



# CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

**Directive Current as of 16 May 11**

J-3

DISTRIBUTION: A, B, C, JS-LAN, S

CJCSM 1630.01

16 March 2009

## JOINT INFORMATION OPERATIONS FORCE

References: See Enclosure D.

1. Purpose. This manual provides operationalized guidance regarding the composition, education, and training requirements for the Joint Information Operations (IO) Force.
2. Cancellation. N/A.
3. Applicability. This manual applies to the Joint Staff, Services, combatant commands, Defense agencies, and other joint activities that will either provide or utilize members of the Joint IO Force.
4. Procedures. See Enclosure A.
5. Summary. This manual identifies the Military Occupational Specialties (MOSs), Air Force Specialty Codes (AFSCs), branches, functional areas (FAs), skill identifiers (SIs), and Navy Designators/Navy Enlisted Classifications from which the Joint IO Force is drawn, along with the specific education and/or training requirements necessary to serve in Joint IO billets. It also provides a force structure illustration that includes Joint IO Force education and training requirements (Enclosure B) and IO Graduate-Level Education Competencies (Enclosure C).
6. Releasability. This manual is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this manual through the Internet from the CJCS Directives Home Page--  
[http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives).

7. Effective Date. This manual is effective upon release.

For the Chairman of the Joint Chiefs of Staff:



STANLEY A. MCCHRYSTAL  
Lieutenant General, USA  
Director, Joint Staff

Enclosures:

- A -- Joint IO Force Policy
- B -- Joint IO Force Requirements
- C -- Joint IO Graduate-Level Education Competencies
- D -- References
- GL -- Glossary

DISTRIBUTION

Distribution A, B, C, and JS-LAN plus the following:

	<u>Copies</u>
Secretary of State.....	2
Secretary of Defense.....	2
Director of National Intelligence .....	2
Commandant, United States Coast Guard.....	2

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 2	O	C-1 thru C-2	O
i thru viii	O	D-1 thru D-2	O
A-1 thru A-10	O	GL-1 thru GL-4	O
B-1 thru B-2	O		

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

	Page
ENCLOSURE	
A -- JOINT IO FORCE POLICY .....	A-1
General .....	A-1
Commissioned Officers .....	A-3
Non-Commissioned Officers.....	A-9
B -- JOINT IO FORCES REQUIREMENTS .....	B-1
C -- JOINT IO GRADUATE LEVEL EDUCATION COMPETENCIES.....	C-1
D -- REFERENCES.....	D-1
GLOSSARY .....	GL-1
Part I -- Abbreviations and Acronyms .....	GL-1
Part II -- Terms and Definitions .....	GL-3
FIGURES	
A-1 Joint IO Force Structure (Commissioned Officer).....	A-3
A-2 Joint IO Force Structure (Commissioned Officer).....	A-4
A-3 Joint IO Force Structure (Commissioned Officer).....	A-6
A-4 Joint IO Force Structure (Commissioned Officer).....	A-6
A-5 Joint IO Force Timeline (Commissioned Officer) .....	A-7
A-6 Joint IO Force Structure (Commissioned Officer).....	A-8
A-7 Joint IO Force Structure (Commissioned Officer) .....	A-9

(INTENTIONALLY BLANK)



(INTENTIONALLY BLANK)

ENCLOSURE A

JOINT IO FORCE POLICY

1. General. The Joint Information Operations (IO) Force is drawn from commissioned officers in grades O-4 through O-9 and non-commissioned officers (NCO) in grades E-6 through E-9. Members of the Joint IO Force must have completed either the U.S. Joint Forces Command (USJFCOM) certified Joint IO Planning Course (JIOPC) or a USJFCOM certified Joint IO Core Capabilities Specialist Course and occupy an electronic Joint Manpower and Personnel Systems (eJMAPS) billet requiring Joint IO education and/or training. Service IO Military Occupational Specialties (MOSs) Air Force Specialty Codes (AFSCs), branches, functional areas (FA) skill identifiers (ASIs/SIs) or Navy designators/Navy Enlisted Classifications from which this Joint IO Force will be drawn include:

