

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF NEW YORK

SUSAN B. LONG )  
 )  
 and )  
 )  
 DAVID BURNHAM )  
 )  
 Plaintiffs )  
 )  
 v. ) C.A. No. 5:5cv1522 (NAM/DEP)  
 )  
 OFFICE OF PERSONNEL )  
 MANAGEMENT )  
 )  
 Defendant )

---

**DECLARATION OF MICHAEL B. DONLEY**

---

I, Michael B. Donley, declare under penalty of perjury that the following information is true and correct to the best of my knowledge.

1. I am the Director, Administration and Management ("DA&M"), Office of the Secretary of Defense, and have held that position since May, 2005. As DA&M, I am the principal staff assistant to the Secretary of Defense for Department of Defense ("DoD") organizational and management planning. I also serve as the DoD Chief Freedom of Information Act ("FOIA") Officer responsible to oversee the Defense Freedom of Information Policy Office, which is responsible for implementation of the DoD FOIA Program to include issuance of agency wide policy guidance on FOIA matters. Additionally, my security responsibilities include oversight of the Pentagon Force Protection Agency, which is responsible for the antiterrorism, security, and law enforcement programs concerning DoD facilities within the National Capital Region.

Other positions I have held in the government include Deputy Executive Secretary and Director of Defense Programs on the National Security Council, Assistant Secretary of the Air Force (Financial Management and Comptroller), and Acting Secretary of the Air Force.

2. I am familiar with the procedures followed in responding to FOIA requests received by the DoD FOIA Office. I am also familiar with the subject litigation and the FOIA requests submitted by plaintiffs in this case. The statements in this declaration are based upon my personal knowledge, upon my review of information available to me in my official capacity, and upon my conclusions.

3. On October 8, 2004, February 4, 2005, June 13, 2005, and January 25, 2006, plaintiffs submitted five FOIA request to the Office of Management and Personnel ("OPM"), asking for the status and dynamics files contained within OPM's Civilian Personnel Data File ("CPDF"). These requests asked for six CPDF files: the March, June, and September 2004 and March, June, and September 2005 CPDF files. See Declaration of Gary Lukowski ("Lukowski Declaration"). OPM conducted a reasonable search of the CPDF files and withheld from release all information from these files with regard to DoD employees.<sup>1</sup> See Lukowski Declaration. OPM also forwarded copies of these requests to DoD for consultation, in accordance with DoD's specific request to OPM that OPM work with DoD on all FOIA requests seeking information pertaining to DoD employees. See Id.

---

<sup>1</sup> DoD has acted in a consulting capacity with OPM in regards to these FOIA requests and OPM, rather than DoD, conducted the search for the DoD records. OPM's thorough and reasonable search for these files is fully addressed in the Declaration of Gary Lukowski.

4. After reviewing these FOIA requests, the Department of Defense determined that it did not object to OPM releasing forty two separate data elements within the requested files.<sup>2</sup> However, DoD asked that OPM deny to plaintiffs the names, duty stations, and bargaining unit data elements from the CPDF database.

5. Prior to the events of September 11, 2001, personally identifying information of DoD personnel, except for those assigned to overseas, sensitive, and routinely deployable units, was routinely released by both OPM and DoD. Release of names and identifying information of personnel assigned to these types of units was, and continues to be, denied. Due to the national emergency declared by the President after the events of September 11, DoD reevaluated its policy of releasing personally identifying information of its employees, and no longer does so.

#### Withholdings Pursuant to Exemption 3

6. Some of the names, duty stations, and bargaining units are denied pursuant to 5 U.S.C. § 552 (b)(3), which allows for the withholding of information “specially exempted from disclosure by statute.” In this case, the applicable statute is 10 U.S.C. § 130b, which allows for the withholding of personally identifying information of DoD employees assigned to overseas, sensitive, or routinely deployable units. The statute defines personally identifying information as, among other items, the person’s name and duty address. Even though 10 U.S.C. § 130b does not specifically address the bargaining unit code element as qualifying for withholding, DoD also requested that OPM withhold this element when it is attached to the name of a DoD employee covered by this statute. These bargaining unit codes are in the public domain, and some of

---

<sup>2</sup> Forty two data files containing data elements have been provided to plaintiffs. These files are listed in the attached Vaughn Index.

them even can be obtained from the OPM internet website. A person in possession of these codes would then be able to identify specific duty locations and be in possession of information specifically exempt from release under Exemption 3.

Withholding of DoD Personnel Information for Individuals in Sensitive Occupations by OPM under Exemption 6.

7. In accordance with its data release policy, OPM has denied release of some DoD employee information within the CPDF; specifically, the names and duty stations of personnel within sensitive career fields, pursuant to 5 U.S.C. § 552 (b)(6). See Declaration of Gary Lukowski.

