environment is our fundamental challenge. The purpose of this Vision document is to chart a new path forward for a globally networked and integrated Intelligence Enterprise for the 21st century based on the principles of integration, collaboration, and innovation.

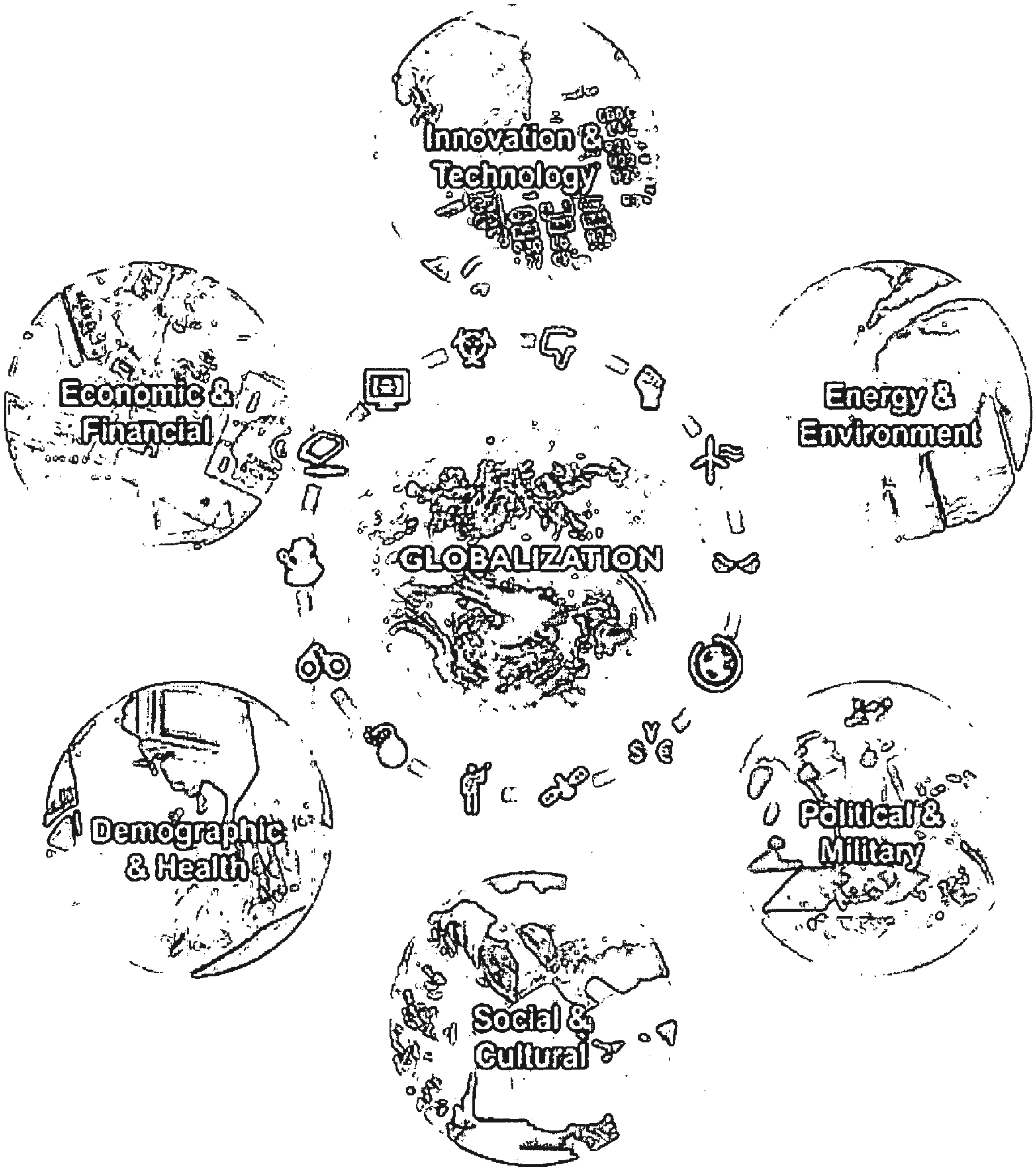
The mission of the Intelligence Community is to create decision advantage for our customers — policymakers, military commanders, law enforcement and homeland security officials. This means we collect and analyze intelligence to improve our customers' ability to make a decision while denying our adversaries the same advantage. To transform the Community and create decition advantage, we will need to accomplish the following:

- *Develop integrated capabilities to address emerging challenges in cyber space and support new missions such as energy security.*
- *Create a customer-driven intelligence model.*
- *Improve our ability to anticipate and prevent strategic surprise through better global awareness and strategic foresight.*
- *Integrate the Community through mission-focused operations that transcend agency and funcional silos. This also requires us to network our collection assets to allow them to work, autonomously and cooperatively in near-real time, to penetrate the most difficult targets.*
- *Field a net-centric information enterprise that enables end-users to discover, access, and exploit intelligence information in a secure, tailored manner.*
- *Remove the barriers to cross-agency collaboration by integrating the strategic enablers of the Intelligence Enterprise — human capital, education and training, business systems, facilities, science and technology, and acquisition and procurement.*

A vision without a map is just a wish. To make this Vision real, I challenge the Community's senior leaders, who participated in creating it, to develop a well-defined roadmap that details the steps we will take immediately, and throughout the next several years, to translate this Vision into reality. While our Vision extends to 2015, we must make real progress sooner rather than later. Our commitment to this Vision will be manifested in our budget priorities and implementation plans.

In 1996, the Chairman of the Joint Chiefs of Staff, General John M. Shalikashvili, published Joint Vision 2010, which detailed the conceptual template for our military forces. The document was brief, conceptual, and controversial, but it proved an effective guide for developing the superb military capabilities the United States now possesses. I invite all intelligence professionals to join in this fundamental transformation of our Community into an Intelligence Enterprise poised to continue to succeed for the foreseeable future.

J. M. McConnell


Innovation & Technology
Economic & Financial
Energy & Environment
GLOBALIZATION
Demographic & Health
Political & Military
Social & Cultural

1 THE SHIFTING STRATEGIC LANDSCAPE

Era of Uncertainty
Implications for the Intelligence Community

2 CREATING DECISION ADVANTAGE

3 MAKING IT REAL - IMPLEMENTING THE VISION

1 THE SHIFTING STRATEGIC LANDSCAPE

"When the rate of change outside your organization exceeds that within your organization, the end is near."

- Jack Welch, former CEO, General Electric

We live in a dynamic world in which the pace, scope, and complexity of change are increasing. The continued march of globalization, the growing number of independent actors, and advancing technology have increased global connectivity, interdependence and complexity, creating greater uncertainties, systemic risk and a less predictable future. These changes have led to reduced warning times and compressed decision cycles. Although this interconnected world offers many opportunities for technological innovation and economic growth, it also presents unique challenges and threats. In this environment, the key to achieving lasting strategic advantage is the ability to rapidly and accurately **anticipate and adapt to complex challenges.**

The integration of international politics and economics over the last century outpaced the integration of U.S. institutions. Our statecraft adapted over the decades with new policies and institutions. The future portends discontinuities with new threats from non-traditional actors, new modes of attack, and more lethal impact. Intelligence must be more integrated and agile to assist in preventing and responding to these challenges.

Era of Uncertainty

Many drivers and trends are shaping the future global environment in which the Intelligence Community must operate — demographic and social change, increased economic integration and competition, rapid technological innovation and diffusion, environmental pressures and growing energy demand, broad geopolitical changes and new forms of governance. Each driver and trend independently produces unique changes and challenges; those points where factors intersect often reinforce and amplify the effects of change and create a series of complex and often unpredictable threats and risks that **transcend geographic borders and organizational boundaries.**

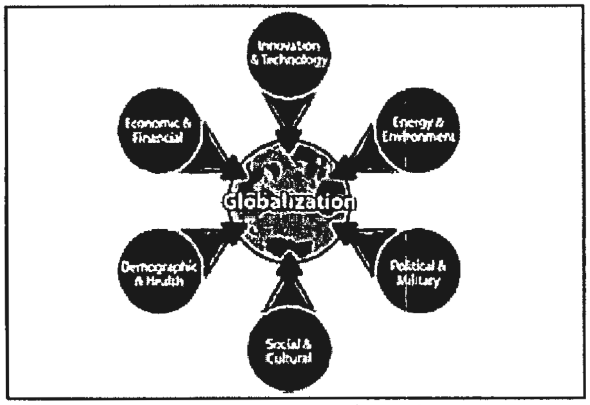


Figure 1: Drivers and Trends

Global networks of information, finance, commerce, transportation, and people shape and empower these threats. This infrastructure increasingly is being targeted for exploitation, and potentially for disruption or destruction, by a growing array of state and non-state adversaries.

> *"We see globalization – growing interconnectedness reflected in the expanded flows of information, technology, capital goods, services and people throughout the world – as an overarching 'megatrend,' a force so ubiquitous that it will substantially shape all the other major trends in the world of 2020."*
>
> *- National Intelligence Council, "Mapping the Global Future, 2020"*

Persistent Threats

For the foreseeable future, we will act to prevent the next terrorist surprise, while addressing the root causes that fuel extremism. We will track the spread of technologies that enable individuals, groups, or rogue states to acquire weapons of mass destruction. We will compete with adversary foreign intelligence services to prevent exploitation of our security vulnerabilities. We will encounter deft attempts at denial and deception as we conduct our collection activities. Finally, we will monitor the economic, military, political and ideological dynamics of regional powers to identify and warn of impending challenges.

Emerging Missions

To these persistent threats we add a growing array of emerging missions that expands the list of national security (and hence, intelligence) concerns to include infectious diseases, science and technology surprises, financial contagions, economic competition, environmental issues, energy interdependence and security, cyber attacks, threats to global commerce, and transnational crime. Foremost among these challenges is the **blurring** of lines that once separated **foreign and domestic intelligence**, and the increased importance of homeland security. By necessity, we must be involved with numerous new partners in interactive relationships, but we must also **respect and maintain the privacy and civil liberties of all Americans.**

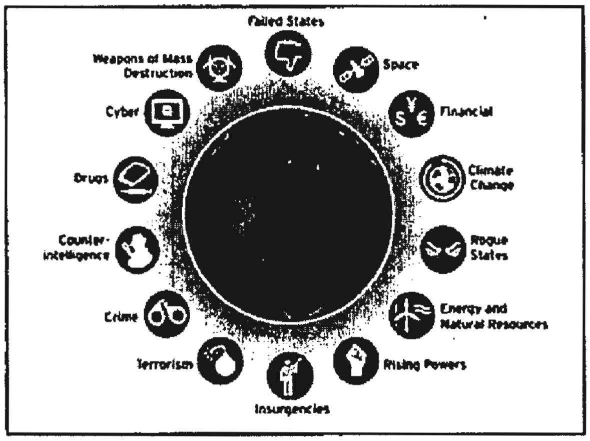


Figure 2: Persistent Threats and Emerging Missions

Old problems assume new dimensions: information operations with emphasis on a cyber domain, asymmetric political or military responses, and illicit trafficking. Lastly, we confront the challenge of acting in an environment that is more time-sensitive and open to the flow of information, in which intelligence sources and analysis compete in a public context established by a global media. By 2015 we will need integrated and collaborative capabilities that can anticipate and rapidly respond to a wide array of threats and risks.

Implications for the Intelligence Community

In this new environment, geographic borders and jurisdictional boundaries are blurring; traditional distinctions between intelligence and operations, strategic and tactical, and foreign and domestic are fading; the definitions of intelligence and information, analysts and collectors, customers and producers, private and public, and competitors and allies are changing. Simply distinguishing between intelligence and non-intelligence issues may prove a major challenge.

To succeed in this fast-paced, complex environment, the Intelligence Community must change significantly. The implications are already apparent. For example, our counterintelligence activities face an array of new and traditional adversaries, yet we must operate within a protected information-sharing environment that challenges existing notions of security and risk.

For collection, the challenge will extend beyond developing a critical source or exploiting a key data stream to determining how to synchronize dissimilar platforms and sources against fleeting and vaguely defined targets, using our collection assets to prompt, detect and respond to what the collection system discovers. **Deep and persistent penetration** is key for collection.

Our analytic professionals will collaborate with world-class experts in academe, commercial interests, and think tanks, all with similar knowledge and personal networks. Deep expertise will require **broad access to open source information**, our unique collection results, and a network of outside experts. Our understanding of the breadth and depth of U.S. policy, intelligence doctrine, and global situational awareness must match the depth of our analyses.

Our most senior intelligence users will place a premium on synthesized presentations that **meld deep expertise with relevance** to the policy agenda and understanding of the nuance of the global situation. Analytic precision and accuracy will be merely the minimum requirements expected by our customers; our analysis must be clear, transparent, objective, and intellectually rich.

Customer demographics and expectations will change; the typical customer in 2015 will be a new generation of government decision-maker, accustomed to instantaneous support, comfortable with technological change, and unfamiliar with intelligence as a privileged source. Such users will expect intelligence to provide customized, interactive support "on demand," and will expect to be treated as a partner – both a source of input and an ultimate intelligence end user.

A Tradition of Evolution & Adaptation

The American intelligence system has long evolved in the face of strategic and technological shifts. Over the first half of the last century, we responded to challenges with advances in aerial imagery, analysis, cryptology, and human intelligence with new organizations like the Federal Bureau of Investigation (FBI) and the Office of Strategic Services (OSS).

During the Cold War, the Intelligence Community fielded high-altitude (e.g., U2/A12), space-based (e.g., Corona), and terrestrial sensors and platforms to peer inside the denied territory of the Communist bloc. The continuing acceleration of change associated with globalization will challenge the Community to respond with innovation once again.

By 2015, a globally networked Intelligence Enterprise will be essential to meet the demands for **greater forethought and improved strategic agility**. The existing agency-centric Intelligence Community must evolve into a true Intelligence Enterprise established on a collaborative foundation of shared services, mission-centric operations, and integrated mission management, all enabled by a smooth flow of people, ideas, and activities across the boundaries of the Intellligence Community agency members. Building such an Enterprise will require the sustained focus of hard-nosed leadership. Services must be shared across the entire spectrum, including information technology, human resources, security, facilities, science and technology, and education and training.

CUSTOMER-DRIVEN INTELLIGE
MISSION-FOCUSED OPERATIONS
NET-CENTRIC INFORMATION ENTERPRISE
ENTERPRISE INTEGRATION

1 THE SHIFTING STRATEGIC LANDSCAPE

2 CREATING DECISION ADVANTAGE

Customer-Driven Intelligence
Mission-Focused Operations
Net-Centric Information Enterprise
Enterprise Integration

3 MAKING IT REAL - IMPLEMENTING THE VISION

2 CREATING DECISION ADVANTAGE

To respond effectively to the changing strategic landscape, we need structures, people and systems aligned to ensure a **unified effort**, ready to adapt with greater agility. As we adjust to new challenges and customers, we reaffirm our enduring mission: to provide objective and relevant support to help our customers **achieve decision advantage.**

The Role of Intelligence

Intelligence employs quiet means **to improve our decision-making** while frustrating that of our enemies. We work behind the scenes to inform and facilitate the actions of diplomatic, military, law enforcement, and other customers. We seek to ensure that they know as much as possible about a situation and that their initiatives have the best chance for success. At the same time, intelligence also helps to impair the reliability, speed, and efficacy of adversaries' decision-making.

Although they may be incremental and short-lived, the advantages provided by intelligence may yield significant results — disrupting a terrorist plot, identifying an illicit account, or halting the proliferation of sensitive technology. Intelligence provides a wealth of leads and opportunities that might otherwise be missed. The fragility of such advantages reinforces the need to preserve our sources and methods.

The historical record provides examples of intelligence providing a competitive edge to American and allied decision-makers:

- **Midway, 1942**: American code breakers provided our military forces with a decisive understanding of enemy intentions and capabilities during the darkest days of World War II. Intelligence provided our military commanders the assurance to turn the tables on an intended Japanese naval trap and gain the strategic initiative in the Pacific.

- **Cuban Missile Crisis, 1962**: Imagery intelligence and analysis provided strategic warning of Moscow's dangerous nuclear gambit. The Community provided excellent situational awareness and estimates of possible Soviet responses that greatly assisted the President in navigating a successful outcome from a nearly catastrophic confrontation.

- **The Six-Day War, 1967**: Community all-source analysts correctly forecast the timing, duration, and outcome of the Arab-Israeli crisis. Their pithy, well-reasoned product enabled the President to modulate U.S. involvement and avoid a larger U.S.-Soviet confrontation.

Decision Advantage

Decision advantage results in the ability of the United States to bring instruments of national power to bear in ways that resolve challenges, defuse crises, or deflect emerging threats. Such advantage will not be permanent or absolute.

> *"...the key to intelligence-driven victories may not be the collection of objective 'truth' so much as the gaining of an information edge or competitive advantage over an adversary. Such an advantage can dissolve a decision-maker's quandary and allow him to act. This ability to lubricate choice is the real objective of intelligence."*
>
> *- Jennifer Sims, Director of Intelligence Studies, Georgetown University*

In dealing with future challenges, it is vital to understand how intelligence makes a difference to the decision-maker. The purpose of intelligence is not solely to determine truth, but to enable decision-makers to make better choices in dealing with forces outside their control. Intelligence helps reduce the degree of uncertainty and risk when critical choices are made. Our measure of success is simple: did our service result in a real, measurable advantage to our side?

This approach neatly resolves the potential tension between intelligence objectivity and relevance, often summarized by the axiom that the Intelligence Community **"speaks truth to power."** At times, members of the Intelligence Community have sought to distance themselves from the customer, in order to remain objective; yet such distance could come at a cost in terms of relevance. This is a false choice; **we must be both objective and relevant.** We will do so by acquiring information more crucial to winning, and by denying competitors that same information (e.g., through denial and deception). We will use all facets of intelligence to accomplish this pledge, without confusing

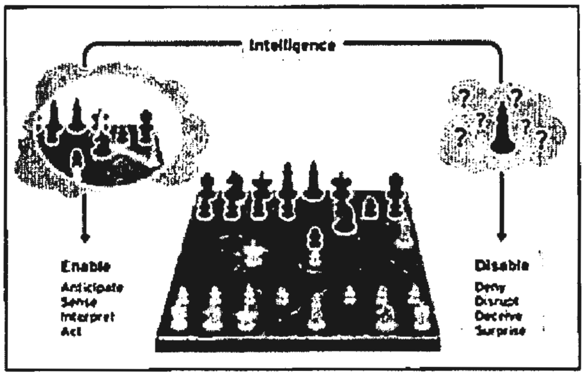


Figure 3: Creating Decision Advantage

the functions with the essentials. For example, some view secrecy as inherent to the intelligence mission. Secrecy, however, is only one technique that may lead to decision advantage; so may speed, relevance, or collaboration. We will not rely on any single; "time-honored" approach in creating decision advantage.

