Report No. D-2009-090 July 2, 2009

Inspector General
United States Department of Defense

Information Operations Career Force Management

Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE
hotline

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

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

Acronyms and Abbreviations

DPG	Defense Planning Guidance
IO	Information Operations
JPG	Joint Programming Guidance
QDR	Quadrennial Defense Review
SPG	Strategic Planning Guidance
USD(I)	Under Secretary of Defense for Intelligence
USSTRATCOM	U.S. Strategic Command

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

July 2, 2009

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE(COMPTROLLER)/ DOD CHIEF FINANCIAL OFFICER
UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
COMMANDER, U.S. STRATEGIC COMMAND
DIRECTOR, JOINT STAFF

SUBJECT: Information Operations Career Force Management (Report No. D-2009-090)

We are providing this report for review and comment. We considered comments from the Under Secretary of Defense for Intelligence and the Joint Staff on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The comments from the Under Secretary of Defense for Intelligence were only partially responsive because they did not identify any actions taken or planned to coordinate with the Deputy Secretary of Defense to ensure the resolution of deficiencies where issues are not adequately resolved. We request additional comments on the recommendation by August 31, 2009. On the basis of comments from the Under Secretary of Defense for Intelligence, we revised the finding and recommendation to clarify the actions needed to improve the management of the Information Operations career force.

Please provide comments that conform to the requirements of DoD Directive 7650.3. If possible, send management comments in electronic format (Adobe Acrobat file only) to audros@dodig.mil. Copies of management comments must have the actual signature of the authorizing official for your organization. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at 703-604-8905 (DSN 664-8905).

Paul J. Granetto
Assistant Inspector General
Readiness, Operations, and Support

Report No. D-2009-090 (Project No. D2008-D000LH-0140.000) July 2, 2009

Results in Brief: Information Operations Career Force Management

What We Did

Military operations depend on information and information systems for many simultaneous and integrated activities. Information Operations is essential to the successful execution of military operations; therefore, a key goal of Information Operations is to achieve and maintain information superiority for the United States and its allies.

We evaluated the management of the Information Operations career force. Specifically, we intended to review how the combatant commands identified and prioritized requirements for Information Operations billets and training and education. However, each Service defines its career force differently, and the training and education requirements vary as well.

Thus, we focused on the overall management of Information Operations rather than at the combatant command level. In addition, we reviewed the internal controls as they related to Information Operations management.

What We Found

Although DoD has made strides in advancing Information Operations as a core military competency, we determined that there was a weakness in the oversight management processes. Until DoD improves the oversight, it cannot efficiently and effectively advance Information Operations into a warfighting capability for combatant commanders.

DoD has issued policy and guidance and conducted several Information Operations assessments. The responsibilities were dispersed across different DoD Component heads, which had related or collateral joint Information Operations responsibilities and functions specifically related to policy and oversight.

What We Recommend

To improve the advancement of Information Operations as a core military competency, the Under Secretary of Defense for Intelligence should coordinate with DoD Component heads and the Deputy Secretary of Defense to ensure that deficiencies in the training and education requirements of the Information Operations career force are resolved.

We also determined that there was a weakness in the controls over the management of Information Operations. The control issue is described in our finding and recommendation section of this report, and the recommendation addresses the action necessary to improve the control issue.

Management Comments and Our Response

Management agreed with the recommendation with one exception. The Under Secretary of Defense for Intelligence stated that the definition of Information Operations is clearly defined in DoD guidance. As a result of management comments, we revised the recommendation. Management comments are partially responsive, and we request additional comments by August 31, 2009. Please see the recommendation table on the back of this page.

U.S. soldier drops information leaflets in Iraq
U.S. Navy photo, Petty Officer 1st Class Mario A. Quiroga

Recommendation Table

Management	Recommendation Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Intelligence	1.	

Please provide comments by August 31, 2009.

Table of Contents

Results in Brief i

Introduction 1

Objective 1
Background 1
Review of Internal Controls 2

Finding. Improvements Needed in Oversight of Information Operations 3

Recommendation, Management Comments, and Our Response 9

Appendices

A. Scope and Methodology 12
Prior Coverage 15
B. Glossary 16
C. Timeline of Information Operations Guidance and Assessments 17

Management Comments

Under Secretary of Defense for Intelligence 18
Joint Staff 19

Introduction

Objective

The overall audit objective was to evaluate the management of the Information Operations (IO) career force. Specifically, we intended to examine how the combatant commands identified and prioritized requirements for IO billets and training and education. However, varying interpretations of training and education requirements within DoD resulted in our focusing on the overall management of IO rather than at each combatant command. In addition, we examined the internal controls as they related to the audit objective. See Appendix A for a discussion of the audit scope and methodology and for prior audit coverage related to the audit objective.