Withholding of DoD Personnel Information Pursuant to Exemption 6.

8. In addition to withholding names and duty stations for some personnel pursuant to Exemption 3 and under the OPM data release policy pursuant to Exemption 6, DoD asked OPM to withhold the names, duty stations, and bargaining unit data elements for all DoD personnel pursuant to 5 U.S.C. § 552 (b)(6).

9. Prior to the events of September 11, 2001, and the subsequent war on terrorism, the standing policy within DoD was to release lists of names of all DoD personnel who were not assigned to overseas, sensitive, or routinely deployable units. As stated above, release of names and identifying information of personnel assigned to these types of units was, and continues to be, denied in accordance with 10 U.S.C. § 130b.

10. For DoD, however, the attack on the Pentagon of September 11, 2001, instilled a new sense of personal vulnerability and created a need for greater security for DoD personnel. An example of DoD's response to this need for greater security is the

creation of the PFPA, whose Director reports to me. Through my association with PFPA, I have become more aware not only of the threats to DoD and its personnel, but also of the prevention, preparedness, detection, and response measures employed by PFPA in response to these threats. A key to the success of these measures is denying a potential or actual enemy information that such an enemy could use against our personnel. By killing more than 120 DoD personnel, civilian, military, and contractors at their place of work and injuring an estimated 100 more, the attack on the Pentagon made clear that all DoD personnel are potential targets of terrorist violence, regardless of what they do for DoD and regardless of where they are assigned. The threat of violence that all such personnel now face creates an extremely strong privacy interest for DoD personnel in their personal information that, when weighed against the virtually non-existent public interest in the requested information, justifies the use of Exemption 6 to withhold from release any information that could be used to identify and target them, including the information that plaintiffs have requested.

11. Within the DoD, many other extensive measures have been taken both within the United States and abroad to protect military and civilian personnel and their families against the modern threat posed by terrorists and other enemies of the United States. These protection measures include publicized efforts such as the introduction within DoD facilities of escape masks for all DoD personnel within the National Capital Region. Additional measures include military bases, which prior to 9/11 had been open to the public, now operating on a very restricted security basis and the implementation of a computer emergency notification system on the desktop computers of DoD personnel within the National Capital Region. These measures illustrate the awareness

on the part of DoD of the need for additional protection against current and future threats.

12. Because of the September 11 attacks and the war against terrorism, the Deputy Secretary of Defense issued a memorandum dated October 18, 2001 (Attachment to Exhibit 1) to all DoD components advising them that “[m]uch of the information we use to conduct DOD’s operations must be withheld from the public because of its sensitivity.” In light of this guidance, it was determined by one of my predecessors, Mr. David O. Cooke, that the practice of releasing lists of names and personally identifying information of DoD personnel not protected by 10 U.S.C. § 130b would identify personnel performing specific DoD missions that could allow enemies of the United States to target these individuals with the intent to harass, stalk, or cause harm in order to degrade the individual’s or group’s performance and thus threaten national and homeland security. Therefore, on November 9, 2001, Mr. Cooke issued a specific policy addressing the withholding of lists of names of DoD employees under the FOIA. See Exhibit 1. The new disclosure policy directs all DoD Components to deny requests under the FOIA for “lists of names and other personally identifying information of personnel currently or recently assigned within a particular component, unit, organization, or office within the Department of Defense.” Id. This policy was posted on the DoD FOIA website at the time it was published and is still available at <http://www.defenselink.mil/pubs/foi/withhold.pdf>.

13. As a general matter, federal employees do not give up all privacy rights by virtue of their employment by the federal government. By virtue of their work and DoD’s mission, DoD employees and their families are particularly vulnerable to harassment

and attack and therefore there is a heightened privacy interest in their identities, duty stations, and information, such as bargaining unit data elements, that can be used to identify duty stations. These individuals are often put in harm's way directly and indirectly. This is particularly true in a post-September 11, 2001, security-conscious world, in which terrorist attacks are no longer a matter of speculation or theory, but a reality against which we must take appropriate defensive measures. Even releasing information regarding specific duty stations or that could be used to identify duty stations of DoD personnel could provide terrorists and others seeking to do harm with potentially valuable information for planning and executing an attack on certain targets important to national and homeland security. The attack on the Pentagon showed that all DoD personnel at all duty stations, both within and outside of the United States, are potential targets for attacks and unwarranted and unwanted contacts as a direct result of the work they do. For instance, hostile enemy forces and terrorists, either foreign and domestic, armed with information regarding the number of DoD personnel who work at a particular DoD duty station could plan an attack on the duty station using either conventional or biological or chemical weapons so as to maximize the number of personnel killed or wounded. If these enemy armies or terrorists knew the grades and position titles of personnel in a particular duty station, they could design a plan of attack to kill or injure specific categories of personnel.