**ARMY BRANCHES/FA/SIs/PROJECT DEVELOPMENT SKILL IDENTIFIERS (PDSIs)**

**Commissioned Officers**

**FA 30** INFORMATION OPERATIONS  
**25A** SIGNALS GENERAL  
**35G** SIGNALS INTELLIGENCE/ELECTRONIC WARFARE  
**37A** PSYCHOLOGICAL OPERATIONS  
**FA 53** INFORMATION SYSTEMS MANAGEMENT  
**FA 59** STRATEGIC PLANS AND POLICY/**6Z** STRATEGIST  
**P4** TACTICAL INFORMATION OPERATIONS  
**H1B** OPERATIONS SECURITY (OPSEC) PRACTITIONER SPECIALIST  
**9N** COMPUTER NETWORK OPERATIONS PLANNER

**Warrant Officers**

**250N** NETWORK MANAGEMENT TECHNICIAN  
**251A** INFORMATION SYSTEMS TECHNICIAN  
**254A** SIGNALS SYSTEM SUPPORT TECHNICIAN  
**351L** COUNTERINTELLIGENCE TECHNICIAN  
**351M** HUMAN INTELLIGENCE COLLECTION TECHNICIAN  
**352S** NON-MORSE INTERCEPT TECHNICIAN  
**353T** INTELLIGENCE AND ELECTRONIC WARFARE (EW) TECHNICIAN

**Non-Commissioned Officers**

**25B** INFORMATION TECHNOLOGY SPECIALIST  
**25F** NETWORK SWITCHING SYSTEMS OPERATOR/MAINTAINER  
**25N** NODAL NETWORK SYSTEMS OPERATOR/MAINTAINER  
**05H** EW/SIGNALS INTELLIGENCE MORSE INTERCEPT OPERATOR  
**35I** COUNTERINTELLIGENCE  
**37F** PSYCHOLOGICAL OPERATIONS SPECIALIST  
**1J** OPERATIONAL EW OPERATOR  
**2S** BATTLE STAFF OPERATIONS  
**H1B** OPSEC PRACTITIONER SPECIALIST  
**P4** TACTICAL INFORMATION OPERATIONS

**NAVY DESIGNATORS**

**Commissioned Officers**

**161X** INFORMATION WARFARE  
**160X** INFORMATION PROFESSIONAL  
**111X** SURFACE WARFARE (Surface EWOs)  
**132X** NAVAL FLIGHT (EA-6B, EP-3E)  
**644X** LIMITED DUTY OFFICER

**Non-Commissioned Officers**

**CT** CRYPTOLOGIC TECHNICIAN  
**IT** INFORMATION SYSTEM TECHNICIAN

**MARINE CORPS MOSs**

**Commissioned Officers**

**0510** BASIC IO STAFF OFFICER (ALTERNATIVE MOS)  
**8834** TECHNICAL IO OFFICER  
**0206** EW (GROUND) (PRIMARY MOS)  
**2602** SIGNALS INTELLIGENCE /EW OFFICER (III) (PRIMARY MOS)  
**7588** EW (AIR) (PRIMARY MOS)  
**0520** PSYCHOLOGICAL OPERATIONS OFFICER (ALTERNATE MOS)

**Non-Commissioned Officers**

**2691** SIGNALS INTELLIGENCE/EW CHIEF (PRIMARY MOS)  
**0521** PSYOP (ALTERNATE MOS)  
**2611** COMPUTER NETWORK OPERATIONS (PRIMARY MOS)

**AIR FORCE AFSCs**

**Commissioned Officers**

**11RX** RECCE/SUR/ELECT WARFARE PILOT  
**12RX** RECCE/SURV/ELECT WARFARE NAVIGATOR  
**14NX** INTELLIGENCE  
**33SX** COMMUNICATIONS & INFORMATION  
**16FX** REGIONAL AFFAIRS STRATEGIST  
**16GX** AIR FORCE OPERATIONS STAFF OFFICER  
**16PX** POLITICAL-MILITARY AFFAIRS STRATEGIST  
**16RX** PLANNING & PROGRAMMING  
**21RX** LOGISTICS READINESS  
**31PX** SECURITY FORCES  
**61SX** SCIENTIST  
**62EX** DEVELOPMENTAL ENGINEER  
**71SX** SPECIAL INVESTIGATOR

**Non-Commissioned Officers**

**1NXXX** INTELLIGENCE  
**2A5X1** AEROSPACE MAINTENANCE  
**2E2X1** COMM-ELEC/WIRE SYSTEMS MAINTENANCE  
**3CXXX** COMMUNICATIONS-COMPUTER SYSTEMS  
**3P0X1** SECURITY FORCES  
**7S0X1** SPECIAL INVESTIGATIONS

## 2. Commissioned Officers

a. To be considered part of the Joint IO Force, commissioned officers from the aforementioned categories will have completed a Service IO course; previously served in IO related-assignments within their respective Service components at the unit, intermediate, or higher headquarters level; and satisfied the requirements outlined in paragraph 1 of this enclosure (see Figure A-1).