Background

The Secretary of Defense stressed the importance of IO at the Association of the U.S. Army's Annual Meeting, October 10, 2007. He stated: "We can expect that asymmetric warfare[1] will remain the mainstay of the contemporary battlefield for some time. … Success will be less a matter of imposing one's will and more a function of shaping behavior of friends, adversaries, and most importantly, the people in between."

According to DoD Directive (DoDD) 3600.01, "Information Operations," August 14, 2006, IO is

> the integrated employment of the five 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.

See Appendix B for a glossary defining the five core capabilities.

Military operations depend on information and information systems for many simultaneous and integrated activities. IO is essential to the successful execution of military operations; therefore, a key goal of IO is to achieve and maintain information superiority for the United States and its allies. Training the IO career force to understand the information environment, the role of IO in military affairs, and how IO differs from other information functions that contribute to information superiority is essential to carrying out the core capabilities.

The 2001 DoD Quadrennial Defense Review (QDR) outlined six critical operational goals to provide the focus for DoD's efforts to transform military capabilities to keep pace with emerging threats. One of these goals was having information systems available

---

[1] The definition of asymmetric warfare is evolving and usually focuses on a conflict in which the less capable opponent fights across the spectrum of political, economic, social, and military activity, paying little or no attention to the law of war.

in the face of attack and conducting effective IO. The 2006 QDR, however, identified gaps in conducting IO. Subsequently, the Defense Planning Guidance (DPG) for FY 2004-2009, which provides guidance on capabilities needed to implement the nation's military strategy, directed that IO become a core military competency. See Appendix A for further information on the QDR and DPG.

Review of Internal Controls

We determined that there was an internal control weakness as defined by DoD Instruction (DoDI) 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006. We reviewed applicable IO criteria, interviewed personnel, and determined that there was a weakness in the controls over the management of IO. The control issue is described in our finding and recommendation sections of this report, and the recommendation addresses the action necessary to improve the control issue. In addition, the Under Secretary of Defense for Intelligence plans to update DoDD 3600.01, "Information Operations," to better articulate the roles, responsibilities, and authorities across the IO community. We will send a copy of this report to the senior USD(I) official responsible for internal controls.

Finding. Improvements Needed in Oversight of Information Operations

Although DoD has made strides in advancing IO as a core military competency, deficiencies and shortfalls remain in the oversight management processes. Until DoD improves oversight by coordinating the responsibilities of the DoD Components outlined in DoD guidance, it cannot efficiently and effectively advance IO into a warfighting capability for combatant commanders.

The Under Secretary of Defense for Intelligence (USD[I]) is the principal staff assistant to the Secretary of Defense and the functional proponent for the IO career force. USD(I) should coordinate with DoD Component heads[2] and the Deputy Secretary of Defense to ensure that deficiencies in the training and education requirements of the IO career force are resolved.

Shortfalls in the Oversight of Management Processes

The DoD Component heads were tasked to perform related or collateral joint support responsibilities and functions pertaining to IO. Although DoD has made significant strides in advancing IO as a core military competency, improved oversight of the Components' efforts is needed to ensure that IO deficiencies and shortfalls are resolved.

The DoD "Information Operations Roadmap," October 30, 2003, provided DoD with a plan to advance the goal of having IO as a core military competency. It outlined 57 recommendations specific to IO and assigned responsibility for them to various DoD Component heads, all reporting to the Deputy Secretary of Defense. USD(I) officials stated to us that the related and collateral joint responsibilities hindered enforcing implementation of the 2003 recommendations, and as a result, USD(I) closed them and identified current deficiencies in the IO career force.

The "U.S. Strategic Command [USSTRATCOM] Combatant Command IO Assessments," January and March 2008, looked across the combatant commands; identified shortfalls; recognized themes and trends; identified high-impact, cross-cutting solutions; and made specific recommendations for improvement. The overall conclusion of the assessments was that despite previous efforts to address IO deficiencies, shortfalls remain. Although the assessments highlighted IO deficiencies and shortfalls, we believe improvements to the oversight management processes would help resolve them.

Responsibilities of the DoD Components

The IO responsibilities for DoD personnel are defined in DoDD 3600.01, "Information Operations," August 14, 2006; DoDI 3608.11, "Information Operations Career Force," November 4, 2005; and DoDI 3608.12, "Joint Information Operations Education,"

---

[2] DoD Component head refers to the Office of the Secretary of Defense, Military Departments, Chairman of the Joint Chiefs of Staff, combatant commands, and Defense agencies.

November 4, 2005. The responsibilities were dispersed across the different DoD Component heads, which had related or collateral joint IO responsibilities and functions specifically related to policy and oversight as outlined below.