Global Awareness and Strategic Foresight

Another important aspect of decision advantage lies in preparing our decision-makers for **strategic surprises** — those forces or issues that lie off the decision-maker's agenda but may emerge to challenge our intended outcomes. The ability to anticipate change — recognizing key early indicators and alerting decision-makers — is a key role of intelligence. While our capabilities to monitor already-known threats are well-honed — with mission managers generally assigned to oversee our handling of top-tier threats — adaptive intelligence also requires strategic capabilities for sensing and evaluating "weak signals" and other indicators of emerging issues and security risks. The need to prevent strategic surprise was one of the prime factors in the genesis of the U.S. Intelligence Community in 1947. America's rise to superpower status, combined with the complexity and interconnectedness of the emerging strategic landscape, demand that our Intelligence Enterprise provide global awareness and strategic foresight.

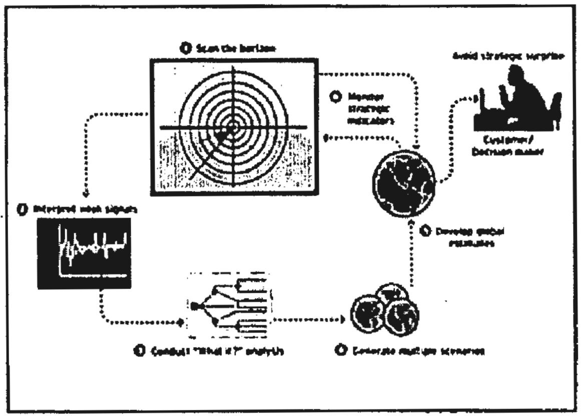


Figure 4: Global Awareness and Strategic Foresight

Strategic warning and predictive estimates were standard art forms in the less dynamic Cold War period. Our anticipated strategic environment models closely on chaos theory: initial conditions are key, trends are nonlinear, and challenges emerge suddenly due to unpredictable systems behavior. In this environment, one prerequisite for decision advantage is **global awareness**: the ability to develop, digest, and manipulate vast and disparate data streams about the world as it is today. Another requirement is **strategic foresight**: the ability to probe existing conditions and use the responses to consider alternative hypotheses and scenarios, and determine linkages and possibilities. We believe our customers will seek our inputs on what may surprise them, if we are capable of placing such inputs in a larger context and demonstrating rigor in our analytic approaches to complexity.

To carry out its mission in an increasingly turbulent and complex global environment, the Intelligence Enterprise must enhance capabilities to evaluate global risks affecting our national security. Greater systems interconnectedness increases the need to identify **vulnerabilities emerging at the nexus of multiple systems** (e.g., critical information infrastructures, disruptions in energy supplies, fragile financial markets, and climate change-related spread of diseases) and the potential for multiple, simultaneous crises. Global awareness and strategic foresight will provide the response to these challenges, linking methods for strategic forecasting and assessment of systems vulnerabilities in constantly renewed communities of diverse expertise and insight. As much of this expertise will be outside of the Intelligence Community, our efforts will be **done in partnership with business, academic, other government, and non-government sectors.**

Customer-Driven Intelligence

By 2015, the Intelligence Community will be expected to provide more details about more issues to more customers. We anticipate different types of customers — with greater expectations — and new demands to change the basic engagement model by which we serve them.

Although there is no typical customer, we will be providing intelligence to a computer-literate generation that grew up with the Internet and user-generated content (e.g., YouTube, blogs, wikis), in which they acted as both a consumer and contributor of information in an "on-demand" environment.

As a consequence, customers in 2015 will define their relationships with the Intelligence Enterprise differently — shifting focus from today's product-centric model toward a **more interactive model** that blurs the distinction between producer and consumer. To create and sustain deep partnerships, the Intelligence Community will require greater use of liaisons who can build relationships and leverage networks to connect information, expertise, and needs in a fluid environment. We will also need to exploit commercial technologies to develop new ways of providing service.

Not only will the type of customer change within our existing federal policy-making sets, but the range of customers will broaden to emphasize other federal departments (e.g., Health and Human Services, Agriculture, Commerce), state and local agencies, international organizations, and private sector and non-governmental organizations.

Generation Y Mindset for 2015

- *Born around 1980; they have no meaningful recollection of the Reagan era or the Cold War.*
- *"Digital natives" who have owned a cell phone their entire adult lives.*
- *Always received most of their news from the Internet.*
- *Sept 11, 2001 dramatically changed their college experience.*
- *Comfortable multi-tasking and working in teams.*
- *Currently in the third career (not job).*
- *Telecommuting is a way of life, not an agency initiative.*
- *Savvy in rapidly accessing and evaluating public domain knowledge.*

Tailored Support

Not all customers will expect the same level of interaction with our Intelligence Enterprise. Our approach to providing customers with tailored support resulting in decision advantage will span a spectrum of customer types, **from partners to clients to consumers.** Our partners will demand the most intense, personalized support and desire to be actively engaged with us while jointly coming to conclusions. Partners will seek to provide us with their expertise, access to their networks, or feedback from their actions and policies. Clients will prefer a more consultative role: close and sustained interaction focused on outcomes relevant to their agenda. Consumers will accept a more transactional relationship with the Enterprise; they will ask questions and expect quick, straightforward answers. One common theme among all of our customers will be a growing substantive and technological sophistication.

Customer Relationships

The importance of the customer in the future clearly calls the Intelligence Community to apply best practices in customer support. To engage customers effectively, we must use sophisticated techniques to elicit their needs and to evaluate our performance. Rather than asking customers, "What are your intelligence priorities?," we will engage them with, "What do you want to accomplish?" Intelligence support to customers will become more of a relationship than an event.

We will begin by extending the lessons learned from our own successful customer support activities (e.g., the President's Daily Brief). We must offer customer service at many levels (not just for the most senior customers) and monitor our progress to inform future changes. We must build an approach that exposes our intelligence professionals to customers and familiarizes new customers with our capabilities and limitations. Key to this will be development of a customer engagement and management model that assigns **"channel managers"** to support specific customers, and apportionment of the channel management function by customer type, by functional topic, or by other means.

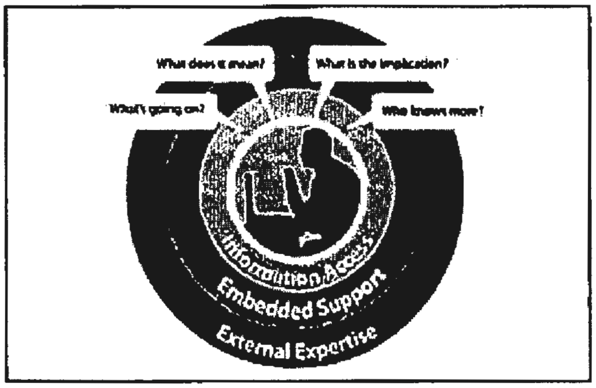


Figure 5: Customer-Driven Intelligence

Our analytic products will increasingly resemble **customized services**, with an emphasis on maximum utility rather than simple releasability. Under concepts such as effects-based analysis, we will engage customers with "What if?" considerations in addition to "What?" conclusions. To do so, our analysts will leverage disparate data and analytic tools and services, working in mission-focused distributed analytic networks.

We also anticipate a growing public demand for intelligence. Most intelligence work will remain classified and limited in distribution to ensure it produces the desired decision advantage for our U.S. government clients. However, the Intelligence Community must adapt to the growing requirement for its analysis to inform the American public.

Although the customer sets, expectations, and engagement models will change, the Intelligence Community will still be expected to provide objective, relevant, and timely intelligence to give our customers a sustained decision advantage in support of our national security objectives.

Mission-Focused Operations

In the past, the Intelligence Community was siloed into discrete disciplines (e.g., signals intelligence, human intelligence, geospatial intelligence, counterintelligence) and functions (e.g., tasking, collection, analysis, dissemination). These silos often led to competition and duplication. Although the agency-centric operating model worked well during the Cold War, it cannot succeed in the current environment, which changes rapidly. We need a mission-focused operating model that is agile, lean, and flexible enough to respond to a dynamic environment. Our new operating model must adapt our enduring roles to our new challenges, incorporate new technologies and processes, and build on our initial successes at integration and collaboration. On the one hand, we

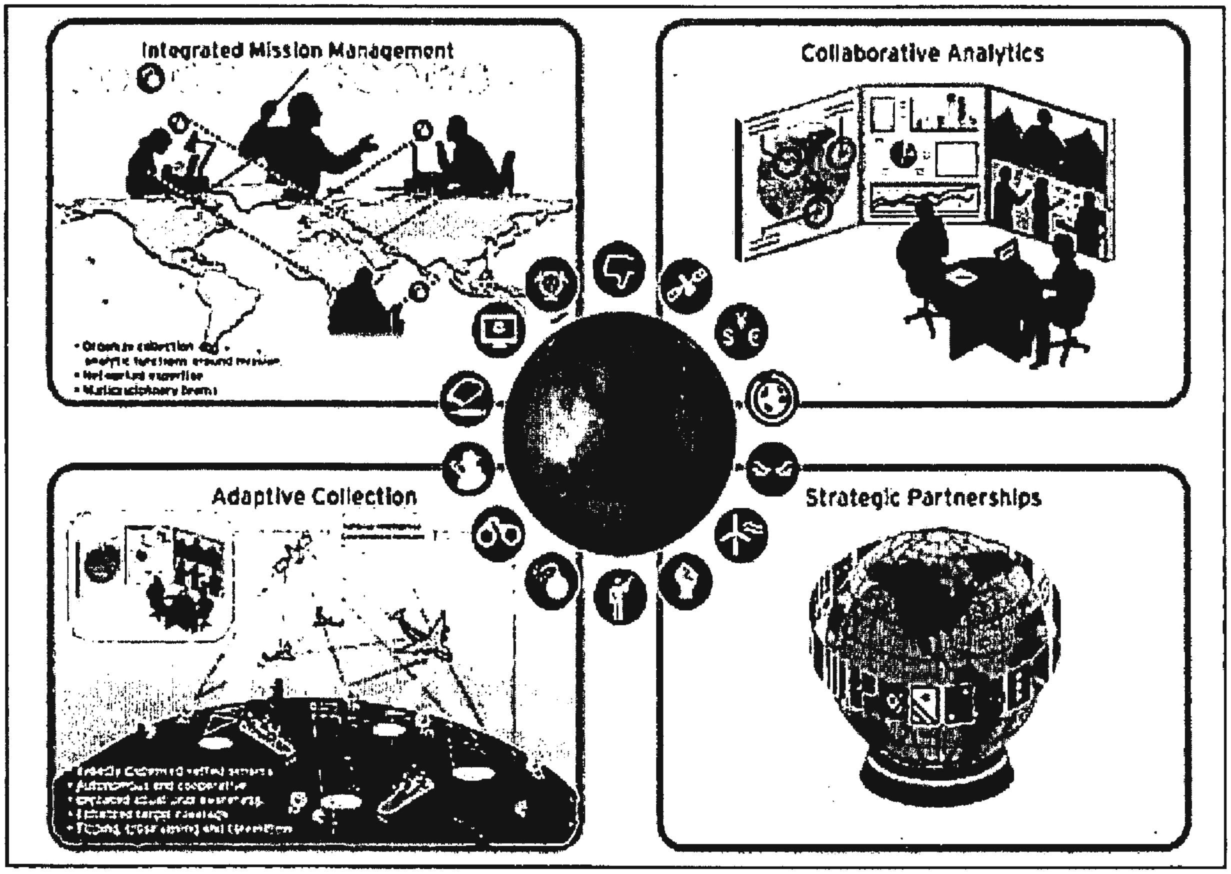


Figure 6: Mission-Focused Operations

must maintain excellence in separate disciplines; on the other, we must develop greater functional integration. More specifically, we must transcend the current agency-based linear model — task, collect, process, exploit, and disseminate — and develop a more mission-based model that is fluid, synchronizes collection, collaborates on analytic issues in real time, and broadens our partnership strategy.

Accordingly, this **integrated operating** model will transform the traditional intelligence cycle into a more dynamic series of interactions among four key operating principles: Integrated Mission Management; Adaptive Collection; Collaborative Analytics; and Strategic Partnerships. This model is designed to promote accuracy, speed and agility without the constraints of organizational equities or functional stovepipes. This new operating model has a simple objective: to operationalize the Intelligence Enterprise, raising mission focus from the unit or agency-level up to a Community-wide activity. To this end, we will need to clarify roles and responsibilities, streamline decision rights, and establish Enterprise-wide governance to enable this new operating model. When this objective has been realized, the Intelligence Enterprise will be both agile and capable, and our partner-customers will benefit from an intelligence-based decision advantage.

Integrated Mission Management

With some exceptions, the current structure and operation of the Intelligence Community are oriented toward agencies, disciplines and specific functions rather than around priority missions. To respond to the dynamic and complex threat environment of the 21st century, our operating model must emphasize **mission integration** - a networked knowledge-sharing model that rapidly pulls together dispersed and diverse expertise and resources against specific missions. This model could manifest itself through an array of networking options - national intelligence centers, mission managers, task forces, and communities of interest.

Integrated Mission Management will improve collection and analysis speed by reducing vertical levels and clarifying tasking authority; enhance innovation through diversity and cross-pollination of ideas; ensure completeness by leveraging niche expertise; and reduce duplication through better coordination. Mission managers will oversee all aspects of national intelligence related to their mission areas and serve as the customer interface for their respective mission responsibilities. Historically, the Community has employed **mission-focused opera-**

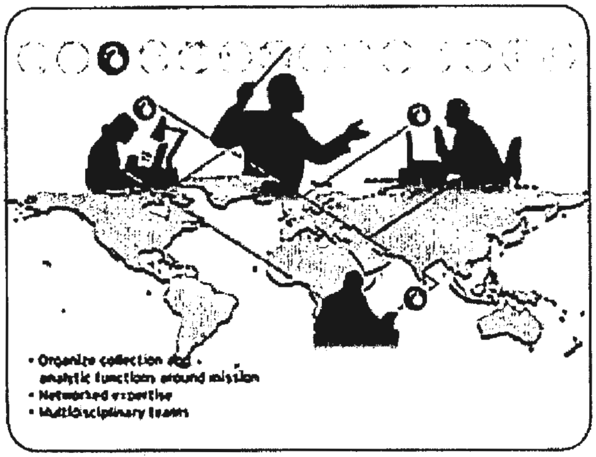

• Organize collection and analytic function around mission
• Networked expertise
• Multidisciplinary teams

Figure 7: Integrated Mission Management

tions as a best practice for forward-deployed intelligence support. The time has come to import this "lesson learned" back to our stateside organizations and activities. Doing so will require **resolute leadership**, since it will entail a **dramatic reconceptualization of how we organize, train, and operate.**

Adaptive Collection

To overcome uncertainty, the collection community will have to "hedge its bets" about future targets and technologies, and adapt quickly to challenges and opportunities; reaction time will be the key to success. The elusive, transitory nature of our targets, and the imbalance between the increasing demand for information and the capacity of our means to collect it, **require multiple, integrated collection systems.** Each of the collection disciplines — human intelligence, signals intelligence, computer network exploitation, geospatial intelligence, measurements and signatures intelligence, open source intelligence, acoustic intelligence, and foreign materiel acquisition — will continue to play key roles, although their relative importance will almost certainly change over time. Our future success demands integration of collection capabilities at all levels.

The principle of Adaptive Collection emphasizes the dynamic allocation and re-allocation of collection, processing, and exploitation. It also provides a mandate to prioritize between open and secret collection means, since secret sources and methods must be reserved for use against those targets that cannot be penetrated using other, more efficient (i.e., open source) means. No aspect of collection requires greater consideration, or holds more promise, than open source information; transformation of our approach to open sources is critical to the future success of Adaptive Collection.

Adaptive Collection is built on a global collection network comprising many netted sensors that can work autonomously- and cooperatively in near-real time. Collection assets would move into and out of specific areas of interest, using already collected information to inform their activities, and in turn, focusing on collecting only that which cannot be obtained by other means. These assets would both push and pull data — raw, semi-processed, and final — into and from our information technology backbone network. The collected data will belong to the Intelligence Enterprise; no single agency "owns" its collection take. We would improve situational awareness, reduce collection time, enhance target coverage, increase robustness of collection capability, and sharpen accuracy through cross-cueing and correlation.

Above all else, the collection community will be measured against its ability to achieve deep and persistent penetrations that are key to understanding foreign leaders' intentions, foreign nuclear programs, terrorist groups, and proliferation networks. Second, there will be more emphasis on multi-agency teams pursuing "multi-INT" collection strategies. Third, we envision a collection community comprising people who speak the languages and know the cultures in which we must operate. Fourth, we envision a collection community capable of rapidly fielding technological innovations that obtain needed information. Finally, we envision a collection community with a **fully integrated processing, exploitation, and dissemination architecture** that moves information quickly to its users. Such architecture will feature both automated and "user-in-the-loop" collection and processing. It will also entail modernization of the collection enterprise to facilitate a holistic awareness of sensor status, tasking and alignment of all collection systems to better respond to its customers. Above all else is the demand that the information reach those who need it, when they need it, in a form that they can easily absorb.