14. Further, the release of names, duty stations, and information that reveals duty stations of DoD personnel could enable hostile enemy forces and terrorists, foreign and domestic, to identify and target the DoD personnel and their families. Hostile enemy forces and terrorists armed with names, duty stations, and information that reveals duty stations could use information available on the Internet to determine the

home addresses of DoD personnel. They could then plan and carry out attacks on DoD personnel and their families in their homes. Similarly, the disclosure of names, duty stations, and information that can identify duty stations could facilitate harassment of DoD personnel and their families. To illustrate this point, although not directly attributed to terrorist activity, spouses of military personnel engaged in Iraq have received crank casualty notification calls from individuals posing as military notification personnel, and one spouse of a U.S. servicemember was approached at her home by an individual in an Army dress uniform and told that her husband had been killed in Iraq, when in fact he was not. See Exhibit 2. Releasing the personnel information plaintiffs have requested would potentially facilitate such harassment. Given the world security climate, DoD employees are at a heightened risk of endangerment and harassment. In these ways, providing the names, duty stations, or information that can identify duty stations of DoD employees makes these individuals and their families more vulnerable to attack, harassment, and unwarranted attention, whether it be to further military or terrorist purposes or merely to vent misplaced frustrations.

15. Mr. Cooke, the personnel within the DoD FOIA Office who helped him formulate this release policy, and another 24,000 DoD civilian and military personnel were in the Pentagon on September 11, 2001, and they realized what it means to be targeted for death simply because of the federal agency they work for and the building that they work in. In the wake of September 11, 2001, the DoD FOIA Office reevaluated the release of personally identifying information of DoD personnel, what they do, and where they can be found under the FOIA because this information can potentially aid

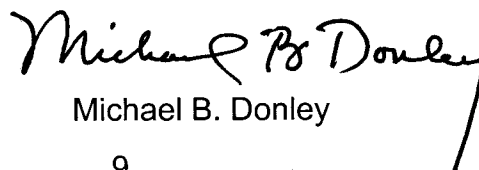


enemies of the United States. Therefore, the previously mentioned policy of November 11, 2001, was established.

16. The DoD applied Exemption 6's balancing analysis to this information. In making this Exemption 6 analysis, information of public interest was determined to be information which would shed light on the DoD's performance of its statutory duties. There is no discernable public interest in knowing the specific identities, duty stations, or information that can be used to identify duty stations of individuals employed by DoD. This information provides no meaningful information about government activities. In each category where information was withheld pursuant to Exemption 6 it was determined that the individual's very strong privacy interests, which were dramatically illuminated by the attacks of September 11, 2001, outweighed the virtually non-existent public interest in their identities, duty stations, and bargaining unit data elements, which shed no light on government activities. Because the national emergency declared by the President on September 14, 2001, is still in affect, the DoD policy to deny lists of names when they are requested under the FOIA is current.

I hereby declare under penalty of perjury that the matters and facts set forth in this Declaration fall within my official purview and, based upon my personal knowledge, information, and belief, are correct and true.

Dated this 6<sup>th</sup> day of June 2006, at the Pentagon, Arlington, Virginia.

  
Michael B. Donley

**DECLARATION OF MICHAEL B. DONLEY**

**EXHIBIT 1**



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



ADMINISTRATION &  
MANAGEMENT

November 9, 2001

Ref: 01-CORR-101

MEMORANDUM FOR DOD FOIA OFFICES

SUBJECT: Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)

The President has declared a national emergency by reason of the terrorist attacks on the United States. In the attached memorandum, the Deputy Secretary of Defense emphasizes the responsibilities all DoD personnel have towards operations security and the increased risks to US military and civilian personnel, DoD operational capabilities, facilities and resources. All Department of Defense personnel should have a heightened security awareness concerning their day-to-day duties and recognition that the increased security posture will remain a fact of life for an indefinite period of time.

This change in our security posture has implications for the Defense Department's policies implementing the Freedom of Information Act (FOIA). Presently all DoD components withhold, under 5 USC § 552(b)(3), the personally identifying information (name, rank, duty address, official title, and information regarding the person's pay) of military and civilian personnel who are assigned overseas, on board ship, or to sensitive or routinely deployable units. Names and other information regarding DoD personnel who did not meet these criteria have been routinely released when requested under the FOIA. Now, since DoD personnel are at increased risk regardless of their duties or assignment to such a unit, release of names and other personal information must be more carefully scrutinized and limited.

I have therefore determined this policy requires revision. Effective immediately, personally identifying information (to include lists of e-mail addresses) in the categories listed below must be carefully considered and the interests supporting withholding of the information given more serious weight in the analysis. This information may be found to be exempt under 5 USC § 552(b)(6) because of the heightened interest in the personal privacy of DoD personnel that is concurrent with the increased security awareness demanded in times of national emergency.