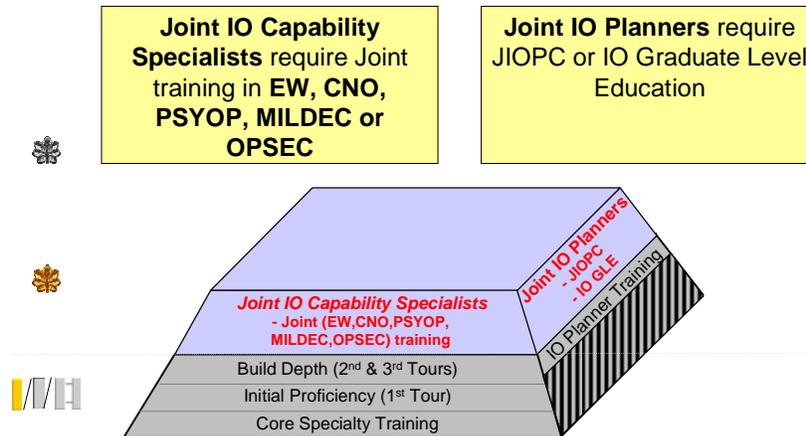


Figure A-1. Joint IO Force Structure (Commissioned Officer)

b. Guidance provided in Department of Defense Instruction (DODI) 3608.11 “Information Operations Career Force,” (4 November 2005) (reference b) states the IO Career Force includes “. . .the military professionals that perform and integrate the core IO capabilities of EW, CNO, PSYOP, MILDEC and OPSEC,” and provides further elaboration indicating that “The IO Career Force consists of IO Capability Specialists and IO Planners.”

c. Guidance provided in DODI 3608.11 (reference b) directly affecting the Joint IO Force includes the statement that IO planners “. . .usually serve one or more tours as an IO capability specialist prior to assignment as an IO planner. . .” IO planners will not be drawn exclusively from capability specialists. Some Joint IO planners will come from backgrounds other than the core capability specialties. Given the need to fully integrate IO into the Adaptive Planning and Execution System, priority consideration for selecting personnel to augment the Joint IO Force from outside the IO community will be given to personnel from the more traditional warfighting career paths (e.g., pilots, combat arms officers, surface warfare officers, and planners) across all Services, who have completed a Service planner’s course (see Figure A-2).

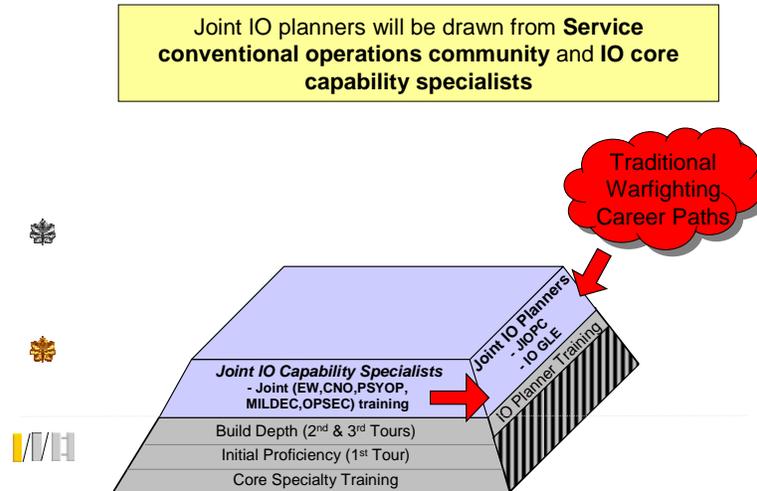


Figure A-2. Joint IO Force Structure (Commissioned Officer)

Additional MOSs/AFSCs/SIs, and Navy Designators/Navy Enlisted Classifications from which the Joint IO Force are drawn include:

- ARMY MOSs**  
**Commissioned Officer**  
11X INFANTRY  
12X ARMOR  
13X FIELD ARTILLERY  
14X AIR DEFENSE ARTILLERY  
15B AVIATION  
18A SPECIAL FORCES
- NAVY Designators**  
**Commissioned Officer**  
111X SURFACE WARFARE  
112X SUBMARINE WARFARE  
113X SPECIAL WARFARE  
114X EXPLOSIVE ORDNANCE DISPOSAL  
13XX PILOT/NAVAL FLIGHT
- MARINE CORPS MOSs**  
**Commissioned Officer**  
03XX INFANTRY  
08XX FIELD ARTILLERY  
18XX TANK & ASSAULT AMPHIBIOUS VEHICLE  
2305 EXPLOSIVE ORDNANCE DISPOSAL  
7208 AIR SUPPORT CONTROL  
7210 AIR DEFENSE CONTROL  
75XX PILOT & NAVAL FLIGHT
- AIR FORCE AFSCs**  
**Commissioned Officer**  
11X PILOT  
13BX BATTLE MANAGER  
13SX SPACE & MISSILE

Including the conventional operations MOSs/AFSCs or designators will help promote the best possible integration of IO capabilities into the Adaptive Planning and Execution System.

d. Initial assignment for a Joint IO Force commissioned officer will most likely be to a combatant command as a member of a headquarters staff, Joint Planning Group (JPG), IO cell, or Joint Task Force (JTF) (see Figure A-3). In the case of a combatant command, the tour of duty will normally be 36 months. For a JTF, the tour duration could range from 60 days to more than a year. While the combatant command headquarters staff and JTF require fully qualified, Joint IO capability specialists and planners, the specific skills and training/education required by members of each organization are different. Therefore, capability specialist qualifications for JTF duty will include component-level experience in an IO core capability, along with the successful completion of a USJFCOM-certified Joint IO capability specialist course (i.e., EW, CNO, PSYOP, MILDEC, or OPSEC).

e. In the case of Joint IO planners, all must successfully complete a Service planner's course and JIOPC before being assigned to a JTF. For individuals selected for assignment to a combatant command staff, JIOPC is the minimum requirement and should be completed prior to assignment. The combatant command IO Division/Branch Chief (J-39) must have previously completed an O-4/O-5 PCS tour of duty as an IO planner or IO capability specialist at a combatant command headquarters/Joint Staff, or possess O-5/O-6-level experience as a planner/staff officer involved in an IO program within a J-3/J-5/J-8 directorate. Combatant commands may also choose to require selected personnel to have completed IO graduate level education (IO GLE). IO GLE is a postgraduate-level course of academic instruction, where students develop functional expertise in 13 joint IO competency areas (Enclosure C). It is designed to provide selected members of the Joint IO Force with in-depth study opportunities related to strategic-level applications of the "informational" instrument of national power.

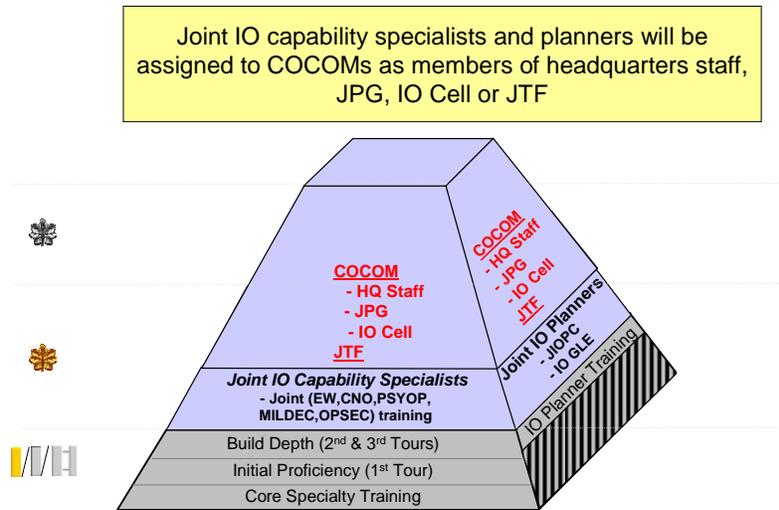


Figure A-3. Joint IO Force Structure (Commissioned Officer)

f. Besides those officers serving at the JTF- and Combatant Command-levels, members of the Joint IO Force will also be posted to billets on the Joint Staff and in the Office of the Secretary of Defense (OSD) (see Figure A-4).