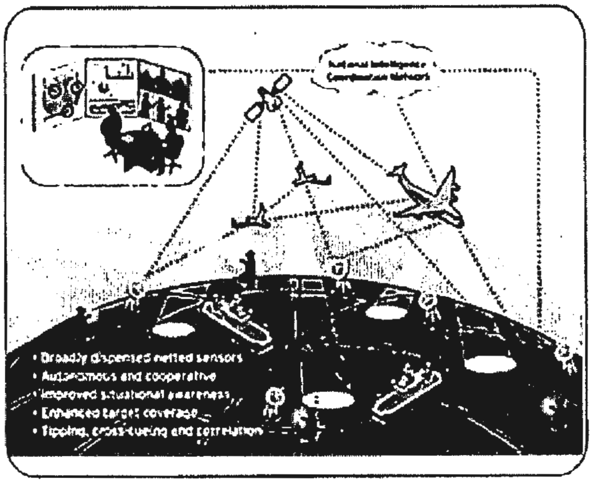

National Intelligence Coordination Network
• Broadly dispersed netted sensors
• Autonomous and cooperative
• Improved situational awareness
• Enhanced target coverage
• Tipping, cross-cueing and correlation

Figure 8: Adaptive Collection

Collaborative Analytics

The analytic community will be expected to understand and develop judgments on a broad spectrum of national security threats, support a more diverse customer set, and cope with access to unprecedented amounts and types of information. Information overload already presents a profound challenge to our business model. Given these challenges, the analytic community has no choice but to pursue major breakthroughs in capability. Applying the principle of Collaborative Analytics, analysts will be freed to work in a fundamentally different way **— in distributed networks focused on a common mission.**

Analytic organizations will therefore make a dramatic shift from traditional emphasis on self-reliance toward more collaborative operations — a shift that will allow the Community as a whole to perform routinely at levels unachievable in the past. Analysts will act individually and as members of Community teams — addressing customer queries, driving collection, trying new methodologies, and collectively building corporate knowledge. The focus of their collaboration will shift away from coordination of draft products toward regular discussion of data and hypotheses, early in the research phase. Collaboration will be aided by expertise registries updated automatically. Managers will use these registries with smart networks to disseminate customer requests directly to the Community analysts best able to contribute. Analysts who offer to join in a response will be directed to a collaborative work site ready to support them.

Information overload will be averted through sophisticated data preparation and tools. In 2015, new information will be tagged so tools can trace related data across our holdings. Analysts will use such tools to mine the data, to test hypotheses and to suggest correlations. Analysts will routinely employ advanced analytic techniques, including scenario-based analysis, alternative analysis, and systems thinking. The move toward extensive use of data, tools, and modeling is at the heart of collaborative analytics.

Collaboration in analysis will also foster smarter collection. The Library of National Intelligence and shared postings of ongoing research will continuously record what we know — and this will help avoid unnecessary new collection. In 2015, the library will hold half a decade of disseminated intelligence, where analysts can discover all available reports — granting immediate access if they are cleared and offering guidance on next steps if they are not. Analyst proposals for new collection will be posted for collaborative review. Collectors will mine that data to improve their own collection planning. Many collectors will share large amounts of newly collected data, tagged for easy discovery and linking, in secure environments with analysts. Bringing analysts and collectors closer together will promote deeper knowledge of collection across the analytic community, which will further improve both the quality of collection requests and the sophistication of analytic judgments.

As analysis becomes more integrated, collaborative efforts will emerge to serve our customers. Our products and services will change to meet evolving needs for timely information and insight, delivered in ways that are personalized. Demand will vary from one client to the next, including virtual meetings, models and simulations, mobile access, and user-selectable versions at different classification levels. New breakthroughs will be driven by timely corporate sharing of information about the needs of key clients, plans for meeting those needs, actual intelligence provided, and feedback received.

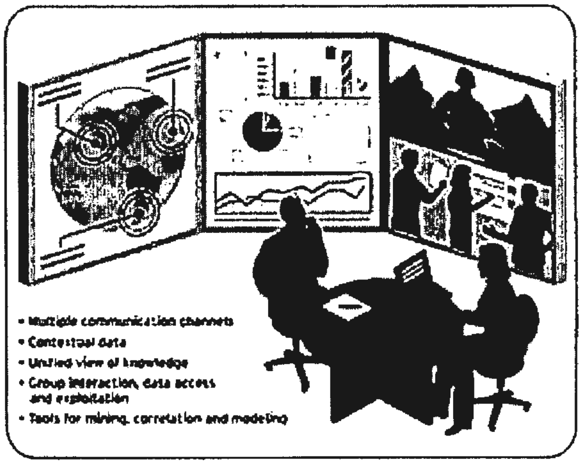

• Multiple communication channels
• Contextual data
• Unified view of knowledge
• Group interaction, data access and exploitation
• Tools for mining, correlation and modeling

Figure 9: Collaborative Analytics

Without obscuring critical disagreements, the Community will free customers from the burden of doing their own intelligence comparison, integration, and deconfliction. Close ties between an integrated analytic community and its customers will allow real-time engagement and clarification of customer needs. By 2015, we will track Community performance against priority topics in a standardized fashion. Managers will be able to see the impact of local contributions to overall Community support to key customers, and will use this information to drive continual improvement and **rapid adaptation** to changing customer needs.

Strategic Partnerships

Given the broad spectrum of threats, looming budget constraints, and the need for deep analytic expertise, the Intelligence Enterprise will have to expand its network beyond the boundary of the traditional Intelligence Community. The global nature of intelligence makes it imperative that we continue to seek opportunities to collaborate with our allies and foreign partners. Our strategic partnerships will

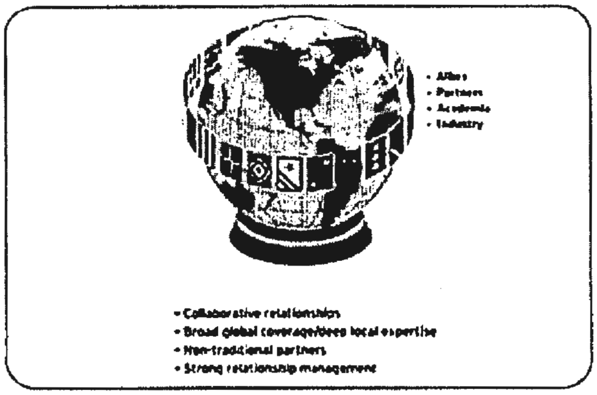

• Allies
• Partners
• Academia
• Industry
• Collaborative relationships
• Broad global coverage/deep local expertise
• Non-traditional partners
• Strong relationship management

Figure 10: Strategic Partnerships

include traditional international allies, opportunistic partners, multinational organizations, civil societies, academe, and industry.

The U.S. Intelligence Enterprise clearly benefits through **increased global coverage, local expertise, and improved synergies.** These benefits span the entire partnership spectrum, depending on the breadth and depth of the relationship: historical bilateral partnerships, alliances, joint programs, transactional, and ad hoc. To reach their full potential, strategic partnerships will need Community-wide strategies. and policies, strong relationship managers and liaisons, and a flexible and secure information-sharing environment. Our partnerships are based on a series of personal relationships reinforced by policy and process. While we must have oversight into the full range of our partnership activities, their success ultimately comes down to the flexibility and effectiveness of those representing us in the relationship. Our representatives must be empowered to engage in the relationship with a strong understanding of the overall "commander's intent" of our activities.

Net-Centric Information Enterprise

Information — classified and open source — is the fuel that powers intelligence. Sharing products is no longer adequate; collectors and analysts have the responsibility to provide much more of what they produce beyond final reports. As a consequence, the Intelligence Enterprise must be built on a robust information infrastructure, based on a culture of information sharing and supported by a range of common services that allow the analytic end user to transform the **deluge of data** into predictive, actionable intelligence.

The end state will be **seamless access** to all intelligence information, tools and processes across multiple agencies and databases. Our information architecture will have to undergo a fundamental shift: from the multiple hub-and-spoke model of information collection, analysis, and dissemination based on specific discipline to a **unified architecture** designed around a common "cloud" (i.e., a distributed peering network) containing our information. This information infrastructure will allow authorized end-users to discover, access, and exploit data through a range of services, from federated query to integrated analytic tool suites.

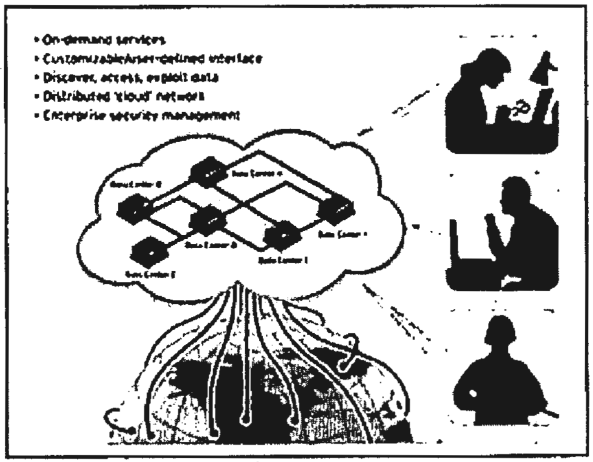

• On-demand services
• Customizable/user-defined interface
• Discover, access, exploit data
• Distributed 'cloud' network
• Enterprise security management

Figure 11: Net-Centric Information Enterprise

Common Information Infrastructure

Currently, each intelligence agency operates and maintains its own network and information infrastructure: power, cooling, circuits, switches, routers, databases, information management systems, data centers, security and enterprise systems management tools. By 2015, we will migrate to a common "cloud" based on a single backbone network and clusters of computers in scalable, distributed centers where data is stored, processed, and managed. The shared data centers will be unique facilities designed and located for access to communication and power supplies. The Intelligence Enterprise will benefit greatly from a more robust, secure, and effective means to organize, update and retrieve all of the information it collects. The centers will also allow experience and technologies employed across the Community to be leveraged, focusing scarce technical resources and reducing costs.

On-Demand Services

Over the last 20 years, the Intelligence Community has been challenged to keep pace with rapidly evolving information technology. Although a less-than-agile acquisition and procurement system has been part of the problem, the Intelligence Community is also undermined by its basic approach. If we are to maintain a technology edge, we must adopt an enterprise-wide, **service-oriented architecture** that is interoperable with systems in other federal departments, and can share information with non-traditional partners. A service-oriented architecture provides a proven means to adapt new technologies while responding to changing user needs. By creating "software as a service," this architecture reduces system complexity and deployment risks through a shared development style, uniform standards, and common interfaces. These services will enable a user-defined analytic environment through the use of **composite applications** – discrete services that can be pulled from a central library and dropped into a user-defined workspace.

The range of Enterprise-wide services that should be deployed by 2015 include communication services (e.g., common e-mail, directories, calendaring, and collaboration); data services (e.g., federated queries and searches, tagging, entity extraction, and storage); security services (e.g., single sign-on, access control, monitoring, and auditing); and analytic services (e.g., portals, data mining, visualization, and modeling and simulation tools).

Enterprise Integration

Providing our customers with a decision advantage and collaborating around our core mission areas require a **strong foundation** that integrates the vital components of the Intelligence Enterprise — people, processes, and technology. Historically, organizational differences — competing cultures, non-interoperable systems, unclear decision rights, and conflicting business rules — acted as barriers to collaboration, greatly undermining our ability to adapt and reducing our organizational agility. Although we have progressed since the 9/11 attacks, and significant initiatives are under way, we will need **continued leadership and organizational commitment** to truly integrate the Intelligence Enterprise by 2015.

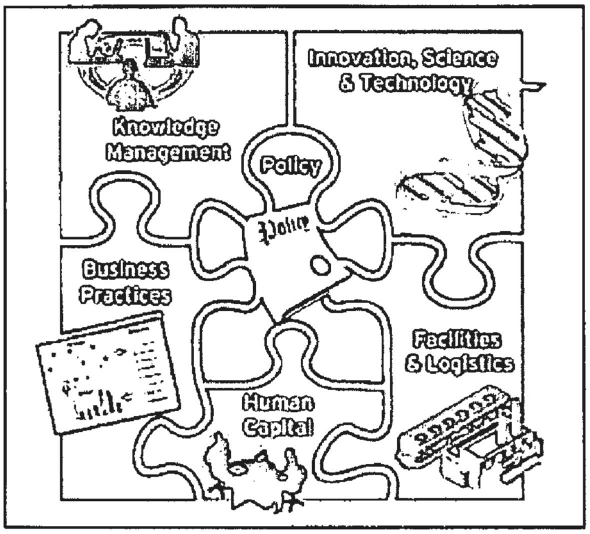


Figure 12: Enterprise Integration

Human Capital and Knowledge Management

At the core of the Intelligence Enterprise in 2015 are our people. One of our biggest challenges will be the ability to attract, train, and retain a highly skilled, innovative and adaptive workforce. The intelligence workforce of the future will be more distributed, virtual, and flexible than at anytime in the past; the implications for our information technology infrastructure and facilities are significant. We need professionals with strong linguistic skills, deep cultural understanding, and mastery of the "human terrain." **Cultural, linguistic, and technical diversity** will be critical to the workforce of the future. Moreover, the changing strategic environment will require a **more entrepreneurial** and customer-focused workforce that can combine deep functional knowledge and expertise with broad networking and collaboration skills. Strict boundaries, such as the distinction between collectors and analysts, must become permeable divisions that highlight different roles our intelligence professionals play during an intelligence career, not exclusive memberships.

Echo of the Future: Joint Duty

In 2007, with the support of the leaders of the six affected US government departments, the DNI signed the Joint Duty policy guidance, making joint duty a prerequisite for promotion to senior executive within the Community. This policy sets a firm standard that -- for the first time -- rewards Enterprise-minded culture

Our leaders will need to transcend the traditional independent, agency-centric orientation, and move toward a leadership style based on cross-agency collaboration and interdisciplinary experience. In particular, this will require **leadership** that can build coalitions across agencies and cultures, bound by a shared purpose and unity of action to achieve mission objectives. Managers will adopt a new role more focused on professional development and measuring work unit quality, less focused on product oversight and review. We will need leadership development programs, performance evaluation systems, and an **incentive structure** that span the Intelligence Enterprise.

By 2015, the focus should shift from information sharing (e.g., interoperable systems, information discovery and access) to knowledge sharing (e.g., capturing and disseminating both explicit and tacit knowledge). Just as we are dismantling today's information "silos," we will need to bridge the knowledge "archipelagos" of tomorrow in a systematic way that combines both content and context in an on-demand environment. Robust social networking capabilities will be required — expertise location, ubiquitous collaboration services, integrated e-learning solutions, visualization tools, and enterprise content management systems. More importantly, a strategic approach to knowledge sharing and management must be incorporated that includes lessons learned and concept and doctrine development.

Modern Business Practices

The Intelligence Community cannot depend on ever-increasing budgets to develop leading-edge technologies, field new capabilities and run current operations. We have to adopt modern business practices that will make us more effective, efficient, nimble, and **accountable**. The current business model is burdened by archaic rules, fragmented practices, and non-interoperable business systems. If we are to optimize our limited resources, we must transform the model; our procedures and systems for planning, programming, **budgeting** and managing personnel **security** must fundamentally change.

Business System Modernization

A key enabler of organizational adaptability and operational agility is an integrated planning, programming, budgeting, enterprise management, and finance system that links and **aligns strategy to budget, budget to capabilities, and capabilities to performance.** We need processes and systems that allow us to anticipate the future for long-term planning, programming and budgeting, and also enable us to respond rapidly to time-critical issues. An integrated business management system must support these business processes. Senior managers must receive timely, accurate and reliable financial and performance information. We must have simple, reliable performance criteria and metrics that demonstrate progress toward our goals.

As part of business modernization, we will move toward a **core financial system** that integrates budget and performance data, while standardizing and streamlining common business processes (e.g., procurement, travel, acquisition, human resources). This will allow us to employ business analytics to drive evidence-based decision-making and more effectively manage our resources.

Security Transformation

By 2015, the security function within the Enterprise will be transformed while growing in importance. Our security practices must parallel, in pace and direction, our technology and workforce efforts. Personnel security must transition from a barrier approach to a **full lifecycle approach**. A web of personal, information technology, and physical security measures will ensure all professionals maintain the highest security standards across an intelligence career. The security officer of the future will be analytically trained and technologically adept, capable of adapting broad security policy to constantly changing technological or customer demands. The Intelligence Enterprise will function on common security standards to empower continuous monitoring. The demands of knowledge sharing with strategic partners will push the security function into a new role: determining classification, and monitoring and governing the overall development of classified information. Security professionals will become primarily responsible for ensuring that our "secrets" are truly secret — and remain so. This new role for security will demand a radical simplification of the classification system and its many codewords and caveats. In the end, the foundation for classification will remain the potential for damage to our nation's security.

Agile Infrastructure

By 2015, employees from different agencies will have to be collocated to more remote locations, away from centralized headquarters. The needs for cross-organizational collaboration, cross-functional teams and programs such as Joint Duty will require a more agile infrastructure. By this, we mean to suggest a deliberate strategy that shifts from agency-centric, massively consolidated facilities towards a more distributed and integrated model that uses **hoteling practices** and creates more **open** and collaborative **workspaces.** Agile infrastructure will be based on two principles — **collocation** of cross-functional teams (e.g., collection disciplines, science and technology, analysts, mission managers) around projects or specific missions, and **virtual collocation**, where a dispersed workforce can rapidly coalesce to respond to new tasking. A facilities strategy will be developed that takes into account both physical and virtual collaboration; a common badging and credentialing system will be required to allow the intelligence workforce to move seamlessly among facilities.

Innovation, Science and Technology

Most of the technology base comes from the private sector; technology cycle times are decreasing, and technological innovation has its source in many countries. Thus, the Intelligence Community will need to fundamentally reconceptualize and redesign our acquisition and procurement policies and processes to emphasize adaptation, speed, and agility. Moreover, since services are a large and increasing portion of the budget, we require procurement policies and practices that acquire capabilities, not simply buy "hours." Innovative, performance-based acquisition solutions will be required. These solutions must reward innovation, performance and risk-taking from our partners in the private sector.

Although we will continue to rely on commercial best-of-breed technologies and best practices, the Intelligence Community will still need to research, develop and field disruptive technologies to maintain a competitive advantage over our adversaries. We cannot evolve into the next technology "S curve" incrementally; we need a revolutionary approach. Breakthrough innovation, disruptive technologies, and rapid transition to end-users will be required, as well as a high tolerance for risk and failure. We need to encourage and reward risk-taking, creativity, and entrepreneurial behavior both with our government employees and our private sector partners. We will need to leverage organizational options (e.g., creating an Intelligence Community version of the Lockheed model Skunk Works®) as well as process improvements (e.g., leveraging workforce diversity to improve cognitive diversity) to foster the creativity we seek. We must work closely with our congressional oversight colleagues to enable an innovation-friendly culture.