USD(I) is to:

- serve as the principal staff assistant to the Secretary of Defense for IO;
- develop and oversee DoD IO policy and integration activities;
- serve as the DoD lead within the Intelligence Community regarding IO issues;
- coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements;
- serve as the DoD functional proponent for the IO career force; and
- designate a general officer, flag officer, or senior executive to serve as a member of the board of advisors and a representative to the board's working group for joint IO education.

The Under Secretary of Defense for Acquisition, Technology, and Logistics is to:

- establish specific policy for the development of electronic warfare as a core IO capability; and
- designate a general officer, flag officer, or senior executive to serve as a member of the board of advisors and a representative to the board's working group for joint IO education.

The Under Secretary of Defense for Policy is to:

- provide DoD oversight of IO planning, execution, and related policy guidance, including establishing a review process within the Office of the Secretary of Defense to assess IO plans and programs submitted by combatant commanders to verify that proposed IO capabilities are appropriately coordinated and consistent with DoD policy;
- lead interagency coordination, exclusive of the Intelligence Community, and international cooperation involving the planning and employment of IO capabilities;
- establish specific policy and oversight for the development and integration of psychological operations as a core IO capability; and
- designate a general officer, flag officer, or senior executive to serve as a member of the board of advisors and a representative to the board's working group for joint IO education.

The Under Secretary of Defense for Personnel and Readiness is to:

- develop policies and procedures on matters pertaining to the establishment and management of an IO career force in coordination with the Secretaries of Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretary of Defense for Policy, USD(I), and others;

- provide training policy and oversight as it pertains to the integration of all IO capabilities into joint exercises and training;
- develop military training policy and oversee IO career force operational training; and
- designate a general officer, flag officer, or senior executive to serve as member of the board of advisors and a representative to the board's working group for joint IO education.

The Chairman of the Joint Chiefs of Staff is to:

- serve as the principal military advisor to the President, National Security Council, and Secretary of Defense on IO;
- develop and maintain joint doctrine for core, supporting, and related IO capabilities in joint operations;
- ensure all joint education, training, plans, and operations include, and are consistent with, IO policy, strategy, and doctrine; and
- designate a general officer, flag officer, or senior executive to serve as co-chair of the board of advisors and a representative co-chair to the board's working group for joint IO education.

The Commander, USSTRATCOM is to:

- integrate and coordinate DoD IO core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security that cross geographic areas of responsibility;
- serve as the operational advocate for the IO career force; and
- designate a general officer, flag officer, or senior executive to serve as co-chair of the board of advisors and a representative co-chair to the board's working group for joint IO education.

The responsibilities shown above were dispersed across the DoD Component heads, all reporting to the Deputy Secretary of Defense. We believe that USD(I), as the functional proponent of the IO career force, needs to improve its oversight of the Components' efforts to resolve IO deficiencies and shortfalls.

Management Initiatives

Since the 2001 DoD QDR identified IO as a critical operational goal, DoD has made strides in advancing IO as a core military competency by identifying areas for improvement in published guidance and planning documents and assessments.

Guidance and Planning Documents

According to the 2004 National Military Strategy, improvements to IO would contribute to a more robust and effective deterrent capability. The 2006 DoD QDR identified gaps in IO, including psychological operations, and the DPG for FY 2004-2009, May 2002, directed that IO become a core military competency.

Additionally, Strategic Planning Guidance (SPG) for FY 2006-2011, March 2004, stated that DoD Components are to use recommendations from the IO Roadmap in formulating programs for FY 2006. Joint Programming Guidance (JPG) for FY 2006-2011 allocated funds to improve IO at the combatant commands, specifically USSTRATCOM. The Unified Command Plan, May 5, 2006, stated that USSTRATCOM is responsible for integrating and coordinating DoD IO that crosses geographic areas of responsibility or the core IO capabilities: electronic warfare, computer network operations, psychological operations, military deception, and operations security.

The DoD "Information Operations Roadmap," October 30, 2003, stressed the importance of IO by providing a plan to advance IO as a core military competency. The Roadmap also called for a dedicated workforce and improved training and education for IO. The Roadmap stated that DoD is committed to transforming military capabilities to keep pace with emerging threats and to develop new opportunities as a result of innovation and rapidly developing information technologies. It provided a common framework for understanding IO policies and procedures.

The mandate in the IO Roadmap was to address the full scope of IO, including conducting studies on policies, plans, organization, education, career force, analytic support, and the core capabilities. The Roadmap outlined 57 recommendations specific to transforming IO into a core military competency.

Some of the recommendations were as follows.

