



ADMINISTRATION AND
MANAGEMENT

OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

01 JUL 2005

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense (DoD) Reporting Guidance for Agency Privacy Management
for Fiscal Year 2005 (FY05)

On June 13, 2005, the Office of Management and Budget (OMB) issued instructions for agency reporting under the Federal Information Security Management Act of 2002 (FISMA) (Attachment 1).

Where before, the report dealt solely with an agency's Information Technology security program, the report has been expanded this year to ask questions regarding an agency's privacy program. Where before, agency Chief Information Officers and Inspectors General provided information, this year's report asks the Senior Agency Official for Privacy, in consultation with other agency privacy officials, to complete the privacy section of the FISMA report.

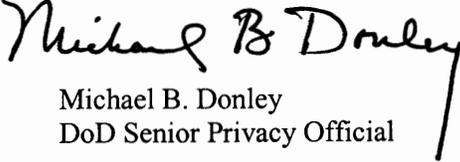
The privacy section asks a series of questions relating to (1) the responsibilities of agency officials having oversight for their respective privacy programs, (2) agency privacy procedures and practices, and finally, (3) internal oversight mechanisms for privacy (Attachment 2). The questions also relate, in part, to agency implementation of the privacy provisions of the E-Government Act of 2002.

In order to prepare the report, each DoD Component shall review its privacy program and provide information responsive to the OMB questions. To assist in this review, supplementary guidance (Attachment 3) has been prepared that can be used by Component Privacy Officials incident to obtaining and reporting the necessary information.

To meet the OMB suspense of October 7, 2005, the senior Component official having responsibility for privacy shall complete the review so that the report can be submitted to the Defense Privacy Office, 1901 South Bell Street, Arlington, Virginia 22202-4512, no later than August 19, 2005.

OSD 12811-05

My point of contact for this report is Mr. Vahan Moushegian, Jr., Director of the Defense Privacy Office. Should you have any questions, he can be contacted at (703) 607-2943 or via email at vahan.moushegian@osd.mil.


Michael B. Donley
DoD Senior Privacy Official

Attachments:

1. OMB Memo
2. Privacy Survey
3. DoD Supplementary Guidance



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D. C. 20503

June 13, 2005

M-05-15
THE DEPUTY DIRECTOR

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

This memorandum provides instructions for agency reporting under the Federal Information Security Management Act of 2002 (FISMA).

This year, we are asking a number of questions regarding your agency's privacy program. As noted in the instructions, the privacy program questions (Section D of the report) shall be completed by the Senior Agency Official for Privacy, in consultation with other agency privacy officials as appropriate. These questions relate, in part, to agency implementation of the privacy provisions of the E-Government Act. Thus, OMB will no longer ask agencies to include privacy related information in their annual E-Government Act submissions.

As you know, FISMA provides the framework for securing the Federal government's information technology including both unclassified and national security systems. All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the effectiveness of their security programs.

OMB uses the information to help evaluate agency-specific and government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and inform development of the E-Government Scorecard under the President's Management Agenda.

Reports are most helpful when they clearly and accurately reflect the status of the Agency's information security program. To promote accuracy and clarity, please make every attempt to resolve any discrepancies between the CIO and IG sections of the report before transmittal. If discrepancies cannot be reconciled, please explain the reasons for the differences in your transmittal letter to the OMB Director and to Congress.

Agencies shall transmit their reports to OMB by October 7, 2005, in the manner described in the attached instructions. In addition to the formal report transmittal to OMB, an electronic copy shall be sent to fisma@omb.eop.gov. Please contact Kim Johnson, Kim_A.Johnson@omb.eop.gov, or Kristy LaLonde, klalonde@omb.eop.gov, if you have any questions regarding information technology security. Eva Kleederman should be contacted at Eva_Kleederman@omb.eop.gov regarding privacy questions.

Attachments

ATTACHMENT 1

Section D - Reporting Template for Senior Agency Officials for Privacy

A reporting template tool will be sent at a later date. Below are the questions to be included in the template, in a narrative format. This shall be completed by all agencies.