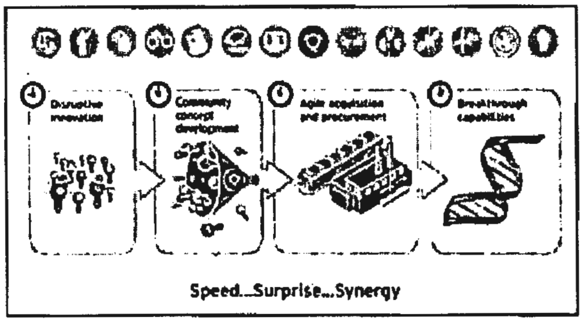

Disruptive innovation
Community concept development
Agile acquisition and procurement
Breakthrough capabilities
Speed...Surprise...Synergy

Figure 13: Innovation, Science and Technology

Creating a culture of innovation will require greater focus on advanced concepts, technology, and doctrine to enhance leadership, organizational alignment and resources. We need to establish a mechanism that allows us to continuously survey the future, capture potential mission impacts, and develop and experiment with new integrative intelligence concepts and technologies.

VISION
2012
2011
2010

1 THE SHIFTING STRATEGIC LANDSCAPE

2 CREATING DECISION ADVANTAGE

3 MAKING IT REAL - IMPLEMENTING THE VISION

THE WAY AHEAD
KEY DESIGN CONCEPTS
STRATEGIC ROADMAP
MANAGING CHANGE

3 MAKING IT REAL - IMPLEMENTING THE VISION

"It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change."
- Charles Darwin

The Intelligence Community of today is composed of some of the most dedicated and capable public servants, and they continue to advance the intelligence reform agenda. However, our efforts to incrementally improve the existing operating model and capabilities will be insufficient in the rapidly evolving, dynamic environment we have entered.

Our many improvements since 2001 have been fueled by sorely needed additional resources, but anticipated budget pressures will likely end this largess in the future. We cannot afford to retreat into incremental improvements or simple efficiencies, which will cause us to fall further behind. We have **no choice but to transform** our profession along the lines presented in our new operating model.

The Way Ahead

Our national security institutions have demonstrated a tendency to focus on their areas of authority and expertise while proving less able to organize joint efforts that fall between domains. The Intelligence Community has suffered the consequences of this problem and perpetuates it. As we learn to unify all instruments of national power in truly joint, interagency initiatives, we will find that intelligence only grows in importance for the new players on the national security team.

The National Intelligence Strategy of October 2005 proclaimed a vision of our Community as "a unified enterprise of innovative intelligence professionals...," but it did not further define that end state. Vision 2015 outlines the rationale for becoming an enterprise, and details the differences in our new operating model. Our Intelligence Enterprise will advance along the distinct paths of adaptability, alignment, and agility.

Key Design Principles

To succeed in this new environment, the Intelligence Community must undertake fundamental organizational and cultural change, moving from a bureaucratic command-and-control model to an integrated, collaborative, networked Enterprise. As we build this Intelligence Enterprise, we need to adhere to a few simple design principles — adaptability, alignment, and agility.

Adaptability is an organization's aptitude for anticipating, sensing, and responding successfully to changes in the environment. It is a process that requires us to continuously survey the external environment, identify discontinuous threats or opportunities, understand the gaps between challenges and capabilities, experiment with new ideas, and learn from experience. The keys to adaptability are active engagement and an openness to outside ideas and influences.

Alignment is the degree of consistency and coherence among an institution's core strategy, systems, processes, and communications. Alignment occurs within a context of strategic direction, ensuring our activities are prioritized to realize a specific vision, without predetermining "how" the vision will be accomplished. It is a control mechanism ensuring that strategic goals, objectives, deployed capabilities, and organizational performance are clearly linked and focused on mission achievement. The key challenge to achieving alignment is ensuring unity of effort without succumbing to conformity of thought.

Agility is an organization's ability to reconfigure processes and structures quickly — with minimal effort and resources — to seize opportunities and address strategic risks. In a complex, dynamic environment, no amount of forecasting can predict every change. We need to create an organization that responds with speed and precision to unforeseen events. Agile organizations possess flexible, modular design, shared infrastructure, and an innovative, risk-tolerant culture.

These design principles need to be integrated and reinforced. Adaptability without alignment creates chaos and wastes resources on duplicate and conflicting efforts; adaptability without agility results in an organization that can "see the train coming down the tracks" but cannot get out of its way. We must ensure that our new organizational models and intelligence concepts adhere to these design principles.

Strategic Roadmap

The Community needs a detailed plan to enact this vision and become an Intelligence Enterprise. The Director of National Intelligence will establish a senior-level design team to develop the specific actions and milestones comprising a roadmap to accomplish our vision. The roadmap will detail actions that will ensure our strategic adaptability, enhance alignment, and improve our organizational agility.

Adaptability actions:

- Develop the means to **forecast** the future environment, anticipate future threats and missions, and consider and deploy innovative alternate intelligence capabilities.
- Develop and experiment with new operational concepts and tactics in support of the integrated operating model.
- Align **innovation** and **experimentation** efforts (e.g., Galileo) in support of this effort.
- Implement and examine multiple models of **mission management** to determine how to best use them operationally.
- Build the organic capability to conduct **exercises** and modeling and simulations throughout our processes (e.g.,analytics, collection, mission management, etc.) to innovate and test new concepts and technologies.
- Integrate lessons learned, history, and education and training activities (as appropriate) to establish the basis for **learning from our successes and failures**.
- Exploit best practices in customer engagement to establish Enterprise-wide **channel managers** who actively engage with our developing partner-customers and evolve our engagement model.
- Establish an intellectual "home" for intelligence professionalism, linked to the **National Intelligence University**, to serve as the thought leader for the Enterprise.

Alignment actions:

- Re-image the Community to acknowledge that member relationships to the Office of the Director of National Intelligence differ. Formalize these different relationships in **policy**.
- Develop an Intelligence Enterprise strategy that **aligns ends, ways, and means.**
- Deploy a unitary, transparent, and disciplined **strategic management process** to drive integrated strategy-to-capabilities-to-plans and budgets across the enterprise.
- Build an annual strategy-to-plans structure that focuses agency and element performance on specific goals and objectives, with tangible **metrics**, to ensure that we progress toward accomplishing our missions and achieving our vision.
- Integrate our **counterintelligence** capabilities through increasingly rigorous policy, doctrine, standards and technology, and align counterintelligence with our broader National Intelligence Strategy goals and objectives.
- Develop the policies, procedures and infrastructure to permit the creation of new, temporary, **mission-focused** elements to serve as the operational arms of the Intelligence Enterprise.
- Embrace a **culture of performance** that encompasses the individual, the agency and the Enterprise.

Agility actions:

- Re-image the Intelligence Enterprise to find ways to flatten the hierarchy and reduce to the "tooth-to-tail" ratio.
- Create an Intelligence Enterprise concept of operations to detail the components of the integrated operating model.
- Clarify roles, missions, functions and decision rights through policies and procedures and streamlined processes.
- **Dramatically improve the access and flow of critical information** — both operational and management — across the Enterprise.
- Shift from large, expensive collection platforms towards smaller, netted collection systems.
- **Identify and consolidate services of common concern** (e.g., human resources, finance, public affairs, general counsel, legislative affairs) to streamline and simplify Enterprise support activities.
- Seek new means to enhance enterprise culture through integrated operations (multi-agency), practices (doctrine, tradecraft, etc.) and support services (alternate work locations, hoteling). Deploy such capabilities in parallel with existing ones and rigorously pursue the better performing options.
- Foster a risk-tolerant culture by rewarding agencies, leaders, or other intelligence professionals who seek to adopt new practices to improve performance or efficiency.

Leading Change

The first and most significant impediment to implementation is internal and **cultural:** we are challenging an operating model of this Vision that worked, and proponents of that model will resist change on the basis that it is unnecessary, risky, or faddish. These opponents will posit that incremental change is working, the environment is not really that different, and the new methods are unproven.

A second impediment is existing institutional barriers, which create **friction**. Few things sap the determination for change as effectively as the friction induced by layers of bureaucratic inefficiency working to frustrate any endeavor. Stove-piped "back-office" functions that make even simple personnel or operational activities difficult will complicate nearly every aspect of transformation.

A third impediment is **budgetary**. Dramatic transformation of the Intelligence Community will require stable and somewhat predictable budgets. While some efficiency gains will be realized through rationalization and consolidation, change cannot happen on the cheap. This challenge must first be addressed by responsible internal management practices at all levels, guided by a detailed strategic roadmap and better communications and engagement with the appropriators and authorizers.

A fourth impediment is environmental: the **tyranny of the immediate.** For nearly four decades, intelligence reform has remained largely stymied by the inability of the Community to emphasize sustained implementation. Senior leaders across the Intelligence Community face constant pressure to depart from carefully considered approaches to deal with pressing day-to-day challenges.

Translating our Vision into reality will take more than desire and good intentions. First, we will need effective outreach and aligned communications to energize the organizations that comprise the Intelligence Enterprise. We will need strong leadership, unyielding commitment, and empowered change agents to mobilize the workforce. Second, we must align the Enterprise through a new National Intelligence Strategy, a strategic roadmap that establishes key capability milestones over the FY11-16 planning and programming horizon, and the development and management of annual implementation plans to ensure accountability and progress. Third, we will need to assign responsibility for accomplishing this Vision to key areas throughout the Enterprise: missions (e.g., counterterrorism, counterproliferation, counterintelligence, etc.), agencies, program managers, and functional leads (e.g., Chief Information Officer, Chief Human Capital Officer, Science and Technology). Fourth, we need to institutionalize change by ensuring short-term wins, measuring and rewarding performance against the vision, and ensuring continuous improvement through quarterly reporting and evaluation sessions with senior leadership throughout the Intelligence Enterprise. Perhaps most importantly, senior leadership must commit to building a culture that will take risk to make this Vision real.

The transformation of the Intelligence Community into an Intelligence Enterprise will not come easily; if it were an easy process, our dedicated intelligence professionals would have completed it long ago. Although change is disconcerting by its very nature, the changes elaborated in this Vision are necessary for our continued success and for the defense of our nation. We will encounter halting progress and occasional setbacks, but we will succeed in remaking today's best Intelligence Community into the best Intelligence Enterprise the world has ever seen.

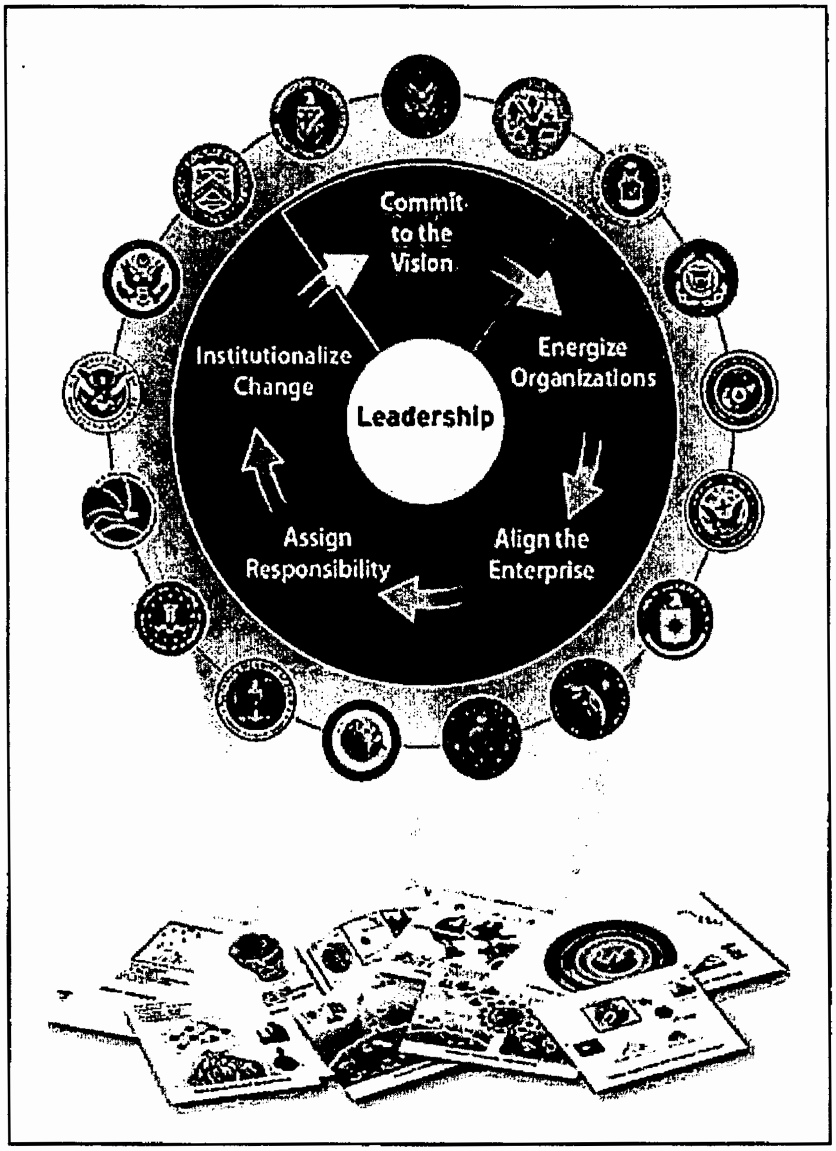


Figure 14: Leadership Driving Transformation

VISION 2015 ~ At-A-Glance

Decision Advantage

The employment of all facets of intelligence to acquire and provide information to gain an edge or competitive advantage that is crucial to winning while denying competitors that same information

Customer-Driven Intelligence

The ability to broaden the customer set while deepening relationships to drive the development and delivery of objective, relevant, timely, and accurate intelligence through a range of tailored products and services

Global Awareness and Strategic Foresight

The ability to anticipate, and alert decision-makers to strategic surprises by sensing and evaluating weak signals and developing alternative hypotheses and a range of scenarios to better understand a complex, rapidly evolving and unpredictable global environment

Mission-Focused Operations

A concept of operations that transcends the current agency-centric model towards a more mission-based configuration that is agile, synchronizes collection, and connects dispersed and divergent expertise to collaborate on hard problems

- **Integrated Mission Management** - Integrates and orchestrates resources and expertise around mission, not agency or discipline
- **Adaptive Collection** - The dynamic reallocation of distributed and networked sensors that can work autonomously and cooperatively to improve situational awareness, reduce collection times, enhance coverage, and improve accuracy through cross-cueing and correlation
- **Collaborative Analytics** - The capability to manage and exploit unprecedented information overload and free analysts to work in distributed information networks focused on a common mission
- **Strategic Partnerships** - The ability to extend the Intelligence Community beyond the traditional network to increase global coverage, deepen local expertise, and capture mission synergies by expanding our partnership model to include allies, opportunistic partners, academe, and industry

Net-Centric Information Enterprise

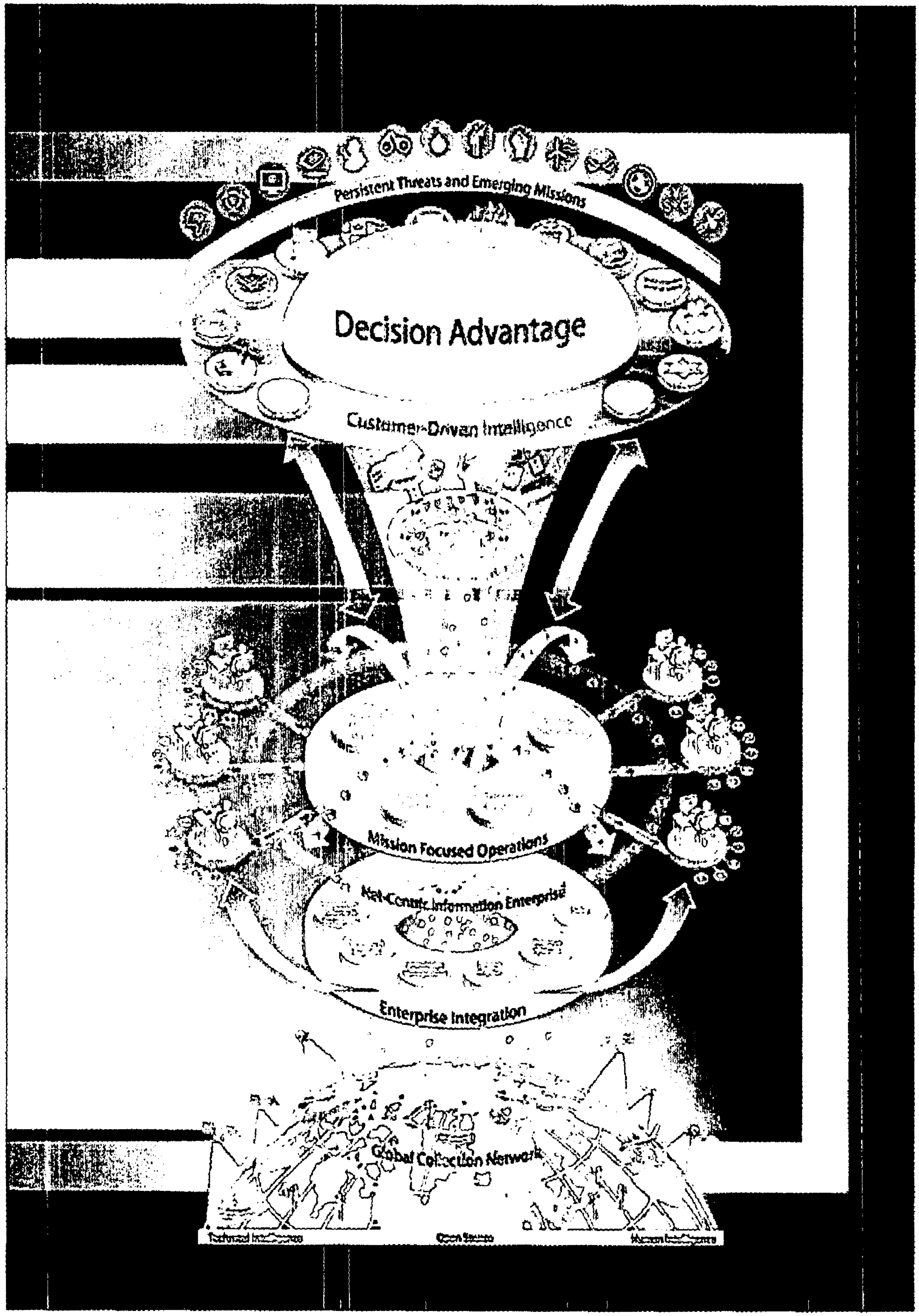
A common information infrastructure that provides seamless access to all intelligence information, services, and tools across multiple agencies and databases

- Develop a common "cloud" based on a single backbone network and clusters of servers in scalable, distributed centers where data is stored, processed and managed
- Discover, access, and exploit data quickly and completely
- User-defined analytic environment through "drag and drop" composite applications
- Protects information from those who should not have it

Enterprise Integration

Creation of a strong institutional foundation that integrates the vital components of the Intelligence Enterprise – policy, people, processes, infrastructure, and technology – to remove the barriers to collaboration and reduce the "tooth-to-tail" ratio through greater economies of scale

A Globally Networked and Integrated Intelligence Enterprise


Persistent Threats and Emerging Missions
Decision Advantage
Customer-Driven Intelligence
Mission Focused Operations
Net-Centric Information Enterprise
Enterprise Integration
Global Collection Network
Technical Intelligence
Open Source
Human Intelligence

Director of National Intelligence
Washington DC, 20511

22. An Overview of the United States Intelligence Community for the 111th Congress.

Prepared for the 111th Congress by the Office of the Director of National Intelligence, this document will provide a general overview of the United States Intelligence Community.