- Consolidate oversight and advocacy for IO.
- Approve a common understanding and approve a definition of IO.
- Create a well-trained and educated career workforce.
- Establish an IO career force comprising two categories: for the time being, IO planners and IO capability specialists.
- Identify joint and Service IO billets.
- Expand or modify current IO training courses and develop new ones.
- Maintain a central database of all DoD IO training and education for both specialized and full-spectrum IO courses to assist in planning and make it Web-accessible. The data should be integrated into the master joint course database maintained by Joint Forces Command for all joint individual training.

The Roadmap assigned responsibility for implementing the 57 recommendations to various organizations, such as the Secretary of Defense Components and Military Departments. The responsibilities were dispersed across the different DoD Component heads, all reporting to the Deputy Secretary of Defense.

Management Assessments

U.S. Strategic Command Combatant Command Information Operations Assessment

The Joint Requirement Oversight Council tasked USSTRATCOM with conducting an assessment of all combatant command shortfalls across the five core capabilities of IO. The goal of the assessment was to look across the combatant commands and identify shortfalls; recognize themes and trends; identify high-impact, cross-cutting solutions; and make specific recommendations.

- Phase I of the USSTRATCOM IO Assessment, January 2008, was the baseline phase or the data collection and analysis phase. The conclusion of the assessment was that despite previous efforts to address IO deficiencies (for example, the 2003 DoD IO Roadmap signed by the Secretary of Defense more than 4 years earlier), a significant number of shortfalls remain.

- Phase II, March 2008, was similar to Phase I. It included the baseline from Phase I and the combatant command validation of the baseline report. The Assessment highlighted the IO Roadmap, which directed numerous actions to address a broad range of IO shortfalls. Phase II also concluded that despite efforts to address IO deficiencies, a significant number of shortfalls remain.

The USSTRATCOM Assessment addressed 52 deficiencies, including the following that relate to our audit objective.

- Lack of personnel with training in joint IO planning and integration at the combatant commands.
  - Incoming personnel lack experience when arriving at the combatant commands.
  - Service IO personnel lack training for the joint level.
- Inadequate IO education system.
  - No standard IO education requirements across the combatant commands.
  - Insufficient IO military education for key IO planning staff members, including Service components.
- Insufficient IO planner billets on combatant command staffs.
- Lack of experienced general IO planners on combatant command staffs.

This assessment, like others, identified deficiencies and shortfalls; however, not having adequate oversight management processes has hindered resolving them.

Director, Joint Staff Memo 0312-08

The purpose of the memorandum on "IO Education and Training Requirements," April 2008, was to develop the baseline requirements for the present and future joint IO force. This effort was designed to ensure that all joint IO professionals possess a common training foundation. The Vice Director, Joint Staff requested that all combatant

commands identify the joint IO training and education requirements for each command by billet. According to Joint Staff, Strategic Operations Division (J-39) officials, the responses they received were not a clear representation of the IO career force.

For example, there were personnel on the list that did not perform an IO function and yet they were listed because their position required some IO training. We visited two combatant commands and were unable to identify a standard IO career force. Until combatant commands provide accurate information regarding baseline training and education requirements, developing the IO career force into a core military competency will be difficult.

Draft USD(I) Defense-Wide IO Program Review Summary

USD(I) conducted a review of the IO program. It recommended updating DoDD 3600.01, "Information Operations," as the first priority and addressing IO career force issues as the second priority. The updates planned for DoDD 3600.01 are intended to better articulate the roles, responsibilities, and authorities across the IO community. The review identified challenges in the development and implementation of a DoD-wide IO career force and concluded that progress has been slow and uneven, varying significantly among the Services.

One of the major roadblocks to achieving core competency thus far is the differing interpretations of training and education requirements for the IO career force. The review further identified the following issues related to the IO career force.

- Combatant commands have too few IO billets.
- The inadequate coding of combatant command-managed billets hinders Service nominations of highly-qualified personnel.
- Combatant commands and agencies identified a shortage of IO professionals within their organizations.
- DoD-wide education and training continues to be lacking within the intelligence and IO disciplines.
- Services need to provide clear paths and leadership positions as IO personnel seek success in their career.

All of the published guidance, planning documents, and assessments have contributed to the advancement of IO as a core military competency. See Appendix C for a detailed timeline of published guidance and assessments.

Conclusions

Since the 2003 publication of the IO Roadmap, DoD has issued policy and guidance and conducted several IO assessments. Although DoD has made strides in advancing IO as a core military competency, DoD is not efficiently and effectively advancing IO into a warfighting capability for combatant commanders.

USD(I) is the functional proponent for the IO career force and is the principal staff assistant to the Secretary of Defense for IO. USD(I) is also responsible for policy and

oversight of IO; however, USD(I) needs to improve its oversight management processes in order to resolve the deficiencies noted in past IO assessments. To improve the advancement of IO as a core military competency, USD(I) should coordinate the resolution of program deficiencies with DoD Component heads and the Deputy Secretary of Defense.