I. Senior Agency Official for Privacy Responsibilities

1. Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)?

Yes or No.

2. Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19?

Yes or No.

3. Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information?

Yes or No.

II. Procedures and Practices

1. Does your agency have a training program to ensure that all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?

Yes or No.

2. Does your agency have a program for job-specific information privacy training (i.e., detailed training for individuals (including contractor employees) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities)?

Yes or No.

3. Section 3, Appendix 1 of OMB Circular A-130 requires agencies conduct -- and be prepared to report to the Director, OMB on the results of -- reviews of activities mandated by the Privacy Act.

Please indicate by component (e.g., bureau, agency) which of the following reviews were conducted in the last fiscal year.

[make chart with the following headings]

Section M Contracts	Records Practices	Routine Uses	Exemptions	Matching Programs	Training	Violations	Systems of Records
---------------------	-------------------	--------------	------------	-------------------	----------	------------	--------------------

4. Section 208 of the E-Government Act requires that agencies (a.) conduct Privacy Impact Assessments under appropriate circumstances, (b.) post web privacy policies on their websites, and (c.) ensure machine-readability of web privacy policies.

a. Does your agency have a written process or policy for:

- | | |
|-----------------------------------------------------------------------------------------------------|--------|
| (i) determining whether a PIA is needed? | Yes/No |
| (ii) conducting a PIA? | Yes/No |
| (iii.) evaluating changes in business process or technology that the PIA indicates may be required? | Yes/No |
| (iv.) ensuring that systems owners and privacy and IT experts participate in conducting the PIA? | Yes/No |
| (v.) making PIAs available to the public in the required circumstances? | Yes/No |
| (vi.) making PIAs available in other than required circumstances? | Yes/No |

b. Does your agency have a written process for determining continued compliance with stated web privacy policies?

Yes or No.

c. Do your public-facing agency web sites have machine-readable privacy policies (i.e., are your web privacy policies P3P-enabled or automatically readable using some other tool)?

Yes or No.

(i) if not, provide date for compliance:

5. By bureau, identify the number of information systems containing Federally-owned information in an identifiable form. For the applicable systems, on how many have you conducted a Privacy Impact Assessment and published a Systems of Records Notice?

a. FY 05 Systems that contain Federally-owned information in an identifiable form

- By bureau: number that contain information in an identifiable form

- Agency Systems
- Contractor Systems
- Total number of systems

b. FY 05 Privacy Impact Assessments

- By bureau: total number requiring a Privacy Impact Assessment in FY 05 (systems that are new or have been substantially altered)

- Agency Systems
- Contractor Systems
- Total number of systems

- By bureau: number that have a completed Privacy Impact Assessment within FY 05
 - o Agency Systems
 - o Contractor Systems
 - o Total number of systems
- c. FY 05 Systems of Records Notices
 - By bureau: number of systems from which Federally-owned information is retrieved by name or unique identifier
 - o Agency Systems
 - o Contractor Systems
 - o Total number of systems
 - By bureau: number of systems for which one or more Systems of Records Notice/s have been published in the Federal register
 - o Agency Systems
 - o Contractor Systems
 - o Total number of systems
- d. Contact Information for preparer of question 5.

6. OMB policy (Memorandum 03-22) prohibits agencies from using persistent tracking technology on web sites except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).

- a. Does your agency use persistent tracking technology on any web site?
Yes/No
- b. Does your agency annually review the use of persistent tracking?
Yes/No
- c. Can your agency demonstrate through documentation the continued justification for and approval to use the persistent technology?
Yes/No
- d. Can your agency provide the notice language used or cite to the web privacy policy informing visitors about the tracking?
Yes or No.

III. Internal Oversight

1. Does your agency have current documentation demonstrating review of compliance with information privacy laws, regulations and policies?

Yes or No.

- (i.) If so, provide the date the documentation was created.