An Overview of the
United States Intelligence Community
for the
111th Congress

2009

Table of Contents

U.S. Intelligence Organization Profiles

Program Managers

Departmental Components

Service Components

Office of the Director of National Intelligence

The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC) and is the principal advisor to the President, the National Security Council, and the Homeland Security Council (HSC) for intelligence matters related to national security. Also, the Director oversees and directs the implementation of the National Intelligence Program. The President appoints the DNI and the **Principal Deputy Director** with the advice and consent of the Senate.

The DNI's responsibilities, among others, are to lead the IC; oversee the coordination of foreign relationships between elements of the IC and intelligence services of foreign governments; establish requirements and priorities for collection, analysis, production, and dissemination of national intelligence; coordinate reform of security clearance and acquisition processes; achieve auditable financial statements; support legislative, legal and administrative requirements; ensure compliance with statutory and Presidentially-mandated responsibilities; and transform the IC into a unified, collaborative and coordinated enterprise.

The DNI Organization is composed of the DNI Staff and Intelligence Community Mission and Support Activities (MSAs). The DNI Staff is primarily responsible for IC policy and oversight and the preparation of the National Intelligence Program Budget. The MSAs are directly responsible for providing IC-wide substantive intelligence, counterintelligence strategy and strategic analysis, research and development, and training and education. The Director of the Intelligence Staff is responsible for synchronizing and integrating efforts across the DNI Organization.

There are four Deputy Directors of National Intelligence:

> **Office of the Deputy Director for Policy, Plans and Requirements** (DDNI/PPR) drives vital intelligence reform by coordinating IC-wide policy and strategy, plans, and requirements; modernizing security processes; and strengthening relationships with Federal, State, Local, foreign, and private sector partners.
>
> **Office of the Deputy Director for Collection** (DDNI/C) coordinates collection throughout the IC under the authorities of the DNI. The DDNI/C ensures that the President's and the DNI's priorities are appropriately reflected in future programming and systems acquisition decisions and puts into context for the DNI the way in which actions affect the total collection mission.
>
> **Office of the Deputy Director for Analysis** (DDNI/A) has responsibility for enhancing the quality, timeliness, and utility of analytic support to intelligence

consumers. DDNI/A's approach for achieving this goal is to increase expertise and improve analytic tradecraft at individual, agency, and Community levels through specialization, collaboration, and cross-fertilization. The DDNI/A serves concurrently as the Chairman of the National Intelligence Council (NIC) and manages the production of the President's Daily Brief.

Office of the Deputy Director for Future Capabilities (DDNI/FC) is the Intelligence Community's catalyst for technical innovation, responsive stewardship, and acquisition excellence. Its approach is to address these key intelligence challenges by: leading advanced research and development focusing on disruptive technology leaps; acting as the DNI's Science & Technology advisor and integrating the Intelligence Community Science & Technology enterprise; developing and evaluating an IC-wide, end-to-end collection architecture to promote innovation and responsible financial stewardship; and establishing and maintaining an agile and transparent best-practice environment that promotes IC acquisition success.

Other elements of the DNI Staff include a **Civil Liberties Protection Office**, and an **Office of Equal Opportunity and Diversity** both of which drive IC-wide policies and programs in their respective areas.

Three Mission Managers integrate IC-wide collection and analysis on North Korea, Iran and Cuba/Venezuela.

IC Mission Support Activities

The DNI organization includes ten functional mission support activities:

National Counterterrorism Center (NCTC) serves as the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the United States Government (except purely domestic terrorism).

National Counterintelligence Executive (NCIX) is staffed by senior counterintelligence and other specialists from across the national intelligence and security communities. The NCIX mission is to exploit and defeat adversarial intelligence activities directed against U.S. interests; protect the integrity of the U.S. intelligence system; provide incisive, actionable intelligence to decision-makers at all levels; protect vital national assets from adversarial intelligence activities; and neutralize and exploit adversarial intelligence activities targeting the armed forces.

National Counterproliferation Center (NCPC) is responsible for coordinating strategic planning within the IC to enhance intelligence support to United States efforts to stem the proliferation of weapons of mass destruction and related delivery systems.

The Special Security Center's (SSC) mission is to assist the DNI in protecting and sharing national intelligence information throughout the IC, the U.S. Government, U.S. contractors, state, local, tribal governments, and our foreign partners by conducting assessments of the security of sensitive compartmented information and other intelligence information under the DNI's authority; document overall IC security compliance for the DNI; monitor, coordinate and advise on significant unauthorized disclosures and compromises of classified national intelligence information; and provide feedback to support policy formulation and training initiatives.

The National Intelligence University (NIU) operates under the DNI's authority to establish an integrated framework that brings together the educational components of the IC in order to promote a more effective and productive Intelligence Community through cross-disciplinary education and joint training. The NIU is made up of the existing IC schools and universities, the Office of the Chancellor of the NIU, and the staff and curriculum that support the goals and authority of the DNI.

Intelligence Advanced Research Projects Activity (IARPA) invests in high-risk/high payoff research that has the potential to provide the U.S. with an overwhelming intelligence advantage over our future adversaries.

The Center for Security Evaluation's (CSE) mission is to strengthen overseas security standards, provide for inter-agency, life-cycle inspections, and aggressively pursue emerging security technologies with security solutions that are risk-based and realistic. CSE is the organization that synchronizes IC emergency preparedness activities for the DNI and National leadership.

The National Intelligence Council (NIC) is the IC's center for mid-term and long-term strategic analysis. The NIC supports the DNI in his roles as head of the IC and principal advisor for intelligence matters to the President and the National Security and Homeland Security Councils, and serves as the senior intelligence advisor representing the IC's views within the U.S. Government. The NIC also provides key products and services, such as the National Intelligence Estimates assessing future trends on a wide range of global issues.

The National Intelligence Coordination Center (NIC-C) was established in October 2007 in collaboration with the Department of Defense and several domestic agencies to provide a mechanism to coordinate intelligence activities across the entire U.S. Government. The NIC-C works to efficiently coordinate, collaborate, assess, and deploy our Nation's total array of intelligence collection capabilities.

The Mission Support Center provides support services to all DNI Staff and Mission Support Activity components.

Central Intelligence Agency

The Central Intelligence Agency (CIA) is the largest producer of all-source national security intelligence to senior U.S. policymakers. The CIA's intelligence analysis on overseas developments informs decisions by policymakers and other senior decision-makers in the national security and defense arenas. CIA does not make foreign policy.

The Director of the CIA is the **National Human Intelligence (HUMINT) Manager** and serves as the national authority for coordination, de-confliction, and evaluation of clandestine HUMINT operations across the IC, consistent with existing laws, Executive Orders, and interagency agreements.

The **National Clandestine Service (NCS)** has responsibility for the clandestine collection (primarily HUMINT) of foreign intelligence that is not obtainable through other means. The NCS engages in counterintelligence activities by protecting classified U.S. activities and institutions from penetration by hostile foreign organizations and individuals. NCS also carries out covert action in support of U.S. policy goals when legally and properly directed and authorized by the President.

The Directorate of Intelligence (DI) analyzes all-source intelligence and produces reports, briefings, and papers on key foreign intelligence issues. This information comes from a variety of sources and methods, including U.S. personnel overseas, human intelligence reports, satellite photography, open source information, and sophisticated sensors.

The Directorate of Science and Technology (DS&T) accesses, collects, and exploits information to facilitate the execution of the CIA's mission by applying innovative scientific, engineering, and technical solutions to the most critical intelligence problems.

The Directorate of Support (DS) delivers a full range of support, including acquisitions, communications, facilities services, financial management, information technology, medical services, logistics, and the security of Agency personnel, information, facilities, and technology. DS services are both domestic and international in focus and are offered on a 24 hours a day/7 days a week basis.

Defense Intelligence Agency

The Defense Intelligence Agency (DIA) is a major producer and manager of foreign military intelligence for the Department of Defense and is a principal member of the United States Intelligence Community. Established on October 1, 1961, and designated a combat support agency in 1986, DIA's mission is to provide timely, objective, all-source military intelligence to policymakers, to U.S. armed forces around the world, and to the U.S. acquisition community and force planners to counter a variety of threats and challenges across the spectrum of conflict.

The Director of DIA is a three-star military officer who serves as the principal advisor on substantive military intelligence matters to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff. Additionally, he or she is the Program Manager for the General Defense Intelligence Program which funds a variety of military intelligence programs at and above the corps level. The Director also serves as Program Manager for the Department's Foreign Counterintelligence Program and is the Chairman of the Military Intelligence Board which examines key intelligence issues such as information technology architectures, program and budget issues, and defense intelligence inputs to National Intelligence Estimates.

With headquarters in the Pentagon, DIA's more than 15,000 highly skilled civilian and military personnel are located around the world with major activities at the **Defense Intelligence Analysis Center** on Bolling Air Force Base in Washington, D.C.; the **Missile and Space Intelligence Center** at Redstone Arsenal in Huntsville, Alabama; and the **National Center for Medical Intelligence** at Fort Detrick, Maryland. DIA also deploys military and civilian personnel worldwide during crises or conflicts to better support military forces.

In December 2007, DIA established the **Defense Intelligence Operations Coordination Center (DIOCC)** to seamlessly integrate all defense intelligence resources on the transnational threats to U.S. national security and to enhance defense intelligence collaboration. The DIOCC collaborates with DoD and national intelligence resources to manage risk and resource requirements. It integrates and synchronizes all-source military and national-level intelligence capabilities in support of the warfighters.

Working closely with the DIOCC to help manage risk and intelligence resources is the **Joint Functional Component Command for Intelligence, Surveillance and Reconnaissance (JFCC-ISR).** The DIA Director is the commander of this U.S. Strategic Command organization. The JFCC-ISR monitors Combatant Command intelligence, surveillance and reconnaissance (ISR) information needs; serves as the Intelligence Community's entry point into the DoD ISR system; works to maximize efficient use of ISR assets and identifies gaps in ISR coverage.

Through the **Joint Staff J2**, DIA operates the intelligence component within the National Military Command Center, providing real-time indications and warning of breaking situations and serving as the national focal point for crisis intelligence support to military operations. During a crisis or contingency, DIA establishes intelligence task forces, working groups or dedicated cells to closely monitor unfolding events.

In an effort to strengthen management, synchronization and deconfliction of HUMINT and counterintelligence capabilities across the Department of Defense, including the military services and Combatant Commands, DIA established the **Defense Counterintelligence and HUMINT Center (DCHC)** in August 2008.

DIA's **Directorate for Human Intelligence (DH)**, conducts human intelligence operations worldwide to obtain critical intelligence often not available from technical collection means. DH operations provide in-depth and actionable intelligence to policymakers and military forces in the field. It manages the Defense Attaché System, which has military attachés assigned to more than 137 U.S. embassies.

To support DoD efforts in the global war on terrorism, DIA established the **Joint Intelligence Task Force for Combating Terrorism** to consolidate and produce all-source terrorism-related intelligence.

As more countries move their critical facilities underground, DIA's **Underground Facility Analysis Center** leverages the Nation's intelligence and other technical resources to coordinate the Intelligence Community's efforts to detect, identify, characterize, and assess for defeat hardened and deeply buried underground facilities and their associated programs worldwide.

The DIA **Missile and Space Intelligence Center** is the DoD authority on man-portable air defense systems and develops scientific and technical intelligence on foreign missile systems such as: short-range ballistic missile systems; surface-to-air missile systems; antitank guided missile systems; antiballistic missile systems; ground-based anti-satellite systems; and associated command and control systems.

DIA's **National Center for Medical Intelligence** provides medical profiles of foreign countries and assesses real and potential health hazards to support U.S. Armed Forces worldwide operations to include humanitarian operations.

DIA operates the **National Defense Intelligence College**, a fully accredited educational institution, to satisfy the growing need for trained intelligence professionals to help safeguard the Nation's interests.

Department of Justice
Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) is a threat-based, intelligence driven, national security organization that protects the United States from critical threats while safeguarding civil liberties. As both a component of the Department of Justice and a full member of the U.S. Intelligence Community, the FBI serves as a vital link between intelligence and law enforcement communities. The FBI brings the discipline of the criminal justice system to its domestic intelligence activities in a manner that is consistent with American expectations and protections for privacy and civil liberties, and thus is uniquely situated to be effective against today's complex adversaries.

The FBI's top priorities are combating the threat of terrorism, counterintelligence and cyber crime. As to counterterrorism, the FBI gives particular attention to terrorist efforts to acquire and use weapons of mass destruction. While numerous plots have been disrupted, the threat continues to evolve; the need for constant vigilance has not diminished. The FBI must continuously adapt to trends in terrorist recruitment, financing and training, as well as terrorists' development of new explosive devices, biological and chemical agents.

As to counterintelligence, foreign intelligence services continue their attempts to infiltrate the U.S. Government; we also face a growing presence of foreign businesspersons, students and scientists seeking to steal technology on behalf of foreign governments or commercial interests. Investigations of economic espionage, financial crimes, export control violations, cyber intrusions and the compromise of U.S. strategic intellectual property, such as innovations and patented inventions, are on the rise.

Cyber threats cross all investigative categories, are borderless, and have the potential for disruption. Of greatest concern are terrorists or foreign state-sponsored elements targeting national information infrastructure, and criminal enterprises and individuals who illegally access computer systems or spread malicious code. There is also growing and evolving forms of identity theft, and use of the Intemet to perpetrate fraud, child pornography and solicitation of children online.

Public corruption and civil rights violations from hate crimes, abuse of power by law enforcement, and human trafficking including the exploitation of children, remain the FBI's top criminal priorities because of unique jurisdiction and the potential impact of these crimes on our democracy. Other areas receiving priority focus are crimes that undermine the health of the economy, including large-scale financial institution frauds, securities and commodities or bank fraud, environmental crimes, health care fraud and telemarketing fraud. In the area of violent crimes, the FBI focuses on increasingly sophisticated national and transnational gangs, dangerous fugitives, and kidnappings. We leverage our partnerships with over 800,000 state, local and tribal law enforcement agencies though task forces and fusion centers to collect and disseminate intelligence, serving as a unique link between the intelligence and law enforcement communities.

Federal law, Attorney General authorities and Executive Orders give the FBI jurisdiction to investigate all federal crimes not assigned exclusively to another federal agency (28 U.S.C. Section 533) and to investigate threats to the national security (EO 12333; 50 U.S.C. Section 401 et seq; 50 U.S.C. Section 1801 et seq).

Additionally, there are other laws that give the FBI responsibility to investigate specific crimes. This combination of authorities gives the FBI the unique ability to address national security and criminal threats that are increasingly intertwined, and to shift between the use of intelligence tools such as surveillance or recruiting sources, and law enforcement tools of arrest and prosecution. Regardless of which tools are employed, law and policy require that the FBI's information gathering activities use the least intrusive techniques possible to accomplish the objective and cannot be based solely on activities protected by the First Amendment.

National Geospatial-Intelligence Agency

The National Geospatial-Intelligence Agency (NGA) is a Department of Defense combat support agency and a member of the national Intelligence Community (IC). NGA develops imagery and map-based intelligence solutions for U.S. national defense, homeland security and safety of navigation.

Headquartered in Bethesda, Maryland, NGA has major facilities in the Washington, D.C., Northern Virginia and St. Louis, Missouri, areas. NGA also provides global support to IC mission partners through NGA representatives stationed around the world.

Mission

NGA provides timely, relevant and accurate geospatial intelligence in support of national security.

GEOINT

Geospatial intelligence (GEOINT) is the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the Earth.

GEOINT answers the questions "When?" and "Where?" It uses imagery to make sense of volumes of data and information. GEOINT builds the bridge from information to intelligence—from decision to action.

NGA's Role in the Intelligence Community

NGA is the IC's principal producer of and adviser for GEOINT. During the 20th century, NGA took a leadership role in collaborating with mission partners. In the 21st century, NGA is building on that tradition as it develops more efficient ways to exchange information and broaden access to all GEOINT sources and data to enable the production of high-quality intelligence throughout the IC.

Know the Earth...Show the Way

NGA supports the vision "Know the Earth...Show the Way" by developing and disseminating GEOINT in all its forms—including imagery, imagery intelligence and geospatial information—to policymakers, decision-makers and warfighters, and by working alongside them to ensure their effective use of the specific GEOINT they need to carry out their missions.

Combat and Humanitarian Support

As a Department of Defense combat support agency, NGA provides the warfighter with precise, timely GEOINT data, information and products.

Accessibility and usability are the watchwords as NGA continues to focus on moving data to people, instead of moving people to data.

In addition to supporting combat operations, NGA also supports disaster relief and homeland defense operations by providing GEOINT data, products and analyses to lead federal agencies and first responders.

National System for Geospatial Intelligence

The National System for Geospatial Intelligence is a unified community of GEOINT experts, producers and users organized around the goal of integrating technology, policies, capabilities and doctrine to produce GEOINT in a multi-intelligence environment.