Recommendation, Management Comments, and Our Response

Revised Recommendation

As a result of comments from USD(I), we revised the draft finding and recommendation to clarify the actions needed to improve the management of the IO career force. We omitted the statement, "deficiencies in the definition of the IO career force," because as pointed out in the USD(I) comments, IO is defined in DoDI 3608.11, "Information Operations Career Force," November 4, 2005," as the military professionals that perform and integrate the core IO capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security.

We recommend that the Under Secretary of Defense for Intelligence coordinate Information Operations with DoD Component heads and the Deputy Secretary of Defense to ensure that deficiencies in the training and education requirements of the IO career force are resolved.

Under Secretary of Defense for Intelligence Comments

USD(I), agreed with the finding and recommendation, stating that, as the Secretary of Defense's Principal Staff Assistant for IO, he has taken substantive actions to correct IO deficiencies and increase oversight in the Department's IO. Specifically, USD(I) noted that the Information Operations and Strategic Studies division had led a Defense-wide IO Program and Capability Review to assess IO across DoD. The outcome of the review revealed that although the development of the IO career force had started in earnest, progress has been slow and uneven.

To augment progress in developing the IO career force (for example, Joint IO doctrine, training, education, and billet codification), USD(I) stated that a civilian personnel and readiness branch chief was added to the IO division to manage IO career force activities. In addition, USD(I) noted that the IO Executive Committee process is used for informing, coordinating, and resolving Defense-wide IO career force deficiencies. USD(I) also noted that his office is best positioned to address the responsibilities and concerns of IO stakeholders within DoD as well as across the Intelligence Community.

Our Response

USD(I) comments were partially responsive. We agree that USD(I) has taken action to coordinate with DoD Component heads to identify and address IO deficiencies and that progress has been slow and uneven.

However, although USD(I) agreed with the recommendation, he did not specify any actions taken or planned to coordinate with the Deputy Secretary of Defense to ensure the resolution of deficiencies where issues are not adequately resolved. We request that USD(I) provide additional comments in response to the final report to address this part of the recommendation.

Joint Staff Comments

Although not required to comment, the Joint Staff, Deputy Director for Global Operations, J-39 (Deputy Director) agreed with the overall finding that the oversight of IO needs improvement. However, the Deputy Director believed that the recommendation should focus on assigning a single oversight office empowered to compel the IO career force stakeholders to execute their specific assigned responsibilities. Further, the Deputy Director stated that he believes that assigning this responsibility to USD(I) in coordination with DoD Component heads and the Deputy Secretary of Defense could add further ambiguity to an area that needs more clarity.

The Deputy Director noted that a single office should be charged with controlling the fragmented responsibilities and holding the stakeholders accountable for the execution of IO because it would significantly contribute to the development of IO as a core military competency. He stated that the Deputy Secretary of Defense should exercise direct oversight responsibility for all appropriate entities identified in DoDD 3600.01 and DoDI 3608.11.

As an alternative to the Deputy Secretary of Defense exercising direct oversight, the Deputy Director stated that a single USD office could be effective if it had the resources and authority needed to execute the responsibilities of this complex and challenging role. Finally, the Deputy Director noted that regardless of which USD office assumes overall oversight, DoD must update the guidance to more clearly define the stakeholder responsibilities.

Our Response

Although we agree that a single USD office with the resources and authority would contribute to the maturation of IO as a core military competency, we believe that a single office would still have to coordinate with the Deputy Secretary of Defense on unresolved IO issues. In our opinion, if there are unresolved issues requiring the Deputy Secretary of Defense's attention, then USD(I), as the Principal Staff Assistant for IO, should closely coordinate those issues with the Deputy Secretary of Defense.

We are obtaining additional USD(I) comments on planned actions on this matter in the final report. We believe the actions taken by USD(I) to correct deficiencies and increase oversight of DoD IO validate that USD(I) is best positioned to coordinate and implement IO mitigation strategies.

Regarding guidance, we highlight the peer-level DoD Component head responsibility issues in the report, and we believe a single office charged with controlling the fragmented responsibilities and holding the stakeholders accountable for the execution of

IO should significantly contribute to the development of IO as a core military competency. In addition, our recommendation that USD(I) coordinate unresolved IO issues with the Deputy Secretary of Defense should ensure that deficiencies in the training and education requirements of the IO career force are resolved.

Appendix A. Scope and Methodology

We conducted this performance audit from February 2008 through March 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

We were unable to properly address the established audit objectives because IO oversight is decentralized. DoDI 3608.11, "Information Operations Career Force," specifically outlines the IO career force; however, the policy allows for a broad interpretation. We found that each Service identifies its career force differently. As a result, we were unable to identify a standard definition of the IO career force or a prioritization of training and education requirements in order to meet the audit objective.