2. Can your agency provide documentation demonstrating corrective action planned, in progress or completed to remedy identified compliance deficiencies?

Yes or No.

- (i.) If so, provide the date the documentation was created.

3. Does your agency use technologies that allow for continuous auditing of compliance with stated privacy policies and practices?

Yes or No.

4. Does your agency coordinate with the agency Office of Inspector General on privacy program oversight by providing to OIG the following materials:

a. compilation of the agency's privacy and data protection policies and procedures?

Yes/No

b. summary of the agency's use of information in identifiable form? Yes/No

c. verification of intent to comply with agency policies and procedures? Yes/No

5. Does your agency submit an annual report to Congress (OMB) detailing your privacy activities, including activities under the Privacy Act and any violations that have occurred?

Yes or No.

(i.) If so, when was this report submitted to OMB for clearance?

IV. Contact Information

Please provide the names, phone numbers, and e-mail addresses of the following officials:

Agency head:

Chief Information Officer:

Agency Inspector General:

Chief Information Security Officer:

Senior Agency Official for Privacy:

Chief Privacy Officer:

Privacy Advocate:

Privacy Act Officer:

Reviewing Official for PIAs:

DoD FY05 FISMA Privacy Guidance

References:

- (a) The Privacy Act of 1974, as amended (5 USC 552a)
- (b) E-Government Act of 2002, Section 208 (Public Law 107-347)
- (c) OMB Circular A-130, Appendix I, February 8, 1996
- (d) OMB Memo, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003
- (e) DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004
- (f) DoD 5400.11-R, "DoD Privacy Program," August 1983
- (g) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 17, 1998, as amended

Part I – Introduction. This guidance is intended to supplement and expand upon the OMB guidance. Therefore, it shall be read in conjunction that guidance. Each of the OMB questions is discussed below where, if appropriate, expanded guidance is furnished regarding how the review should be conducted. If there is a conflict between the OMB guidance and the supplementary guidance, the OMB guidance shall be followed.

Though many of the OMB questions are framed as "yes" or "no" questions, each answer shall be supported by a narrative statement that expands upon the Component reply. Because the DoD Privacy Program is decentralized, the approach taken by Components is not uniform. In order to properly reflect the current DoD program, a detailed explanation shall be furnished for each question, where applicable, so that a complete picture may be obtained for the Component's Privacy Program.

In responding to each of the OMB questions, care must be taken to document how you arrived at your response. Though unknown, it may be that the Privacy section of the FISMA report will be independently evaluated to ensure that the responses furnished by the Components and the Department are in fact supportable. Therefore, it is imperative that you ensure, incident to preparing the Component's report, that the information being provided is based on Component policies, procedures and practices.

References (a) through (f) can be found at www.defenselink.mil/privacy and reference (g) at www.defenselink.mil/webmasters. A copy of reference (b) is set forth as Attachment B to OMB Memo M-03-22 (reference (d)).

Part II – Reporting Template for Senior Agency Officials for Privacy

a. Senior Component Official for Privacy Responsibilities

Questions 1-3. Documentation of Component Privacy Official participating in

Component information activities; Component review of draft legislation, regulatory authority, and policy, as well as OMB Circular A-19 testimony and comment; Component assessment of the impact of technology on privacy.

It is recognized that the senior Component official having oversight responsibility for privacy normally is not directly involved in the day-to-day operations of the Component Privacy Program. It is further recognized that Component Privacy Officials having such responsibility sometimes have multiple portfolios. More often than not, the Component Privacy Official also is the Component Freedom of Information Act Official as well, a significant responsibility in and of itself. And finally, it is acknowledged that limited time and resources, when combined with other responsibilities, does not permit the Component Privacy Official to focus solely on privacy.