NGA, as the Functional Manager for the National System for Geospatial Intelligence, provides strategic thinking, guidance and direction to the IC concerning all aspects of GEOINT, from its acquisition to its utilization. NGA collaborates with mission partners to ensure that accurate and timely GEOINT is a part of decision making and operations where it is needed and when it is needed.

The Future

NGA is developing new partnerships, strengthening existing collaborations and advancing the agency's mission within the context of the larger IC to meet the challenges of the post-9/11 world.

As part of that effort, NGA continues to advance from a hardcopy orientation to a data-centric digital environment in which mission partners will have ready access to GEOINT databases through an open architecture of interoperable systems.

National Reconnaissance Office

The National Reconnaissance Office (NRO) was established in September 1961 as a classified agency of the Department of Defense. The existence of the NRO and its mission of overhead reconnaissance were declassified in September 1992. The NRO is the "nation's eyes and ears in space." Headquartered in Chantilly, Virginia, the NRO is a joint organization engaged in the research and development, acquisition, launch, and operation of overhead reconnaissance systems necessary to meet the needs of the IC and the Department of Defense. The NRO conducts other activities as directed by the Secretary of Defense and/or the DNI. The Director of the National Reconnaissance Office is selected by the Secretary of Defense with the concurrence of the DNI and also serves as the Assistant to the Secretary of the Air Force (Intelligence Space Technology).

The NRO's workforce includes personnel assigned to the NRO primarily from the Air Force, the CIA, and the Navy. However, the other uniformed services and other elements of the Department of Defense and the IC are also represented. Another important part of the NRO team includes some of this country's leading aerospace corporations and research centers.

NRO's organizational goals are to:

- Be a foundation for global situational awareness; and
- Provide intelligence on timelines that are responsive to user needs.

The NRO collaborates closely with its mission partners: NSA, NGA, CIA, U.S. Strategic Forces Command, U.S. Air Force, U.S. Army, and the Department of the Navy, as well as other intelligence and defense organizations.

Information collected using NRO satellites is used for intelligence and analysis for a variety of tasks, such as warning of potential foreign military aggression, monitoring weapons of mass destruction programs, enforcing arms control and environmental treaties, and assessing the impact of natural and manmade disasters.

National Security Agency

The National Security Agency (NSA) is the U.S.'s cryptologic organization, with responsibility for protecting U.S. National Security information systems and collecting and disseminating foreign signals intelligence. Areas of expertise include cryptanalysis, cryptography, mathematics, computer science, and foreign language analysis. NSA is part of the Department of Defense, and is staffed by a combination of civilian and military personnel.

.NSA has an extensive customer outreach system, with representatives in many intelligence customer organizations in the Washington, DC, area, in other parts of the U.S., and around the world. NSA's headquarters is at Fort Meade, Maryland.

The **Signals Intelligence Directorate** is responsible for understanding customers' intelligence information needs, and for the collection, analysis and production, and dissemination of Signals Intelligence (SIGINT).

Operating under the authority of the Secretary of Defense, the **Information Assurance Directorate** ensures the availability, integrity, authentication, confidentiality, and non-repudiation of national security and telecommunications and information systems (national security systems).

The **Central Security Service (CSS)** oversees the function of the military cryptologic system, develops policy and guidance on the contributions of military cryptology to the Signals Intelligence / Information Security (SIGINT/INFOSEC) enterprise, and manages the partnership of NSA and the Service Cryptologic Components. NSA as a whole is known as "NSA/CSS."

The **NSA/CSS Threat Operations Center** monitors the operations of the global network to identify network-based threats and protect U.S. and allied networks.

The **National Security Operations Center** is a 24 hours a day/7 days a week operations center that, on behalf of the NSA/CSS, provides total situational awareness across the NSA/CSS enterprise for both foreign Signals Intelligence and Information Assurance, maintains cognizance of national security information needs, and monitors unfolding world events.

The **Research Directorate** conducts research on signals intelligence and on information assurance for the U.S. Government.

Department of Justice
Drug Enforcement Administration
Office of National Security Intelligence

The Drug Enforcement Administration (DEA) is responsible for enforcing the controlled substance laws and regulations of the U.S. It brings to the criminal and civil justice system of the U.S., or any other competent jurisdiction, those organizations and the principal members of those organizations, involved in the growing, manufacturing, or distribution of controlled substances appearing in or destined for illicit traffic in the U.S. In addition, DEA recommends and supports non-enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets.

DEA has 21 field divisions in the U.S. and more than 80 offices in over 60 countries worldwide.

DEA's **Office of National Security Intelligence (ONSI)** became a member of the IC in 2006. Located at DEA Headquarters in Arlington, Virginia, ONSI facilitates full and appropriate intelligence coordination and information sharing with other members of the U.S. Intelligence Community and homeland security elements. ONSI leverages the global law enforcement drug intelligence assets of DEA to report on matters relating to national security. Its goal is to enhance U.S. efforts to protect national security, and combat global terrorism, as well as facilitate IC support to DEA's law enforcement mission.

Department of Energy
Office of Intelligence and Counterintelligence

The Department of Energy's (DoE) Office of Intelligence is the Intelligence Community's premier technical intelligence resource in four core areas: nuclear weapons and nonproliferation; energy security; science and technology; and nuclear energy, safety, and waste. Tapping the broad technology base of DoE's national laboratories and the international reach of the DoE complex as a whole, the Office of Intelligence accomplishes a three-part mission:

- To provide DoE, other U.S. Government policymakers, and the Intelligence Community with timely, accurate, high-impact foreign intelligence analyses.
- To ensure that DoE's technical, analytical, and research expertise is made available to the intelligence, law enforcement, and special operations communities.
- To provide quick-turnaround, specialized technology applications and operational support based on DoE technological expertise to the intelligence, law enforcement, and special operations communities.

DoE's intelligence program traces its origins to the days of the Manhattan Project, when the former Atomic Energy Commission (AEC) was tasked to provide specialized analysis of the nascent atomic weapons program of the Soviet Union. Since then, that program--like the functions of the old AEC—has come to reside within DoE. It continues to evolve in close concert with changing policy needs and the strengths of DoE's unique scientific and technological base, from the world energy crisis of the 1970s, and consequent demand for intelligence expertise in international energy supply and demand issues, to growing concerns over nuclear proliferation and energy security in this decade.

Department of Homeland Security
Office of Intelligence & Analysis

The Department of Homeland Security (DHS) is responsible for leading the unified national effort to secure the United States by preventing and deterring terrorist attacks and responding to threats and hazards.

The **Office of Intelligence and Analysis (I&A)** is DHS's headquarters intelligence element and is led by the Under Secretary for Intelligence and Analysis, with guidance from the Homeland Security Council and Homeland Security Intelligence Council. As a member of the IC, I&A is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States. The Office of Intelligence and Analysis provides actionable intelligence to support national and DHS decision-makers while working closely with state, local, tribal, and private sector partners. The Office of Intelligence and Analysis focuses on threats related to border security; chemical, biological, radiological, and nuclear issues, to include explosives and infectious diseases; critical infrastructure protection; extremists within the homeland; and travelers entering the homeland.

Although they are not part of the Intelligence Community, several of DHS's other subcomponents have extensive interactions with the Intelligence Community, including U.S. Immigration and Customs Enforcement, Customs and Border Protection, Transportation Security Administration, Secret Service, and Citizenship and Immigration Services.

Department of State
Bureau of Intelligence and Research

The Bureau of Intelligence and Research (INR) provides expert intelligence analysis to the Secretary of State and senior policymakers, giving them "decision advantage" as they seek to protect and advance American interests around the world. INR serves as the focal point within the Department of State for all policy issues and activities involving the Intelligence Community. The INR Assistant Secretary reports directly to the Secretary of State and serves as the Secretary's principal adviser on all intelligence matters.

INR's expert, independent foreign affairs analysts draw on all-source intelligence, diplomatic reporting, INR's public opinion polling, and interaction with U.S. and foreign scholars. Their strong regional and functional backgrounds allow them to respond rapidly to changing policy priorities and to provide early warning and in-depth analysis of events and trends that affect U.S. foreign policy and national security interests. INR analysts – a combination of Foreign Service officers often with extensive in-country experience and Civil Service specialists with in-depth expertise – cover all countries and regional or transnational issues.

The Bureau provides daily briefings, reports, and memoranda to the Secretary and other Department principals. INR also briefs members of Congress and their staffs as appropriate. INR products cover the globe on foreign relations issues such as political/military developments, terrorism, narcotics, and trade. INR contributes to the Community's National Intelligence Estimates, the Presidential Daily Brief and other analyses, offering its particular focus on relevance to policy. In support of the statutory authority of the Secretary of State and Chiefs of Mission for the conduct of foreign policy and oversight of U.S. Government activities overseas, INR coordinates on behalf of the Department on issues concerning intelligence, counterintelligence, and special operations. INR participates in a wide variety of Intelligence Community working groups and policymaking committees, including those involving visa denial, intelligence sharing, analytic production, requirements and evaluation for collection in all intelligence disciplines.

INR develops intelligence policy for the Department of State and works to harmonize all agencies' intelligence activities abroad with U.S. policy. Acting to ensure that collection resources and priorities accord with U.S. diplomatic interests and requirements, INR engages Chiefs of Mission, Department resource managers, and the Intelligence Community for this purpose.

In addition to all-source analysis and intelligence policy coordination, INR's third core activity is to serve as the DNI's recently named Executive Agent for Outreach. In this role, INR leverages community resources to tap into the expertise of academia, think tanks, research councils, non-governmental organizations, and the private sector to expand the universe of knowledge available to policymakers and the intelligence community. INR also analyzes geographical and international boundary issues. **Its Humanitarian Information Unit (HIU)** serves as a nucleus for unclassified information related to complex emergencies and provides a coordinating mechanism for data sharing among the U.S. Government, the UN, non-governmental organizations, and foreign governments. The Bureau also administers the Title VIII Grant Program, an initiative funded by Congress for senior level academic research in Russian, Eurasian and East European studies.

Department of the Treasury
Office of Intelligence and Analysis

The Office of Intelligence and Analysis (OIA) was established by the Intelligence Authorization Act for fiscal year 2004. The Act specifies that OIA shall be responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of the **Department of the Treasury.**

OIA's strategic priorities:

- *Terrorist Financing*: Over the past several years, the terrorist threat has become far more decentralized in nature, and many terrorist groups affiliated with al Qa'ida now pose a serious threat to U.S. national security.
- *Insurgency Financing*: OIA will continue to improve its understanding of the insurgency financing, primarily through the Baghdad-based Iraq Threat Finance Cell (ITFC) for which Treasury serves as co-lead with the Department of Defense.
- *Rogue Regimes/Proliferation Financing*: OIA has assumed an increasingly important role in Treasury's effort to combat other national security threats, including rogue regimes involved in WMD proliferation. OIA will continue to build on its efforts in these critical areas.

United States Army

The Department of the Army's IC component is **Army Military Intelligence (Army MI). The Deputy Chief of Staff (DCS),** G-2 is the Army Staff Principal responsible for Army MI. The mission of the DCS G-2 is to formulate Army intelligence policy, plans, programs, and budgets and is responsible for Army-level oversight of multidisciplined intelligence operations, intelligence support to Computer Network Operations, MI personnel, training, readiness and equipping (with the DCS, G-8), security, foreign liaison and future threats. The DCS G-2 plans and executes the Army Intelligence Campaign Plan in support of Army transformation, enabling effective all-source intelligence at Brigade Combat Team, Battalion, and Company levels, as well as other tactical Army organizations and activities.

The **vision of the DCS** G-2 is to transform Army intelligence capabilities to enable decisive action by Army and Joint Commanders in an era of persistent conflict, complex environments, and asymmetric challenges; integrate advanced fusion and "find, fix, finish, exploit, analyze and disseminate" capabilities into Battle Command processes; and holistically adapt how we equip, train, share information, grow leaders and improve reasoning skills to generate actionable intelligence at the lowest possible level.

The Army's operational-level intelligence organization is the **U.S. Army Intelligence and Security Command (INSCOM)** located at Fort Belvoir, Virginia.

The Army's principal intelligence training organization is the **U.S. Army Intelligence Center (USAIC)** located at Fort Huachuca, Arizona. The USAIC reports to the U.S. Army Training and Doctrine Command.

The Army's **Military Intelligence Readiness Command (MIRC)** is responsible for overseeing Army Reserve intelligence activities and is co-located with INSCOM at Fort Belvoir, Virginia. The MIRC reports to the U.S. Army Reserve Command.

The National Ground Intelligence Center (NGIC) provides the Army with military, scientific and technical intelligence. The NGIC is located in Charlottesville, Virginia, and reports to INSCOM.

Army MI efforts are fully integrated with the Army Campaign Plan and focused on six key initiatives:

- Increasing MI Capacity and Advanced Skills Readiness
- Growing Army Human Intelligence (HUMINT) Capabilities
- Force-wide Employment of Distributed Common Ground System-Army
- Increasing Capacity of Army Cyberspace Operations
- Expanding Persistent Surveillance & Exploitation Capabilities
- Changing the Culture.

United States Navy

Naval Intelligence is the oldest continuous serving U.S. intelligence service, established on March 23, 1882. Its mission today is to enable decision superiority for Navy commanders and operational forces by harmonizing intelligence and information operations efforts, and by achieving a penetrating knowledge of adversaries and a profound understanding of the maritime environment.

The Director of Naval Intelligence, located in the Pentagon, is responsible for the oversight, planning, programming, strategy and policy of all Navy Intelligence organizations and activities. The Navy's lead intelligence center, the **Office of Naval Intelligence (ONI)**, is headquartered at the **National Maritime Intelligence Center (NMIC)** in Suitland, Maryland. ONI is a major IC production center for maritime intelligence, analyzing and producing assessments of foreign naval capabilities, trends, operations and tactics, global civil maritime activity, and an extensive array of all-source analytical products.

Naval Intelligence supports Joint Military Operations through embedded personnel in operational units or Expeditionary Intelligence teams. Naval Intelligence also provides a maritime intelligence reach-back capability from ONI and an emerging network of Fleet intelligence centers, as well as Joint Task Force and Combatant Command Joint Intelligence Operations Centers.

United States Air Force

The Headquarters Air Force A2 is the **Deputy Chief of Staff of the Air Force for Intelligence, Surveillance and Reconnaissance (ISR)**. He or she provides policy, oversight, and guidance to all Air Force intelligence organizations.

The Air Force Intelligence, Surveillance and Reconnaissance Agency (AF ISR Agency), with headquarters at Lackland Air Force Base, Texas, was activated on June 8, 2007. Formerly, the Air Intelligence Agency, the Air Force ISR Agency is aligned under the Air Force Deputy Chief of Staff for ISR as a Field Operating Agency.

The Agency's mission is to organize, train, equip and present assigned forces and capabilities to conduct ISR for Combatant Commanders and the Nation. It implements and oversees the execution of Air Force headquarters policy and guidance to expand Air Force ISR capabilities to meet current and future challenges. The Agency's 14,500 assigned personnel serve at 70 locations worldwide including **the 70th Intelligence Wing** at Ft. Meade, Maryland, and the **National Air and Space Intelligence Center (NASIC)** at Wright-Patterson AFB, Ohio. The AF ISR Agency commander serves as the Service Cryptologic Component under NSA, and oversees Air Force Signals Intelligence activities.

United States Marine Corps

The U.S. Marine Corps (USMC) produces tactical and operational intelligence for tactical and operational commanders and their staffs, as well as for other customers. Its IC component is comprised of all intelligence professionals in the Marine Corps. Most Marine Corps intelligence professionals are integrated into operating forces at all echelons of command from battalion/squadron to Marine Expeditionary Force.

The Marine Corps' **Director of Intelligence (DIRINT)** is its principal intelligence staff officer and is the service's functional manager for intelligence, counterintelligence, and cryptologic matters.

Marine Corps Intelligence Activity (MCIA), Quantico, Virginia, is the Marine Corps' service production center. In addition, MCIA supports other services and government organizations as appropriate. It provides the Marine Corps with intelligence for planning, training, operations, systems development, and exercises. MCIA can be tasked to provide expeditionary warfare intelligence to support any national, theater, or operational command in the U.S. Armed Forces. MCIA's analysis and production supports not only the Marine Corps, but also the national decision-maker, theater commander, and tactical warfighter.

Department of Homeland Security
United States Coast Guard

The United States Coast Guard is a military, multi-mission, maritime service within the Department of Homeland Security. The Coast Guard is one of the Nation's five armed services. A unique blend of humanitarian, law enforcement, regulatory, diplomatic, Intelligence Community, and military capabilities encompasses the five fundamental Coast Guard roles: maritime security, maritime safety, protection of natural resources, maritime mobility and national defense. It performs those missions in any maritime region in which those interests may be at risk, including international waters and America's coasts, ports, and inland waterways. To assist in accomplishing the many diverse missions of the Coast Guard, senior leadership and operational commanders rely on the **Coast Guard Intelligence and Criminal Investigations Program**.

Because the Coast Guard employs unique expertise and capabilities in the maritime environment – in domestic ports, coastal waters, offshore regions, and even in foreign ports – where other U.S. Government agencies typically are not present, there exists the opportunity to collect intelligence that supports not only Coast Guard missions, but other national security objectives, as well.

The Coast Guard's **Intelligence and Criminal Investigations Program** includes its National Intelligence Element, the Criminal Investigations Service, the Counterintelligence Service, the Intelligence Coordination Center (the Coast Guard's production center) and the Cryptologic Service. Its mission is to direct, coordinate, and oversee intelligence and investigative operations and activities that support all Coast Guard objectives by providing actionable (timely, accurate, and relevant) intelligence to strategic decision-makers, as well as operational and tactical commanders. The Coast Guard Intelligence and Criminal Investigations Enterprise also supports the National Strategy for Homeland Security and applicable National Security objectives.

The Coast Guard has fully implemented rigorous policies and procedures to ensure compliance with the mandatory information sharing provisions of Section 905(a) of the USA PATRIOT Act and Section 202 of the Homeland Security Act. It continues to capture and share law enforcement information that is relevant to homeland security and national security with the Department of Homeland Security, Intelligence and Analysis Directorate and the Intelligence Community, where appropriate.