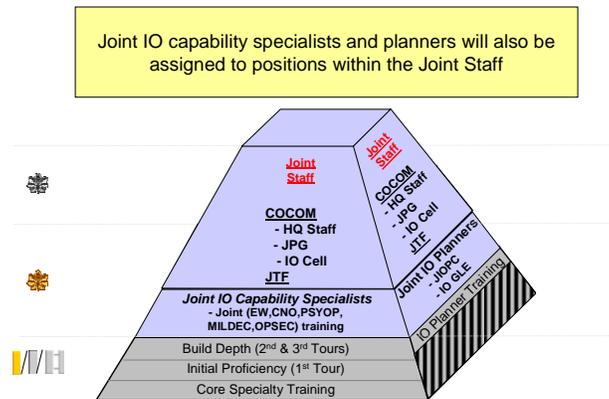


Figure A-4. Joint IO Force Structure (Commissioned Officer)

When serving on the Joint Staff or at OSD-level, IO personnel will spend considerable time on strategic-level issues. The education/training/experience needed to serve in these positions varies from what is required by the combatant command. As such, Joint Staff IO professionals must be fully conversant regarding national interests, strategy, the instruments of national power and the interagency process. For this reason, selected members of the Joint IO Force serving on the Joint Staff and at the OSD-level will be required to complete an IO GLE program and master its associated competencies (Enclosure C).

g. After completing a joint tour at a combatant command, on the Joint Staff or at the OSD level, it would be advantageous for the Services to use Joint IO Force qualified personnel as senior leaders in their component's IO Career Force (see Figure A-5). At the end of a Service component tour, some IO professionals will be selected to attend a Service Senior-Level College (SLC) and may reenter the Joint IO Career Force on the combatant command-, Joint Staff-, or OSD-levels.

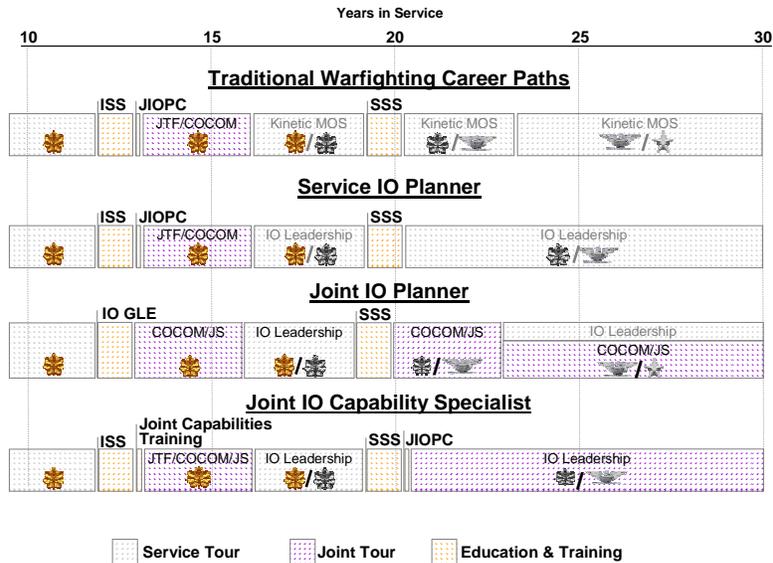


Figure A-5. Joint IO Force Timeline (Commissioned Officer)

h. IO professionals completing resident SLC may reenter the Joint IO Force at the 20-year point (see Figure A-6). Based on operational experience and completion of IO GLE, personnel can serve on a combatant command headquarters staff, the Joint Staff or OSD level, providing IO strategy or policy expertise to senior military and civilian leadership.

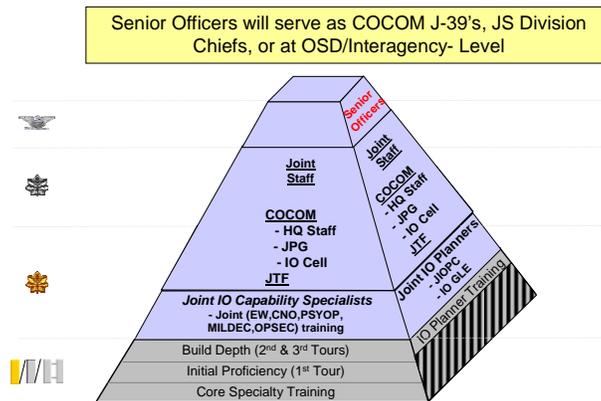


Figure A-6. Joint IO Force Structure (Commissioned Officer)

i. Besides the combatant command-level Colonel/Captain (O-6) Joint IO billets, there are several other O-6 positions within the National Capital Region where members of the Joint IO Force may be assigned. These positions include several within the Joint Staff and at the OSD level. Members of the Joint IO Force will be used to fill these positions following tours of duty on a combatant command headquarters staff or after completing an O-6-level assignment at a higher or Service component headquarters. Selected members of the Joint IO Force serving on the Joint Staff or within OSD at the O-6 level will be required to have completed the IO GLE program.