With the above as a start point, Components shall report how the Privacy Official(s) is(are) normally involved in Component information practices. To the extent Component regulatory/policy authority directs that Privacy Officials are specifically involved in any one of the three identified OMB areas, this authority shall be identified and discussed. It may be that specific authority identifying the Privacy Officials role *per se* does not exist, but that the Privacy Official is involved by virtue of his or her position in the Component's coordination or staffing process. Specifically, if coordination with the Privacy Official is routinely sought or accomplished incident to changes in either Component authority, Component review of legislation, A-19 testimony, and/or technology impact, this shall be identified and reported. It may be that the Privacy Official has established informal practices and procedures whereby he or she participates in the identified activities. In effect, whatever the processes are that result in the Component Privacy Official becoming involved should be captured in the Component's response to these three questions.

b. Procedures and Practices.

Questions 1-2. Does the Component have general and specific training programs that sensitize Component personnel, as well as contractors, to limitations on the collection, maintenance, use, and dissemination of Federal data?

DoD 5400.11-R, chapter 7 establishes the privacy training requirements for the agency. Paragraph C7.4.1 provides that each DoD Component is responsible for the development of training procedures and methodology. If your training requirements are set forth in Component regulatory or other authority, identify such authority and advise what those training policies are, keyed to the specific OMB questions being asked. It is acknowledged that each Component has developed training programs that best serve its Component. The Component shall report what those training programs are. To the extent some Components have developed non-standard training, such as web-based training or video Conference training, the Component shall identify such programs and include an assessment as to their success or failure.

Question 3. Which OMB Circular A-130 privacy reviews were conducted in the past Fiscal Year (i.e., FY05)?

Appendix I, paragraph 3 of the Circular provides that each agency shall conduct a review with a frequency as specified in the Circular and be prepared to report to OMB the results of such reviews and the corrective actions taken to resolve problems uncovered. For example, Section M contracts are reviewed every two years, routine uses are reviewed every four years, matching programs are reviewed annually.

It is therefore possible that a review for one or more of the identified areas will not be conducted in FY05. If not, advise when the review was last conducted or when it will be conducted. It is recognized that Components with a significant number of Privacy Act systems of records are not able to review each and every system notice for which it has responsibility. Where so, the Component shall indicate how it accomplishes the mandated OMB reviews, e.g., a statistical viable sample is reviewed, etc.

Insofar as the review for matching programs is concerned, Components need not respond. Computer Matching for the Department is centralized and the Defense Privacy Office, which has direct responsibility for the Department's matching program, shall address this part of the question.

Question 4. Does the Component have Privacy Impact Assessment (PIA) policies, a compliance policy to ensure that the Component is adhering to web privacy policies, and does the Component have machine-readable privacy policies for its public web sites?

The Office of the Chief Information Officer is the OSD office responsible for implementation of the privacy provisions of the E-Government Act of 2002, specifically section 208. It therefore has the lead for responding to Question 4. However, because some Components have been proactive in this area, this is an opportunity for the Component to discuss what it has done to meet the E-Gov privacy objectives. Therefore, Component Privacy Officials, as well as Component CIOs, shall identify established programs and any and all initiatives undertaken in this very critical area.

Question 5. Identify the number of Component information systems containing Federally owned identifiable information, identify how many require and have had a PIA conducted, and identify how many, if covered, have published a Privacy Act system of records notice.

Background: All IT systems do not contain identifiable information on individuals. This question is only directed at those IT systems, either within or without the Component IT Registry, containing information about U.S. citizens and resident aliens. A PIA is required whenever a new or a substantially altered IT system will collect, maintain, or disseminate information on such individuals unless the system is exempt from the PIA requirement pursuant to the E-Gov Act, as implemented by OMB. In addition, not all IT systems containing information about U.S. citizens and resident aliens are covered by the Privacy Act. IT systems are only covered when information about individuals is retrieved by the name of the individual or some other unique personal identifier. If so retrieved, a Privacy Act system of records notice must be published in the Federal Register giving notice as to the existence and character of the system.