Meetings and Site Visits

We met with USD(I) officials on five occasions to provide audit updates and brief them on the information we found at the combatant commands. We met with the Army, Navy, Air Force, and Marine Corps officials to obtain information on how they define their IO career force and how they train and educate their IO personnel.

We visited the U.S. Southern Command and the U.S. Pacific Command and interviewed officials in IO and the personnel office. We obtained information on their IO billets and training and education requirements.

Although we did not visit the other combatant commands, we obtained information on the IO career force of the U.S. European Command, U.S. Northern Command, and U.S. Central Command from the Directorate for Manpower and Personnel, Joint Staff (J-1). We interviewed J-1, J-39, and USSTRATCOM personnel about their responsibilities and management of the IO career force.

Information Operations Assessments and Reports

We reviewed the following DoD studies and assessment that identified areas for improvement in the IO career force.

- DoD "Information Operations Roadmap," October 30, 2003;
- Results of the USSTRATCOM Combatant Command Information Operations Assessment, January and March, 2008;
- Draft USD(I) Defense-Wide Information Operations Program and Capability Review Summary; and
- Director, Joint Staff Memorandum 0312-08, "Information Operations Education and Training Requirements," April 2, 2008.

These studies and assessments are not publicly available.

DoD Criteria and Guidance

We reviewed the following DoD directives and reports to determine the criteria regulating the management of the IO career force.

- DoDI 3608.11, "Information Operations Career force," November 4, 2005.

    - Section 4.4 states that DoD Components are to develop and implement a process to uniquely identify, in the appropriate personnel systems, a baseline list of joint and military Service IO positions. Joint duty IO positions are to be allocated to the Military Services in accordance with DoD policy.

    - Section 5 outlines the responsibilities of multiple DoD components. Specifically, USD(I) is to serve as the functional proponent for the IO career force and is to exercise overall responsibility for policies and procedures governing the IO career force.

- DoDI 3608.12, "Joint Information Operations Education," November 4, 2005. This instruction assigns responsibilities for joint IO education and establishes a board of advisors for joint IO education.

- DoDD 5143.01, "Under Secretary of Defense for Intelligence," November 23, 2005, states that USD(I) serves as the principal staff assistant to the Secretary of Defense on development and oversight of DoD IO policy and integration activities and as the DoD lead with the Intelligence Community on DoD IO issues. USD(I) is to coordinate, oversee, and assess the efforts of the DoD Components to plan, program, and develop capabilities in support of IO requirements pursuant to DoDD 3600.01.

- DoDD 3600.01, "Information Operations," August 14, 2006, outlines the responsibilities within DoD to support the objective of making IO a core military competency. This policy identifies multiple DoD Components responsible for furthering IO objectives. USD(I) is to develop and oversee DoD IO policy and integration activities and serve as the principal staff assistant to the Secretary of Defense for IO; more specifically, to coordinate, oversee, and assess the efforts of the DoD Components

- Chairman of the Joint Chief of Staff Instruction 3210.01B, "Joint Information Operations Policy," January 5, 2007. This instruction is not publicly available.

We reviewed the following DoD strategic documents on the IO functions and career force.

- The Quadrennial Defense Review (QDR), September 30, 2001, was the product of the senior civilian and military leadership of DoD. This report outlines the key changes needed to preserve America's safety and security in the years to come.

- The Defense Planning Guidance (DPG), May 2002, is prepared by the Secretary of Defense and based on the results of the QDR. It provides guidance on the capabilities needed to implement the National Defense Strategy. Also, it sets policy goals to focus on the highest priority activities and assigns broad responsibilities for implementation actions. It also directed development of the Information Operations Roadmap.

- The Strategic Planning Guidance (SPG), March 2004, is prepared each year by the Deputy Secretary of Defense. It provides general guidance to assist DoD in making resource allocations, developing new joint capabilities, and deciding where to reduce and accept risks. In addition, the SPG presents the future force vision for the Department and provides minimal programmatical direction for development of the Defense Budget.

- The Joint Programming Guidance (JPG), June 2004, is prepared by the Deputy Secretary of Defense. Inputs to the JPG include the Integrated Priority Lists prepared by the combatant commands, the DPG prepared by the Secretary of Defense, and the SPG prepared by the Deputy Secretary of Defense. The JPG provides general, but more detailed, fiscal guidance for preparing budget submissions.

- The 2006 QDR set out where DoD was at the time and the direction DoD's senior leadership believed it needed to go in fulfilling its responsibilities to the American people.

- The Unified Command Plan, May 2006, is prepared by the Secretary of Defense and submitted to and approved by the President of the United States. It assigns missions and functions to the combatant commands, which in turn affects their overall personnel requirements. However, the overall requirements exceed the scope of our audit, which focuses only on personnel requirements related to the IO career force.