j. The “Quadrennial Defense Review (QDR) 2005” identified a total of six General/Flag Officer (G/FO) billets requiring IO experience (reference g), (see Figure A-7). These billets include:

- Commander, JTF Global Network Operations (GNO), (O-9), USSTRATCOM
- Commander, Joint IO Warfare Command (JIOWC), (O-8), USSTRATCOM
- Deputy Commander, Joint Functional Component Command Network Warfare (JFCC NW), (O-7), USSTRATCOM
- Deputy Director for Global Operations, (O-7), USSTRATCOM
- Commander, Military Information Support Command, (O-7), United States Special Operations Command (USSOCOM)
- Deputy Director for Global Operations, (O-7), Joint Staff J-3

(1) From this aggregate, a total of four billets reside with USSTRATCOM and one each with USSOCOM and the Joint Staff, respectively. Four of the six billets call for a Brigadier General/Rear Admiral (lower half) (O-7), with the remaining two billets split between a Major General/Rear Admiral (upper half) (O-8) and Lieutenant General/Vice Admiral (O-9). In addition to this requirement highlighted in the QDR, personnel filling these G/FO IO billets will

have successfully completed an O-4/O-5 PCS tour of duty as an IO planner or IO capability specialist on a Combatant Command headquarters staff or the Joint Staff, an IO GLE program or possess O-5/O-6-level experience as a planner/staff officer involved in an IO program within a J-3/J-5/J-8 directorate.

(2) Establishing this requirement ensures that G/FOs serving in key leadership billets understand the potential capabilities IO brings to the full range of military operations and that there will be sufficient advancement opportunities for the commissioned officers, who constitute part of the Joint IO Force.

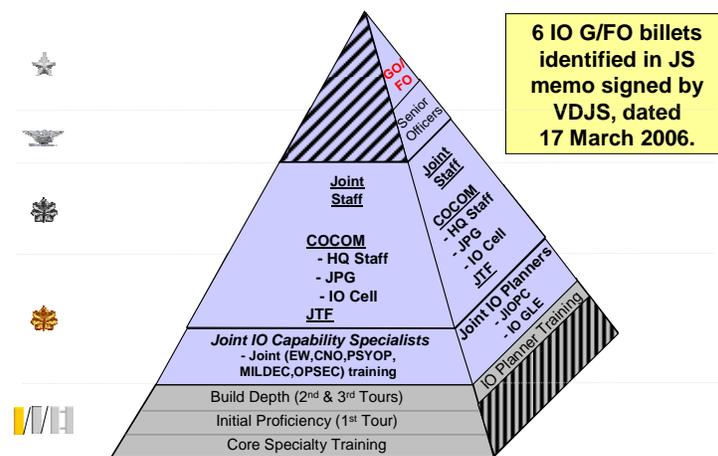


Figure A-7. Joint IO Force Structure (Commissioned Officer)

k. Additional G/FO billets for which IO experience is recommended include the following: Deputy Directors for J-3 and J-5 at U.S. Central Command (USCENTCOM), U.S. European Command (USEUCOM), and U.S. Pacific Command (USPACOM); the Deputy Directors for J-3 at U.S. Northern Command (USNORTHCOM), U.S. Southern Command (USSOUTHCOM), and U.S. Transportation Command (USTRANSCOM); the Deputy Commander of the Joint Warfighting Center at USJFCOM; and the Deputy Commander for Operations at the Joint Special Operations Command (JSOC) of the USSOCOM. In each case, the referenced G/FO is a Brigadier General/Rear Admiral (lower half) (O-7), serving as deputy to a principal whose responsibilities include, but are not limited to, IO. Based on their functional responsibilities, these 11 G/FOs will provide primary subject matter expertise to their principals regarding IO planning and execution. Service components should assign members of the Joint IO Force to these G/FO billets.