In summary, not all IT systems contain identifiable information; but if they do, a PIA is required unless exempt. IT systems containing such information that is retrieved by a name or other identifier are covered by the Privacy Act, thus triggering the need for publication of a system of records notice in the Federal Register. In short, a PIA may be required, but a Privacy Act system of records notice may not be.

Attached for information purposes is a chart prepared by the DoD OCIO identifying the number of IT systems for each Component.

Questions 5a and c (first subpart). Identify the number of Component information systems having Federally owned information in an identifiable form and the number where such information is retrieved by name or unique identifier.

Only the system managers responsible for operating an IT system are in a position to advise whether an IT system contains identifiable information and whether that information is retrieved by an individual's name or some other unique personal identifier. When identifiable information is so retrieved, current DoD privacy policy mandates that the system manager, in coordination with the Component Privacy Official, create a Privacy Act system notice for publication in the Federal Register.

The OMB question requires that all IT systems be reviewed to ensure that those qualifying as Privacy Act systems of records have in fact published the mandated notices for their systems.

Component Privacy Officials should work with the Component CIOs to obtain the needed information to respond to the questions. At a minimum, systems identified in the Component IT Registry should be reviewed. It shall be submitted as part of its response to the privacy section of the FISMA report.

It is recognized that those Components having a significant number of systems may not, in the time permitted, be able to review each and every system it operates. It may be that the most that can be accomplished for this reporting period is to survey but a sampling of the systems with the intent of creating a mechanism by which this information can be collected for next year's report.

The Office of the Chief Information Officer has indicated that it is receptive to modifying its current collection processes to facilitate the collection of FISMA privacy FY06 data. This truly will be extremely helpful, not only to Component Privacy Officials in their efforts to identify all Privacy Act systems or records, but it will be valuable to IT system managers as it will ensure that they are taking steps to comply with existing law and regulation. The Defense Privacy Office will coordinate with the DoD CIO to establish a responsive FY06 data call for privacy.

But while it may not be possible for some Components to survey all their IT system, those Components that do not have a significant number of IT systems are in a position to conduct the review. Where so, and in consultation with the Component CIO, the IT systems should be reviewed and a determination made whether one or more of the systems (1) contain Federally-owned information in identifiable form (i.e., any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means) and, if so, whether one or more systems (2) constitutes a system of records as contemplated by the Privacy Act (i.e., information about an individual is maintained and retrieved by the individual's name or some other personal identifier (e.g., SSN)). Where a determination is made that the IT system contains identifiable information or constitutes a Privacy Act system of records, the Component must identify whether it is operated by the Component or a contractor. Though the OMB subquestion does not take into consideration that some IT and Privacy Act systems of records are hybrid systems, i.e., operated, in part, by both the Component and a contractor, each Component is asked to provide the number of Component only operated IT and PA systems, contractor only operated IT and PA systems, and hybrid systems.

Question 5b. Identify the number of Component information systems requiring a PIA and the number of PIAs that have been completed.

The Office of the Chief Information Officer is the OSD office responsible for implementation of the privacy provisions of the E-Government Act of 2002, specifically section 208. It therefore has the lead for responding to Question 5b. However, as was discussed in Question 4 above, Component Privacy Officials may possess information regarding the conduct of PIAs as Component PIAs should have been coordinated with the Component Privacy Official. To the extent that Components have such information, it shall be reported.

Question 5c (second subpart). Identify the number of Component IT systems for which a Privacy Act system notice has been published in the Federal Register.

Each Component shall review its Privacy Act system notices and determine how many were based on an IT information system. Where a notice (or notices) is (were) based on an IT system, the Component must identify whether it is operated by the Component or a contractor. As discussed above, each Component is asked to provide the number of Component only operated PA systems, contractor only operated PA systems, and hybrid systems.

As needed and required, Component Privacy Officials can obtain from the Defense Privacy Office a listing of those Component system notices that have been published for FY05.

Question 5d. Contact information on who prepared the response to this question.