Use of Computer-Processed Data

We used computer-processed data to obtain background information on the IO career force at the combatant commands. The data were in Excel spreadsheets of the Joint Table of Distribution (a requirements and authorization document) from the Electronic Joint Manpower and Personnel System. Because of the limited scope of the audit, the data did not influence the results of our finding.

Prior Coverage

During the last 5 years, the Department of Defense Office of Inspector General (DoD IG) and Air Force Audit Agency have issued two reports discussing the IO career force. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports. Unrestricted Air Force Audit agency reports can be accessed at https://www.afaa.hq.af.mil/.

DoD IG

DoD IG Report No. D-2006-083, "Information Operations in U.S. European Command," May 12, 2006

Air Force

Air Force Audit Agency Report No. F2005-0003-FD3000, "Information Operations Personnel Data Verification," April 1, 2005

Appendix B. Glossary

Computer Network Operations is one of the five core IO capabilities. It comprises computer network attack, computer network defense, and related computer network exploitation enabling operations.

- **Computer Network Attack** is operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
- **Computer Network Defense** is actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.
- **Computer Network Exploitation** is the enabling of operations and intelligence collection to gather data from target or adversary automated information systems or networks.

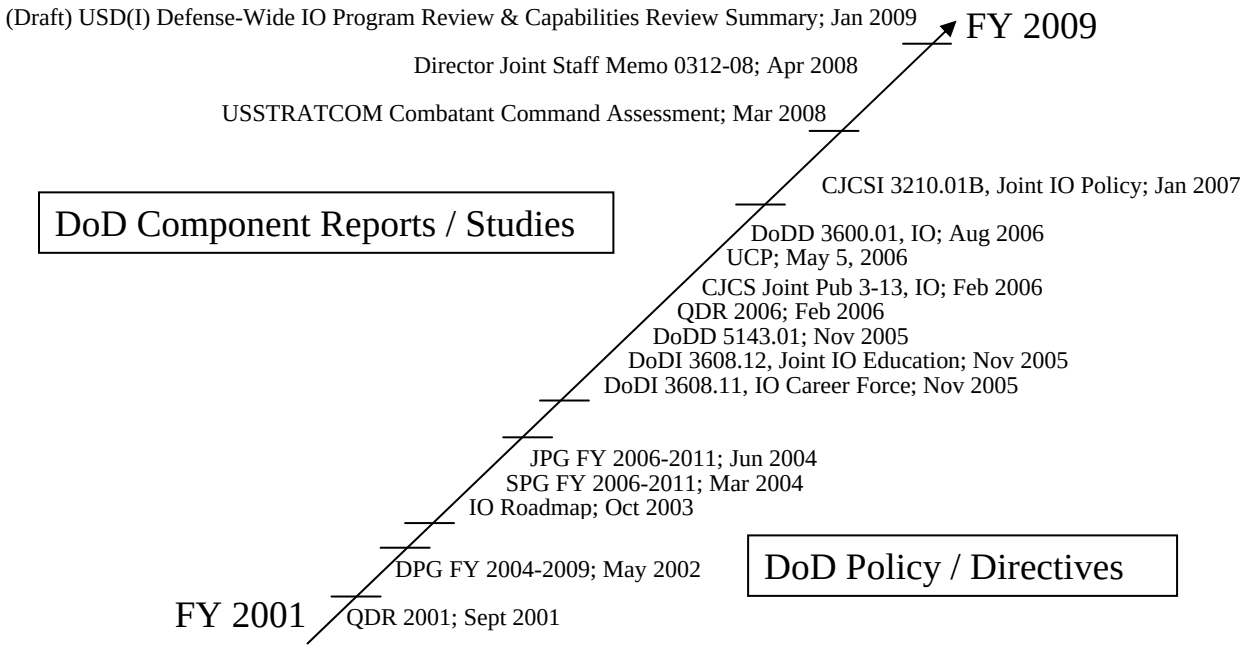
Electronic Warfare is one of the five core IO capabilities. It is any military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy.

Military Deception is one of the five core IO capabilities. It includes those measures designed to mislead an adversary by manipulation, distortion, or falsification to induce the adversary to react in a manner prejudicial to its interests.

Operations Security is one of the five core IO capabilities. It is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems, determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Psychological Operations is one of the five core IO capabilities. It is 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. To see an example of psychological operations, see the picture in the Results in Brief.