### 3. Non-Commissioned Officers

a. Non-Commissioned Officers (NCOs) meeting the criteria identified in paragraph 1 will normally have completed 10 years of service and a Service IO course, and will already have served in IO-related assignments within their respective Service component at the unit-, intermediate-, or higher headquarters-level. These personnel are eligible to enter the Joint IO Force as capability specialists.

b. In order to be considered a member of the Joint IO Force, NCOs are required to have completed a Service IO course and/or planner's course and a Joint IO Core Capabilities Specialist Course that aligns with their respective MOS/AFSC, Navy Designator, or background experience.

c. Upon successful completion of a Joint IO Capabilities Specialist Course, Non-Commissioned Officers will be assigned to either a combatant command or JTF, where they will serve as Joint IO capability specialists.



ENCLOSURE B

JOINT IO FORCE REQUIREMENTS

Level of War	Functional Level	Billet Title	Rank				Joint IO Education and Training		
			E-6/7/8/9	O-4/5	O-6	O-7/8/9	Specialist Course	JIOPC	IO GLE
Strategic	Joint Staff	IO Capability Specialist		X			X		
		IO Planner		X	X			X or	X
		Branch Chief		X				X or	X
		Division Chiefs			X				X
		Deputy Director				X			X
Strategic/ Operational	COCOM	JPG IO Capability Specialist		X			X		
		JPG IO Planner		X				X	
		IO Cell IO Capability Specialist	X	X			X		
		IO Cell IO Planner		X				X	
		HQ Staff IO Capability Specialist	X	X			X		
		HQ Staff IO Planner		X				X	
		HQ Staff IO Division/Branch Chief		X	X			X or	X
	Director*				X			X	
	COCOM SOC	IO Capability Specialist	X				X		
		IO Planner		X				X	
IO Division/Branch Chief			X				X or	X	
Operational/ Tactical	JTF/JFC	Capability Specialist	X	X			X		
		IO Planners		X				X	
		Commander**				X			X

\* In response to QDR tasking, Joint Staff and OSD identified USSTRATCOM Director, Combat and IO, as a G/FO billet requiring IO planner background and experience.

\*\* In response to QDR tasking, Joint Staff and OSD identified four JTF/JFC Commander positions as G/FO billets, requiring IO planner background and experience. These billets include the USSTRATCOM's Commanders of JTF-GNO and JIOWC as well as the Deputy Commander JFCC NW; USSOCOM's Commander, JMISC.

(INTENTIONALLY BLANK)

ENCLOSURE C

JOINT IO GRADUATE LEVEL EDUCATION COMPETENCIES

1. Upon successful completion of a Department of Defense Information Operations Education Board of Advisors approved IO Graduate-Level Education Program, a student will be able to consistently:
  - a. Analyze the global information environment as described in Joint Publication 3-13, "Information Operations," and assess its impact on national security strategy.
  - b. Analyze the role of information operations in national military strategy and maximize its contributions to national military power.
  - c. Analyze information operations' role in national information strategy and maximize its contributions to the non-military elements of national power.
  - d. Evaluate the relationship between information operations and other information-critical activities that support and are related to information operations.
  - e. Evaluate the relationships, linkages, and dependencies between intelligence and information operations.
  - f. Analyze the contributions of the interagency community to information operations, and vice versa.
  - g. Analyze non-U.S. (adversary, allied, and neutral) approaches to, capabilities, and doctrines for information operations.
  - h. Analyze the use of information operations to achieve desired effects across the spectrum of national security threats.
  - i. Evaluate the national military strategy, especially with respect to the changing nature of warfare.
  - j. Analyze how information operations are integrated to support the national military and national security strategies and the interagency process.
  - k. Analyze how information operations apply at the operational and strategic levels of war and how they support the operations of a networked force.

1. Evaluate the national security technological environment as an enabler for current and future competitive advantage.

m. Analyze the principles, capabilities, and limitations of information operations across the range of military operations, to include pre- and post-conflict operations.