Self-explanatory

Question 6. Does the Component use persistent tracking technology, and if so, was approval of such use documented, is the use annually reviewed, does the web site privacy policy contain language advising users about the tracking?

DoD CIO will respond to this question.

c. Internal Oversight

Question 1. Does the Component have policies regarding how the Component complies with information privacy laws and policies, and if so, when were they established?

This question appears to mirror the question posed in Part II, section a (Question 1) above, except the Component is asked to furnish the date the policies were created. While the earlier question primarily relates to participation, this question focuses on compliance. In responding to this question, the Component should be guided, in general, by the guidance set out earlier.

Question 2. If compliance deficiencies have been identified, do documents exist identifying corrective actions taken or planned, and if so, when were they created?

The question is contingent upon the Component identifying a compliance deficiency. If none were identified, the Component shall so advise. Identification of deficiencies is based, in part, on whether the Component has established compliance policies, procedures, and practices.

Question 3. Does the Component employ technologies that permit auditing of your systems to ensure that they are being operated consistent with stated privacy policies and practices?

The Component Privacy Official must coordinate with the Component CIO to determine what compliance technologies are used to ensure that IT systems are being monitored to ensure that they are being operated consistent with law and regulation. This question covers both IT systems that are subject to the PIA requirement but not the Privacy Act and those IT systems that are covered by both the PIA requirement and the Privacy Act notice requirement.

Question 4. To what extent is the Component Inspector General involved in program oversight of the Privacy Program.

Each Component shall identify those circumstances where it coordinates with its IG in the administration of its privacy program. To the extent the Component regulatory or other authority provides for IG involvement, the authority shall be identified. If such authority does not exist, each Component shall discuss to what extent, if any, the IG has been involved in the areas identified by OMB.

Question 5. Does the Component submit annual reports to Congress regarding its Privacy Program?

Under current law, the Department of Defense is not required to submit an annual Privacy Report to Congress.

Components need not respond to this question.

d. Contact information.

Self-explanatory.

Bureau Name	A.1.a. FY05 Programs		A.1.b. FY05 Total Systems		A.1.a. FY05 PIA Required		A.1.a. FY05 PIA Reviewed	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	% of Required Reviewed
Army			1139		22		4	18.2%
Army COE			14		2		2	100.0%
Navy			1098		14		5	35.7%
USMC			172		0		0	#DIV/0!
USAF			1477		61		46	75.4%
AFIS			2		0		0	#DIV/0!
CIFA			8		1		0	0.0%
DARPA			1		0		0	#DIV/0!
DCAA			2		0		0	#DIV/0!
DCMA			10		0		0	#DIV/0!
DeCA			11		0		0	#DIV/0!
DFAS			103		0		0	#DIV/0!
DHRA			9		2		1	50.0%
DISA			119		0		0	#DIV/0!
DLA			47		9		2	22.2%
DODEA			10		0		0	#DIV/0!
DODIG			2		0		0	#DIV/0!
DSCA			11		0		0	#DIV/0!
DSS			0		0		0	#DIV/0!
DTIC			3		0		0	#DIV/0!
DTRA			27		0		0	#DIV/0!
MDA			25		0		0	#DIV/0!
OSD (All)			13		0		0	#DIV/0!
OSD (CIO)			13		0		0	#DIV/0!
PFFPA			1		0		0	#DIV/0!
TMA			40		18		14	77.8%
WHS			16		5		0	0.0%
CENTCOM			0		0		0	#DIV/0!
EUCOM			0		0		0	#DIV/0!
JFCOM			0		0		0	#DIV/0!
JOINT STAFF			0		0		0	#DIV/0!
NORTHCOM			0		0		0	#DIV/0!
NORAD			0		0		0	#DIV/0!
PACOM			0		0		0	#DIV/0!
SOCOM			0		0		0	#DIV/0!
SOUTHCOM			0		0		0	#DIV/0!
STRATCOM			15		0		0	#DIV/0!
TRANSCOM			35		4		0	0.0%
Total			4423		138		74	53.6%