Support to Coast Guard operations are also bolstered with the following intelligence and law enforcement activities:

- Coast Guard Area Maritime Intelligence Fusion Centers (Pacific and Atlantic);
- Sector Intelligence Officers at 26 Coast Guard Sectors;
- Field Intelligence Support Offices at Coast Guard Sectors;
- COASTWATCH and Targeting Programs`at the ICC;
- Global Maritime Intelligence Integration capability (partnering with the U.S. Navy and other key Intelligence Community members);
- Permanent presence on the FBI's National Joint Terrorism Task Force (JTTFs) Offices and ad hoc JTTFs providing a maritime nexus and expertise;
- Expanded participation in the Defense Attaché System that provides unique access to non-traditional foreign partners;
- National Tactical Integration Office – a TENCAP-like program that has increased the Coast Guard's maritime awareness in areas including fusion, identification of ships with imagery, anomaly detection and information sharing;
- Operation Drydock, an interagency operation reviewing personnel holding Coast Guard-issued merchant mariner licenses and documents; and
- Project Scorpion, a national-level collaborative effort with the Departments of Justice, Defense and Homeland Security to identify, track and intercept aliens of interest with possible terrorist or affiliate ties before they arrive in the United States via maritime means.

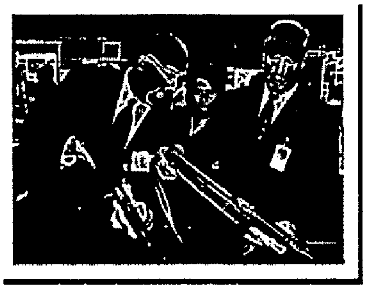
Intelligence Community Legislative Affairs Points of Contact

	Telephone	Fax
Office of the Director of National Intelligence Office of Legislative Affairs	(703) 275-2474	(703) 275-1279
Central Intelligence Agency Office of Congressional Affairs	(703) 482-4151	(703) 482-0672
Defense Intelligence Agency Congressional Affairs Staff	(703) 697-0012	(703) 697-3687
Federal Bureau of Investigation Congressional Affairs	(202) 324-4510	(202) 324-6490
National Geospatial-Intelligence Agency Congressional Affairs Office	(301) 227-7392	(301) 227-7638
National Reconnaissance Office Congressional and Public Affairs	(703) 808-1105	(703) 808-1109
National Security Agency Legislative Affairs Office	(301) 688-7246	(443) 479-2888
Drug Enforcement Administration Congressional Affairs	(202) 307-7423	(202) 307-5512
Department of Energy Office of Congressional and Intergovernmental Affairs	(202) 586-5450	(202) 586-4891
Department of Homeland Security Intelligence and Analysis Legislative Affairs	(202) 447-5439	(202) 772-9734
Department of State Bureau of Intelligence and Research	(202) 647-2921	(202) 647-2285
Department of the Treasury Intelligence Support	(202) 622-1900	(202) 622-0534
U.S. Army Intelligence Legislative Liaison	(703) 695-3918	(703) 614-7599
U.S. Navy Intelligence Legislative Liaison	(703) 695-4156	(703) 693-0656
U.S. Air Force Intelligence Legislative Liaison	(703) 693-9125	(703) 697-8623
U.S. Marine Corps Intelligence Legislative Liaison	(703) 614-2522	(703) 614-5888
U.S. Coast Guard Intelligence Legislative Liaison	(202) 372-2700	(202) 372-2973

23. Directorate Information

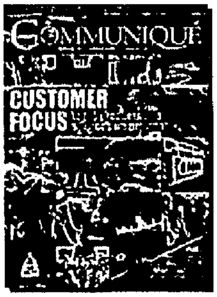
Office for Congressional and Public Affairs

*Our mission is to manage **strategic communications** by representing DIA and its capabilities to Congress, the Public, Senior IC, DoD, and U.S. Government Officials as well as to the DIA workforce.*



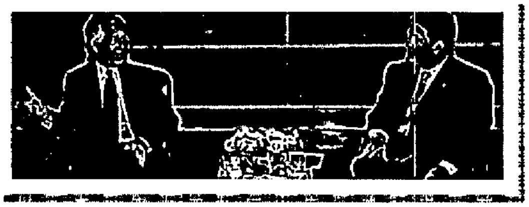
Congressional Affairs

Serves as the single focal point for DIA interaction with Congress.



Public Affairs - Internal Communications

Produces the Communiqué, the Agency's command information magazine and the InterComm, our classified newsletter, manages the internal communications website and facilitates communication with the widely dispersed DIA workforce.

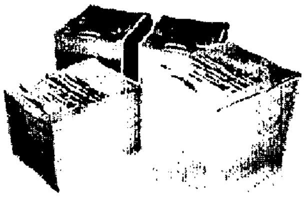


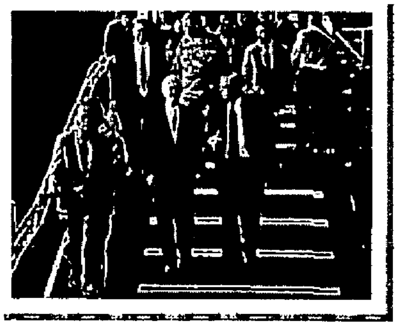
Public Affairs - External Communications

Plans, coordinates and monitors all DIA interaction with the media and the general public to include management of the unclassified website at www.dia.mil.

Prepublication (Security and Policy) Review

Conducts the Agency's prepublication review process for unclassified information prepared and intended for public release.





Outreach Program

Develops, plans, and executes all DIA outreach programs, visits, and orientations with VIPs and other US personnel.

Strategic Engagement

Develops plans that foster strategic relationships with the agency's overseers, stakeholders and customers.

Protect. Educate. Preserve.

DIA EO

Equal Opportunity and Diversity Services

Bolling Air Force Base | 200 MacDill Boulevard | Washington, DC 20340-5100

Director's Committment

DIA is committed to the principles of fair and equal employment opportunity. Unlawful discrimination of any kind is prohibited.

Our vision of a discrimination-free work environment is characterized by an atmosphere of inclusion and free, open competition for employment opportunities. We will work together to establish and sustain the infrastructure necessary to achieve this vision.

Who May File an EO Complaint: Civilians and Military

Civilian employees, former employees, or applicants for employment who believe that they have been discriminated against because of **race, color, national origin, religion, sex, age, disability,** or **reprisal** in an employment matter subject to the control of DIA may initiate the EO complaint process. Contact **must** be made within:

- **45 calendar days** from the date of the discriminatory event or personnel action.
- **45 calendar days** from the date the individual became aware or reasonably should have known of the discriminatory event or personnel action.

Military personnel who believe that they have been subjected to unlawful discrimination based on their **race, color, gender, religion,** or **national origin** may use either of the following options to file a discrimination complaint:

- **File an informal discrimination complaint** in accordance with DIA Regulation 27-3 or the respective service's discrimination complaint process.
- **File a formal discrimination complaint within 60 calendar days** from the alleged discriminatory event in accordance with DIA Regulation 27-3 or the respective service's discrimination complaint process.

Where to File

You must bring the matter to the attention of the EO Office. Contact can be made via:

- **The EO Hotline:** [redacted] (b)(3):10 USC 424
- **Deployed Hotline (24-hour watch):** [redacted]
- **MSIC EO Support Branch:** [redacted]
- **Sign Language Interpreting Services:** [redacted] at "EO Interpreting Services (Signed)" [redacted]
- **Secure Telephone:** [redacted] (b)(3):10 USC 424
- **Personal Visit to the EO Office on Bolling Air Force Base:** DIAC
- **The EO Website:** (JWICS & SIPERNET)
- **Unsecure facsimile:** [redacted]

Additional information can be aquired by contacting [redacted] (b)(3):10 USC 424

Alternative Dispute Resolution (ADR)

ADR is offered as a means to quickly resolve all workplace disputes at the lowest possible level. Mediation is DIA's preferred method of ADR. Additional information can be acquired by contacting [redacted] (b)(3):10 USC 424

Reasonable Accommodations

In accordance with the Rehabilitation Act of 1973, as amended, the **Reasonable Accommodation Program** is available to employees with qualified disabilities. Contact the **Reasonable Accommodations Counselor** at [redacted] (b)(3):10 USC 424

Special Emphasis Programs (SEPs) are managed by the Equal Opportunity and Diversity Services Office; a list of these programs can be found on the EO website.

For more information, access the EO website or call [redacted] (b)(3):10 USC 424

Protect. Educate. Preserve.

DIA EO

HAVE NO FEAR

NO FEAR ACT NOTICE

(Notification and Federal Employees
Antidiscrimination and Retaliation Act)

On May 15, 2002, Congress enacted the "Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002," which is now known as the No FEAR Act. One purpose of the Act is to "require that Federal agencies be accountable for violations of antidiscrimination and whistleblower protection laws." Public Law 107-174, Summary. In support of this purpose, Congress found that "agencies can not be run effectively if those agencies practice or tolerate discrimination." Public Law 107-174, Title I, General Provisions, section 101(1).

The Act also requires this agency to provide this notice to Federal employees, former Federal employees and applicants for Federal employment to inform you of the rights and protections available to you under Federal antidiscrimination and whistleblower protection laws.

Antidiscrimination Laws

A Federal agency cannot discriminate against an employee or applicant with respect to the terms, conditions or privileges of employment on the basis of race, color, religion, sex, national origin, age, disability, marital status, or political affiliation. Discrimination on these bases is prohibited by one or more of the following statutes: 5 U.S.C. 2302(b)(1), 29 U.S.C. 206(d), 29 U.S.C. 631, 29 U.S.C. 633a, 29 U.S.C. 791 and 42 U.S.C. 2000e-16. Other types of discrimination not listed above, including but not limited to, sexual orientation, genetics, and pregnancy discrimination, are also prohibited.

If you believe that you have been the victim of unlawful discrimination on the basis of race, color, religion, sex, national origin or disability, you must contact an Equal Employment Opportunity (EEO) counselor within 45 calendar days of the alleged discriminatory action, or, in the case of a personnel action, within 45 calendar days of the effective date of the action, before you can file a formal complaint of discrimination with your agency. See, e.g., 29 CFR part 1614. If you believe that you have been the victim of unlawful discrimination on the basis of age, you must either contact an EEO counselor as noted above or give notice of intent to sue to the Equal Employment Opportunity Commission (EEOC) within 180 calendar days of the alleged discriminatory action. If you are alleging discrimination based on marital status, sexual orientation, parental status or political affiliation, you may contact the EO office, IG office, or HC for further assistance.

Whistleblower Protection Laws

A Federal employee with authority to take, direct others to take, recommend or approve any personnel action must not use that authority to take or fail to take, or threaten to take or fail to take, a personnel action against an employee or applicant because of disclosure of information by that individual that is reasonably believed to evidence violations of law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety, unless disclosure of such information is specifically prohibited by law and such information is specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.

Retaliation against an employee or applicant for making a protected disclosure is prohibited by 5 U.S.C. 2302(b)(8). If you believe that you have been the victim of whistleblower retaliation, you may file a written complaint with the Inspector General's (IG) office.

Retaliation for Engaging in Protected Activity

A Federal agency cannot retaliate against an employee or applicant because that individual exercises his or her rights under any of the Federal antidiscrimination or whistleblower protection laws listed above. If you believe that you are the victim of retaliation for engaging in protected activity, you must follow, as appropriate, the procedures described in the Antidiscrimination Laws and Whistleblower Protection Laws sections of this Notice, or, if applicable, the administrative procedures, in order to pursue any legal remedy.

[illegible]

Under the existing laws, each agency retains the right, where appropriate, to discipline a Federal employee for discriminatory or retaliatory conduct, or other conduct that is inconsistent with Federal antidiscrimination, whistleblower protection, and retaliation laws. Possible disciplinary actions range up to and include removal. Nothing in the No FEAR Act alters existing laws or permits an agency to take unfounded disciplinary action against a Federal employee or to violate the procedural rights of a Federal employee who has been accused of discrimination.

Additional Information

For further information regarding the No FEAR Act regulations, refer to 5 CFR part 724, as well as the points of contact listed. Additional information regarding Federal antidiscrimination, whistleblower protection and retaliation laws can be found at the EEOC Web site, http://www.eeoc.gov, and the OSC Web site, http://www.osc.gov.

Existing Rights Unchanged

Pursuant to section 205 of the NoFEAR Act, neither the Act nor this notice creates, expands or reduces any rights otherwise available to any employee, former employee or applicant under the laws of the United States, including the provisions of law specified in 5 U.S.C. 2302(d).

[illegible]

For Whistle Blower issues, contact the IG at [redacted]

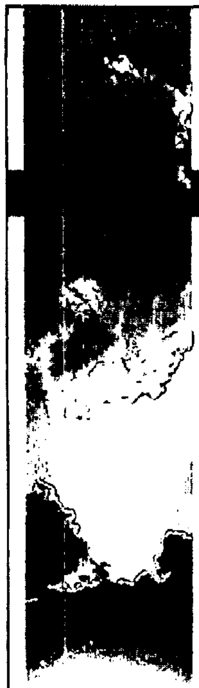
For administrative grievances, contact [redacted]

For discrimination, contact the EO Office at:

- The EO Hotline: [redacted]
  o [redacted]
- Deployed Hotline (24-hour watch): [redacted]
- MSIC EO Support Branch: [redacted]
- Sign Language Interpreting Services: [redacted] at "EO Interpreting Services (Signed)" [redacted]
- Secure Telephone [redacted]
- Personal Visit to the EO Office on Bolling Air Force Base: DIAC
- The EO Website: (JWICS & SIPERNET)
- Unsecure facsimile: [redacted] [redacted]

Additional information can be acquired by contacting [redacted] [redacted]

(b)(3):10 USC 424



Committed to protecting, educating,
and preserving DIA's workforce
one person at a time.

Protect. Educate. Preserve.

DIA EO

Equal Opportunity & Diversity Office (EO)

Mission Statement

The Equal Opportunity & Diversity mission is to support and enhance DIA's commitment to diversity, equality of opportunity and the creation of an optimal work environment. EO staff provides insight, direction and guidance to DIA decision makers in their efforts to recruit and retain a diverse workforce and ensure an environment free from discrimination and harassment.

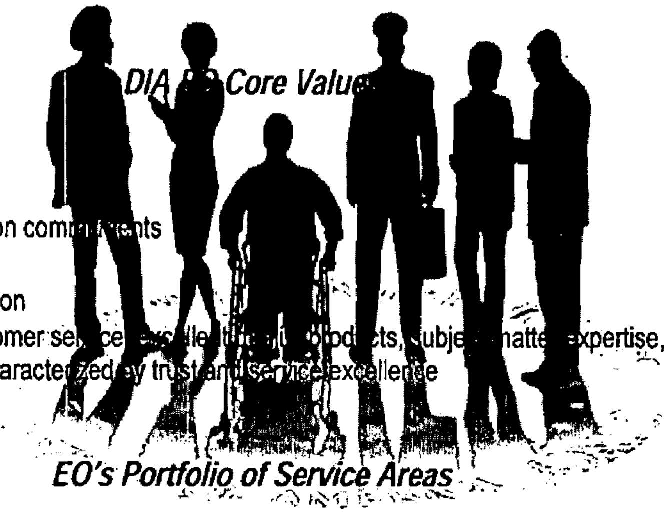
DIA EO Commitment

The men and women of the Equal Opportunity and Diversity Office are committed to:

1. Protect the civil rights of DIA employees and applicants.
2. Educate the workforce on their rights and responsibilities; to value individual differences and appreciate how diversity enhances DIA's capabilities.
3. Preserve employee trust in the integrity and fairness of DIA's employment policies and programs.

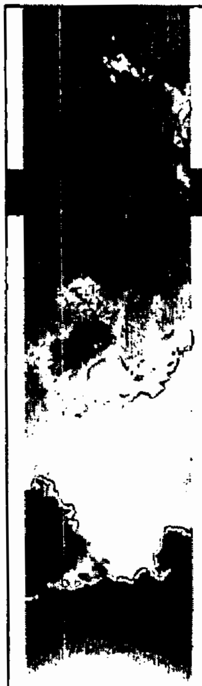
DIA EO Core Values

- Responsive
- Respect
- Follow through on commitments
- Confidentiality
- Conflict Resolution
- Exemplary customer service, excellent quality products, subject matter expertise, enduring relationships characterized by trust and service excellence



EO's Portfolio of Service Areas

- Communications, Outreach and Operational Support
- Compliance and Oversight
- Workplace Development
- Disability Management
- Education
- Sign Language Interpreting
- Complaints Adjudication
- Military Equal Opportunity (MEO) Program
- Conflict Management



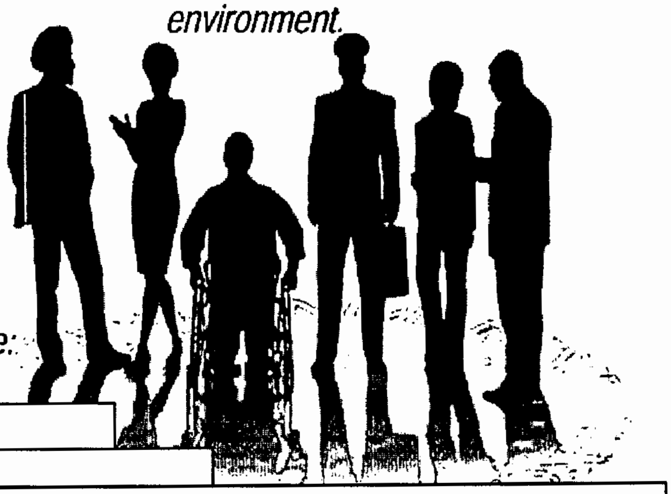
Committed to protecting, educating,
and preserving DIA's workforce
one person at a time.

Protect. Educate. Preserve.

DIA EO

DIA EO Staff

We are proud of our EO staff. As professionals, we are committed to the principles of equal opportunity and are experts in federal EEO laws and procedures. We are always open to all points of view and are dedicated to helping DIA employees and managers create a fair and effective work environment.



Our executives are:

[redacted]

(b)(3):10 USC 424

Contact Information

- **EO Main Office Line:** [redacted]
- **EO Hotline:** [redacted]
- **Deployed Hotline (24-hour watch):** [redacted]
- **MSIC EO Support Branch:** [redacted]
- Sign Language Interpreting Services: [redacted] at “EO Interpreting Services (Signed)” [redacted]
- **Secure Telephone:** [redacted]

(b)(3):10 USC 424

Directorate for Information Management and CIO (DS)

[redacted]

(b)(3):10 USC 424

Directorate for Information Management and CIO Mission:

To provide a secure, standardized, and integrated global IT enterprise that is continuously improved and maintained in response to customer needs and enables collaborative discovery, synthesis, and delivery of critical intelligence to warfighters, defense planners, national-security policy makers, and international partners.