ENCLOSURE D

REFERENCES

- a. DODD 3600.01, 14 August 2006, "Information Operations (IO)"
- b. DODI 3608.11, 4 November 2005, "Information Operations Career Force"
- c. DODI 3608.12, 4 November 2005, "Joint Information Operations (IO) Education"
- d. CJCSI 3210.01B, Chapter 1, 1 March 2008, "Joint Information Operations Policy"
- e. Joint Publication 3-13, 13 February 2006, "Information Operations"
- f. Department of Defense Information Operations Roadmap, 30 October 2003
- g. DJMS-0273-06, 17 March 2006, "Quadrennial Defense Review 2005 – IPT 2 Information Operations (IO) Working Group Directed Study"

(INTENTIONALLY BLANK)

## GLOSSARY

### ABBREVIATIONS AND ACRONYMS

AFSC	air force specialty code
CI	counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMO	civil military operations
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
COMCAM	combat camera
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DSPD	defense support to public diplomacy
eJMAPS	electronic Joint Manpower and Personnel System
EW	electronic warfare
G/FO	general officer/flag officer
IA	information assurance
IC	intelligence community
IO	information operations
IO GLE	information operations graduate-level education
ISS	intermediate service school
JFC	Joint Force Commander
JFSC	Joint Forces Staff College
JIOPC	Joint Information Operations Planning Course
JIOWC	Joint Information Operations Warfare Command
JMISC	Joint Military Information Support Command
JP	joint publication
JPSE	Joint Psychological Operations Support Element
JSOC	Joint Special Operations Command

JTF	Joint Task Force
JTF GNO	Joint Task Force Global Network Operations
MILDEC	military deception
MOS	military occupational specialty
OPSEC	operations security
OSD	Office of the Secretary of Defense
PSYOP	psychological operations
SLC	service senior-level college
USCENTCOM	U.S. Central Command
USEUCOM	U.S. European Command
USJFCOM	U.S. Joint forces Command
USNORTHCOM	U.S. Northern Command
USPACOM	U.S. Pacific Command
USSOCOM	U.S. Special Operations Command
USSOUTHCOM	U.S. Southern Command
USSTRATCOM	U.S. Strategic Command
USTRANSCOM	U.S. Transportation Command

TERMS AND DEFINITIONS

computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (JP 3-13) See also computer network defense; computer network exploitation; computer network operations. (JP 3-13)

computer network defense. Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called CND. (JP 3-13)

computer network exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE. See also computer network attack; computer network defense; computer network operations. (JP 3-13)

computer network operations. Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. (JP 3-13) See also computer network attack; computer network defense; computer network exploitation. (JP 3-13)

electronic warfare. Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic Warfare consist of three divisions: electronic attack, electronic protection, and electronic warfare support. Also called EW. (JP 3-13.1)

information operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Also called IO. See also computer network operations; electronic warfare; military deception; operations security; psychological operations. (JP 3-13)

information operations graduate-level education. Postgraduate-level course of academic instruction, where students develop functional expertise in 13 Joint information operations competency areas (Encl C). At present, there are 3 academic institutions within DOD which offer IO Education Board of Advisors-approved information operations graduate level education programs; the Naval Postgraduate School, National Defense University's National War College/Industrial College of the Armed Forces and the Joint Advanced

Warfighting School. Also called IO GLE. (CJCSM 1630.01)

joint information operations force. Personnel including commissioned officers in pay grades O-4 through O-9 and non-commissioned officers (NCO) in pay grades E-6 through E-9, who have completed either the US Joint Forces Command (USJFCOM) certified Joint IO Planning Course or a Joint IO Core Capabilities Specialist Course (e.g. Joint Electronic Warfare (EW), Joint Computer Network Operations (CNO), Joint Psychological Operations (PSYOP), Joint Military Deception (MILDEC) or Joint Operations Security (OPSEC)) and occupy an electronic Joint Manpower and Personnel Systems billet requiring Joint IO education and/or training. (CJCSM 3210.01B CH 1)

joint information operations billet. An electronic Joint Manpower and Personnel System billet, whose occupant directly functions as either a joint IO core capability specialist or joint IO planner. (CJCSM 3210.01B CH 1)

Joint information operations core capabilities specialist. A member of the Joint IO Force possessing functional expertise in EW, CNO, PSYOP, MILDEC or OPSEC and who has completed a Joint IO Core Capability Specialist Course. (CJCSM 3210.01B CH 1)

joint information operations planner. A member of the Joint IO Force possessing functional expertise with integrating IO capabilities into joint operation planning and execution system efforts, and who has successfully completed the Joint IO Planners Course. (CJCSM 3210.01B CH 1)

military deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called MILDEC. (JP 3-13.4)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 3-13.3)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological

operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP.  
(JP 3-53)

(INTENTIONALLY BLANK)