Appendix C. Timeline of Information Operations Guidance and Assessments



Legend

CJCSI – Chairman of the Joint Chiefs of Staff Instruction
DoDD – Department of Defense Directive
DoDI – Department of Defense Instruction
DPG – Defense Planning Guidance
IO – Information Operations
JPG – Joint Programming Guidance
QDR – Quadrennial Defense Review
SPG – Strategic Planning Guidance
UCP – Unified Command Plan

Office of the Under Secretary of Defense for Intelligence Comments

Final Report Reference

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

INTELLIGENCE

MAY 28 2009

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Information Operations Career Force Management Report, Project No. D2008-D000LH-0140.000

In response to your memorandum, dated March 19, 2009, we concur with the finding and recommendation with one exception. The statement that there is a deficiency in the definition of the Information Operations Career Force (IOCF) is inaccurate. Department of Defense (DoD) Instruction 3608.11, paragraph 3.4 defines the IOCF as "The military professionals that perform and integrate the core IO [Information Operations] capabilities of EW, CNO, PSYOP, MILDEC, and OPSEC. The IO Career Force consists of IO Capability Specialists and IO Planners." Revised

As the Secretary of Defense's Principal Staff Assistant (PSA) for IO, I have taken substantive actions to correct deficiencies and increase oversight in DoD IO. The Information Operations and Strategic Studies Directorate/Information Operations Division (IOD) conducted a Defense-Wide IO Program and Capability Review (DWIOPR) to assess the state of IO across the Department. The DWIOPR concluded that IOCF development has started in earnest, but progress has been slow and uneven. To augment progress in Joint IO doctrine, training, education, and billet codification, a government civilian Personnel and Readiness Branch Chief was added to the IOD staff to manage IOCF activities. In addition, the IO Executive Committee (EXCOM) process is now being used to inform, coordinate, and resolve Defense-wide IOCF deficiencies.

The Office of the Under Secretary of Defense for Intelligence, representing the Secretary's PSA for IO, is best resourced and positioned to integrate and deconflict the responsibilities and concerns of IO stakeholders within the Department and across the Intelligence Community.

My points of contact are [redacted]

James R. Clapper, Jr.

Joint Staff Comments

UNCLASSIFIED

THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-3000

03 April 2009

MEMORANDUM FOR: PROGRAM DIRECTOR, READINESS, OPERATIONS, & SUPPORT, DOD INSPECTOR GENERAL

Subject: Draft Information Operations Career Force Management Report, Project No. D2008-D000LH-0140.000, 19 March 2009

1. I appreciate the opportunity to comment on your draft report regarding *Information Operations Career Force Management*. While I agree with the overall finding that improvements are needed in oversight of Information Operations (IO), I also believe that the associated recommendation should be more focused in terms of assigning a single oversight office empowered to compel IO career force stakeholders to execute their specific assigned responsibilities.

2. Assigning the responsibility to correct the broad range of identified deficiencies to the Undersecretary of Defense for Intelligence (USD(I)) in coordination with DOD Component heads and the Deputy Secretary of Defense (DEPSECDEF) will not ensure that those deficiencies are efficiently and effectively resolved. In fact, execution of this recommendation may have the unintended consequence of adding further ambiguity to an area that needs more clarity. For example DODD 3600.01, *Information Operations*, assigns no IO career force responsibilities to USD(I). According to this directive, responsibility for developing policy and procedures on matters pertaining to an IO career force, as well as providing training policy and oversight for IO, reside with the Under Secretary of Defense for Personnel and Readiness. In contrast, DODI 3608.11, *Information Operations Career Force,* directs USD(I) to serve as the DOD functional proponent and U.S. Strategic Command (USSTRATCOM) as the operational advocate for the IO career force. However, nowhere are the specific responsibilities of an operational advocate explained, contributing to ambiguity regarding what constitutes USSTRATCOM's IO career force management responsibilities.

3. The DOD directives and instructions cited above clearly indicate that oversight responsibilities for the IO career force are fragmented. This

UNCLASSIFIED

fragmentation has significantly inhibited task accountability for IO career force management and is limiting the maturation of IO into a core military competency. A single office charged with the responsibility of harnessing these fragmented responsibilities while holding stakeholders accountable for execution will focus the IO community's efforts and significantly contribute to IO maturation as a core military competency. For this reason I recommend that accountability for IO Career Force management be vested with the DEPSECDEF, who would exercise direct oversight responsibility for all appropriate entities identified in DODD 3600.01 and DODI 3608.11. As an alternative, vesting this responsibility with a single USD office can be effective as well, only if that USD office is empowered with the resources and authority required to execute this complex and challenging role. Regardless of which office assumes overall oversight for coordination and execution, governance must be updated to define this relationship and more clearly define individual stakeholder responsibilities.

4. Further questions regarding this matter can be addressed to my POC for IO Career Force matters, [redacted].

ROWAYNE A. SCHATZ, JR.
Brigadier General, USAF
Deputy Director for Global Operations, J-39

Inspector General
Department of Defense