(b)(3):10 USC 424

[redacted]

IA Mailbox: [redacted] (b)(3):10 USC 424

JWICS Webpage:

[redacted]

(b)(3):10 USC 424

Office of the Inspector General

The Office of the Inspector General (OIG) performs an independent oversight role to assist agency and intelligence enterprise senior management by identifying recommendations to enhance performance, improve accountability, and deter fraud, waste, or abuse.

The OIG performs audits, criminal and administrative investigations, inspections, intelligence oversight inspections and investigations, and workforce assistance.

The OIG has offices in the DIAC and a regional office located in [redacted] (b)(3):10 USC 424

Contact	HQ Office	Regional Office
Hotline	202-231-1000	[redacted]
Commercial	202-231-1010	[redacted]
Class Fax	[redacted]	[redacted]
Unclas Fax	[redacted]	[redacted]
DSN	[redacted]	[redacted]
JWICS	[redacted]	[redacted]
SIPRNet	[redacted]	[redacted]
NIPRNet	IG_Hotline@dia.mil	[redacted]

[redacted]

(b)(3):10 USC 424

Joint Intelligence Virtual University

Delivering Knowledge to the Desktop

WHO ARE WE? JIVU is the premier online learning and knowledge management system, providing the Intelligence Community agencies, combatant commands, and military services with easy access to high-quality e-Learning products, tools, and services in a collaborative online training environment.

WHAT DO WE DO? JIVU is emerging as the central repository for learning throughout the Intelligence Community. You have access to course catalogs from IC member agencies and the COCOMs, bringing valuable knowledge from around the globe to your fingertips!

WHAT DO WE OFFER? JIVU offers *flexibility!* Many courses taught in traditional classroom settings have been adapted to online learning, providing you the flexibility to learn using the modality that best suits your learning style.

We provide you access to more than 4,000 self-paced online courses covering such subject areas as acquisition, foreign languages, intelligence analysis, intelligence collection, intelligence production, and much more.

We also offer live, interactive classes through our Virtual Classroom (V-Class). Using state-of-the-art Voice over IP (VoIP) technology and a microphone-equipped headset, you can participate in fully interactive training sessions with faculty and colleagues located throughout the world right from your workstation. You can also review previously held training sessions through the use of the V-Class playback tool.

WHERE ARE WE? JIVU is accessible on JWICS and SIPRNet. NIPRNet access will be available soon!

JWICS

[redacted]

(b)(3):10 USC 424

SIPRNet

[redacted]

(b)(3):10 USC 424

HOW DO I GET STARTED? Open your web browser to your network's website shown above. Click the **New Users** box and follow the online instructions to create your account. It's that simple!

For further information, please call

[redacted]

(b)(3):10 USC 424

Brought to you by the Directorate for Human Capital – "All Source Intelligence Starts Here"

Directorate for Mission Services

We protect, project, and provide services to enable the DIA workforce to produce high quality intelligence to our Nation's military and intelligence community.

Directorate for Mission Services

(b)(3):10 USC 424

Protect

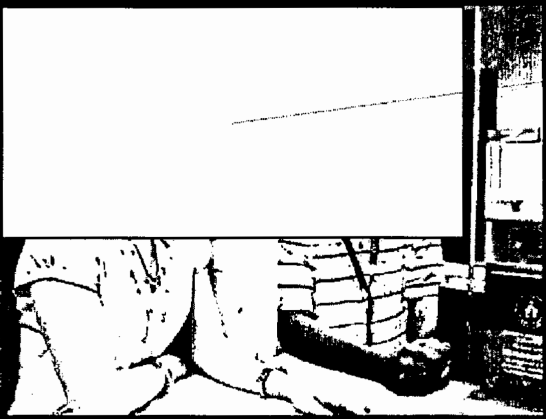
Project

Provide

[redacted]

Visit the DA website on JWICS at

[redacted]



[redacted]

(b)(3):10 USC 424, (b)(6)

(b)(3):10 USC 424

(b)(3):10 USC 424

[redacted]

(b)(3):10 USC 424

[redacted] *is here to assist DIA to protect people, property and information by providing the following services…*

(b)(3):10 USC 424

[redacted]

As a member of DIA you will experience the benefits of [redacted] *everyday—usually without even knowing it. Your primary* [redacted] *responsibilities are…*

(b)(3):10 USC 424

(b)(3):10 USC 424

*
*
*
[redacted]

* *Stay vigilant and immediately report any unusual or suspicious activity to local security officials*

For more information contact the [redacted]

[redacted]

(b)(3):10 USC 424

DIA Travel Training

DIA Travel Training provides DIA employees and their family members information to avoid and deal with the threats of terrorism, espionage, and other crimes while traveling.

Personnel are required to complete training within 90 days prior to travelling…

(b)(3):10 USC 424

[redacted]

(b)(3):10 USC 424

Please contact the [redacted] to or your local Security Official to identify training opportunities.

[redacted]

(b)(3):10 USC 424

Emergency Preparedness

[redacted] (b)(3):10 USC 424

Our mission is to sustain uninterrupted DIA operations by deterring, detecting, responding to, relocating and recovering from ALL HAZARDS

Directorate for Mission Services

Important Telephone Numbers

Facility Emergency Numbers

[redacted] (b)(3):10 USC 424

Useful Emergency Preparedness Websites

Homeland Security
www.ready.gov

American Red Cross
www.redcross.org

Centers for Disease Control
And Prevention
www.bt.cdc.gov

Maryland Emergency
Management Agency
www.mema.state.md.gov

Virginia Department of
Emergency Management
www.vaemergency.gov

DC Homeland Security and
Emergency Management
hsema.dc.gov

How do I ...?

► Get out of the facility in an emergency?
Before an emergency occurs, ask your supervisor to show you the location of evacuation route diagrams and the published evacuation routes. Follow published evacuation routes.

► Know what items to take when evacuating the facility?
Take the appropriate emergency escape hood, your keys, ID (purse or wallet), coat or umbrella, if needed, any items you would need if you were not allowed to return to your work area before departing for the day (such as prescription drugs), and a bottle of water, if available.

► Know where to go in an emergency once I get out of the facility?
Proceed to your assigned assembly area.

► Know what to do when I get to my assembly area?
Report your presence in the assembly area to your supervisor or other person conducting accountability.

► Know what to do if I cannot reach my assembly area?
If you can't reach your assembly area, go to an available assembly area and report in to the assembly area commander. Inform him or her of your assigned assembly area and the fact that you cannot reach your assigned assembly area.

► Know what items to take with me when a shelter-in-place is initiated?
Take the appropriate emergency escape hood, your keys, ID, coat or umbrella, if needed, any items you would need if you were not allowed to return to your work area before departing for the day (such as prescription drugs), and a bottle of water, if available.

► Know when it is OK for me to return to my workstation or leave the building?
In an evacuation, remain in your assigned assembly area until told by your assembly area commander to do otherwise.

•Find out who my facility emergency representative is?
Go to the Employee Disaster Preparedness website or ask your supervisor or co-workers.

► Volunteer to be an emergency response warden, mobility impaired support team member or medical augmenter?
Contact your facility representative.

► Get an escape hood?
Contact your Activity Supply Coordinator or supervisor.

Find more info and contact us at:

[redacted]

(b)(3):10 USC 424

Emergency Preparedness

(b)(3):10 USC 424

[redacted]

Directorate for Mission Services

New Employee Emergency Response Plan Checklist

Purpose: To familiarize yourself with your facility's emergency response plan and your responsibility during an emergency.

(b)(3):10 USC 424

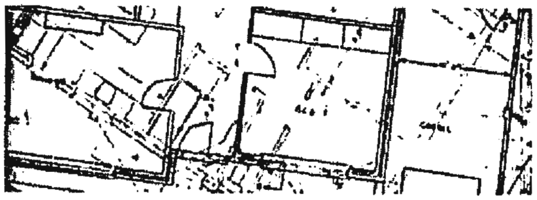
[redacted]

- **Fire Alarm Signaling Procedures**
  - Location of fire alarm stations and activation procedures
  - Audible and visual alarms
  - Actions to take during an alarm
- **Location of First Aid Kits**
  - Actions to take if you or others are injured
  - Location of medically trained personnel
  - Location of safety showers or eye wash stations if available, and how to use them
- **Personal Protective Equipment**
  - Escape hood issue
  - Location/storage of escape hood
  - Location of any other protective equipment
- **Reporting Emergencies**
  - How to report an emergency
  - Emergency telephone numbers
- **COOP Scenario**

(b)(3):10 USC 424

[redacted]

(b)(3):10 USC 424 [redacted]



"Mission FIRST Attitude"

Directorate for Mission Services

Provides high quality engineering and planning, facilities management, and project management for DIA at its worldwide locations. We also perform high quality projects and missions.

(b)(3):10 USC 424

[redacted] manages all major and minor construction projects for DIA. The branch coordinates the efforts of IT, furniture installation, security, movers, and customers.

(b)(3):10 USC 424

[redacted] provides architectural, interior design, electrical, mechanical engineering, and space planning expertise for facility maintenance and repair activity at primary DIA occupied facilities with the National Capital Region and MSIC.

(b)(3):10 USC 424

[redacted] provides a full range of Facility Management services on DIA-occupied facilities throughout the NCR, MSIC campus, and select Regional Service Centers. Initiates and tracks all customer and project work requests. Manages daily facility operations and preventative maintenance and repair activities on infrastructure, building systems, roads and grounds.

Go to our website via JWICS or Contact:

For additional information ⇨

[redacted]

(b)(3):10 USC 424

(b)(3):10 USC 424 [redacted]

"Safety is everybody's business"

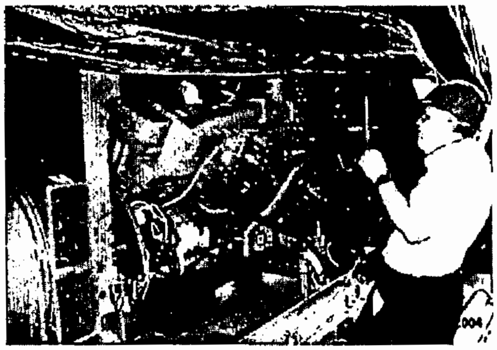
Directorate for Mission Services

Provide management and oversight of the Agency's [redacted] to provide a safe, secure, productive and supportive environment for all DIA employees and visitors.

(b)(3):10 USC 424

(b)(3):10 USC 424

[redacted] serves to assist, guide, and support the mission at all DIA organizational levels by reducing or eliminating the risk of accidents and regulatory non-compliance. [redacted] performs program management, education and training, facility inspections, and accident investigation.



[redacted] provides worldwide support to include the following: a program manager for DIA health services, manages maintenance of GFE Equipment, provides personal property management to include warehousing, and manages the day to day operation of the DoD Collaboration Center.

(b)(3):10 USC 424

Go to our website via JWICS or Contact:

For additional information

[redacted]

(b)(3):10 USC 424

Property Accountability and Management

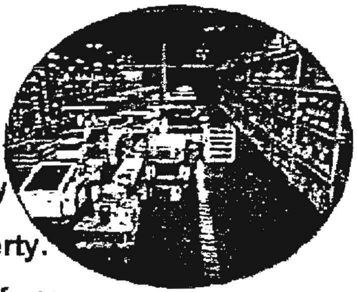
Property Accountability = the inherent responsibility to be answerable for the property that we hold in trust for the taxpayer.
Property Management = the process by which we account for assets...our policies, processes, and systems.

"Security is everyone's business - Property Accountability is too!"

DEFENSE INTELLIGENCE AGENCY · UNITED STATES OF AMERICA

Directorate for Mission Services

(b)(3):10 USC 424



Program Management → The [redacted] is the functional proponent for the Agency's Property Accountability program. They administer the policies, processes and property system for Government property.

Key Personnel → The Property Support Team consists of your Directorate's Accountable Property Officer (APO), Property Book Specialist (PBS), Hand Receipt Holder (HRH), and Activity Supply Coordinator (ASC). These individuals are available to assist with any property accountability questions or concerns.

Good Stewardship → **Always exercise reasonable and prudent actions to properly use, care for, and safeguard all Government property in your physical possession.**

Liability → You can be held liable for the loss, damage or destruction of Government property which can result in the loss of personal funds and adverse administrative actions, to include loss of security clearance and job.

Benefits of an effective Property Program →

- Meet ever-changing operational needs.
- Moves us toward clean audit opinion.
- Enables top decision makers to make better informed investments.

For additional information → Go to our website via JWICS or **Contact us**

[redacted]

(b)(3):10 USC 424

The next page is withheld in full and not provided.

The Do's of
Property Accountability and Management

"Security is everyone's business - Property Accountability is too!"

Directorate for Mission Services

The Do's of the [redacted]

(b)(3):10 USC 424

✓Manage accountable property throughout its lifecycle.

✓Establish accountable property systems of record; ensure integration with core financial systems.

✓Establish and implement property accountability directives and procedures.

✓Develop and maintain effective and meaningful performance measures.

✓Appoint and train Accountable Property Officers (APO) and Property Book Specialist (PBS).

✓Ensure all DIA employees are briefed annually on their obligation to properly use and safeguard property.

✓Provide formal property accountability training to DIA personnel to their level of functional responsibility.

The Do's of Supervisors

✓Know your Hand Receipt Holder (HRH), Activity Supply Coordinator (ASC), APO, and PBS.

✓Ensure your personnel perform their duties IAW DIAI 4000.0001.

✓Ensure the HRH/ASC attend training.

✓Allow personnel assigned as HRH/ASC time to perform duties.

✓Inform office personnel that the HRH/ASC are the individuals authorized to receive, turn-in, or transfer property in their area.

The Do's of all assigned personnel

✓ Use all Government property and equipment IAW its intended use.

✓Sign a sub-hand receipt for property in your possession as requested by the HRH.

✓Report any property discrepancies or movement of property to your HRH/ASC.

✓Fully understand that you are not authorized to move property from one location to another.

✓Know that you do not have to sign for property to be responsible.

✓ Know that loss, damage or destruction of property can result in the loss of funds and adverse administrative actions to include loss of security clearance and job.

The Do's of Hand Receipt Holders and Activity Supply Coordinators

✓Become familiar with DIAI 4000.0001 and complete all required property training.

✓Inventory property and sign an updated hand receipt annually.

✓Sub-hand receipt property to the lowest level (the User).

✓Meet periodically with your APO/PBS to discuss your account.

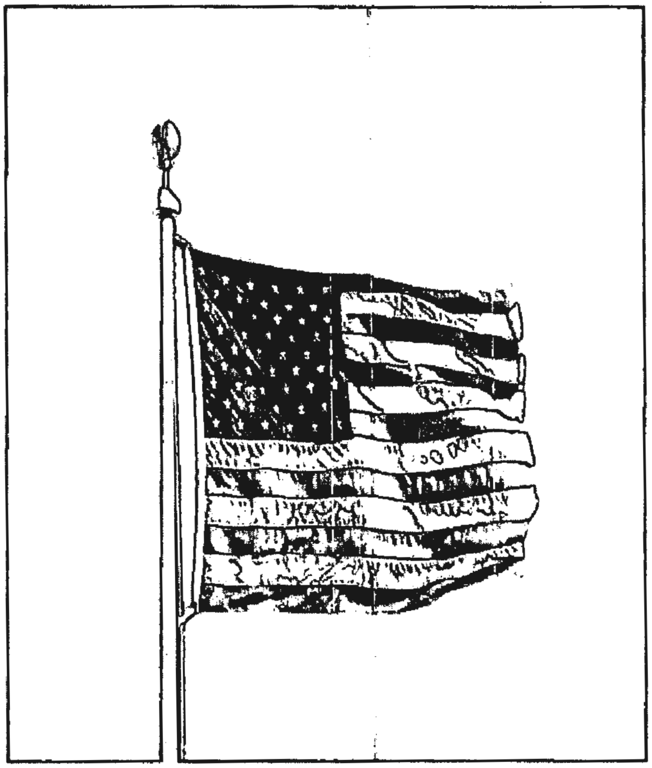
✓Immediately notify your first line supervisor and APO/PBS of any lost, damaged or destroyed property.

✓Ensure all transactions are entered into the Property Accountability System.

✓Establish required supporting document files.

Respect for the Flag.

Approximately 7:00am and 5:00pm each day, the flag is raised and lowered and the national anthem is played. Use the following procedures when showing respect to the flag and when the national anthem is being played:



All personnel in uniform and outside must face the flag and salute during the raising and lowering of the flag. Upon the first note of the national anthem or "To the Colors," all personnel in uniform who are not in formation should stand and face the flag (or the sound of the music if the flag is not visible) and salute. Hold the salute until the last note of the music is played.

All vehicles in motion should come to a stop at the first note of the music and the occupants should sit quietly until the music ends.

All civilian personnel, military in civilian clothes, should face the flag (or the sound of the music if the flag is not visible) and stand at attention with the right hand over the heart.

If indoors during retreat or reveille, there is no need to stand or salute. However, everyone must stand during the playing of the national anthem before a showing of a movie while in the base theater. When listening to a radio or watching television, no specific action is necessary. Additionally, a folded flag is considered cased; therefore, it is not necessary to salute or continue saluting.

DEFENSE INTELLIGENCE AGENCY
UNITED STATES OF AMERICA

THE DIA SEAL SYMBOLISM

The initial letters of the Defense Intelligence Agency (DIA) also comprise the Greek word "dia," which means divided into two parts. In this instance, the flaming torch and its gold color represent knowledge, i.e., intelligence, "lighting" the way of the "known" light blue-green world against the darkness or unknown symbolized by the dark background —"the area of the truth" still sought by the worldwide mission of the Agency. The two red atomic ellipses symbolize the scientific and technical aspects of intelligence today and of the future. The 13 stars and the wreath are adopted from the Department of Defense (DoD) seal and identifies the Agency as a DoD organization

Defense Intelligence Agency
[redacted] (b)(3):10 USC 424
200 MacDill Blvd., Bldg 6000
Washington, D.C. 20340-5100
[redacted]