- Lists of personally identifying information of DoD personnel: All DoD components shall ordinarily withhold lists of names and other personally identifying information of personnel currently or recently assigned within a particular component, unit, organization or office with the Department of Defense in response to requests under the FOIA. This is to include active duty military personnel, civilian employees, contractors, members of the National Guard and Reserves, military dependents, and Coast Guard personnel when the Coast Guard is operating as a service in the Navy. If a particular request does not raise

Exhibit 1

security or privacy concerns, names may be released as, for example, a list of attendees at a meeting held more than 25 years ago. Particular care shall be taken prior to any decision to release a list of names in any electronic format.

- Verification of status of named individuals: DoD components may determine that release of personal identifying information about an individual is appropriate only if the release would not raise security or privacy concerns and has been routinely released to the public.
- Names in documents that don't fall into any of the preceding categories: Ordinarily names of DoD personnel, other than lists of names, mentioned in documents that are releasable under the FOIA should not be withheld, but in special circumstances where the release of a particular name would raise substantial security or privacy concerns, such a name may be withheld.

When processing a FOIA request, a DoD component may determine that exemption (b)(6) does not fully protect the component's or an individual's interests. In this case, please contact Mr. Jim Hogan, Directorate of Freedom of Information and Security Review, at (703) 697-4026, or DSN 227-4026.

This policy does not preclude a DoD component's discretionary release of names and duty information of personnel who, by the nature of their position and duties, frequently interact with the public, such as flag/general officers, public affairs officers, or other personnel designated as official command spokespersons.



D. O. Cooke  
Director

Attachment:  
As stated



DEPUTY SECRETARY OF DEFENSE  
1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

18 OCT 2001

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

SUBJECT: Operations Security Throughout the Department of Defense

On 14 September the President declared a national emergency by reason of terrorist attacks and the continuing and immediate threat of further attacks on the United States. As this Department assists wide-ranging efforts to defeat international terrorism, it is clear that US military and civilian service lives, DOD operational capabilities, facilities and resources, and the security of information critical to the national security will remain at risk for an indefinite period.

It is therefore vital that Defense Department employees, as well as persons in other organizations that support DOD, exercise *great* caution in discussing information related to DOD work, regardless of their duties. Do not conduct *any* work-related conversations in common areas, public places, while commuting, or over unsecured electronic circuits. Classified information may be discussed *only* in authorized spaces and with persons having a specific need to know and the proper security clearance. Unclassified information may likewise require protection because it can often be compiled to reveal sensitive conclusions. Much of the information we use to conduct DOD's operations must be withheld from public release because of its sensitivity. If in doubt, do not release or discuss official information except with other DoD personnel.

All major components in this Department to include the Office of the Secretary of Defense, the Military Departments, the Joint Staff, the Combatant Commands, the Defense Agencies, the DOD Field Activities and all other organizational entities within the DOD will review the Operations Security (OPSEC) Program, described in DOD Directive 5205.2, and ensure that their policies, procedures and personnel are in compliance. We must ensure that we deny our adversaries the information essential for them to plan, prepare or conduct further terrorist or related hostile operations against the United States and this Department.



U17477 /01

**DECLARATION OF MICHAEL B. DONLEY**

**EXHIBIT 2**

[BACK](#) [PRINT](#)

## Army Wife Claims Cruel Hoax

SAVANNAH, Ga., Feb. 23, 2005

(AP) Military police are investigating a cruel hoax in which a man wearing an Army dress uniform falsely told the wife of a soldier that her husband had been killed in Iraq.

Investigators are trying to determine why the man delivered the false death notice and whether he was a soldier or a civilian wearing a military uniform.

"We're taking it extremely seriously. Whatever motivation was behind it, it was a sick thing to do," said Fort Stewart spokesman Lt. Col. Robert Whetstone.

Last month, 19,000 soldiers from the Fort Stewart-based 3rd Infantry Division deployed for their second tour of duty in Iraq. At least eight division soldiers have been killed since then.

Fort Stewart officials would not identify the Army wife who reported to military police that a man posing as a casualty assistance officer came to her door Feb. 10.

"Right off the bat, she noticed some things were not right," Whetstone said. "The individual's uniform wasn't correct - there were no markings or name tags. Plus, the person was alone, and she knew one person does not make (death) notifications."

Whetstone said no similar hoaxes have been reported.

When the 3rd Infantry first deployed to Iraq for the 2003 invasion, some Fort Stewart families reported receiving phone calls from pranksters saying their soldiers had been killed.

This time around, troops and their spouses got pre-deployment briefings that included detailed explanations of how death notices work. Two soldiers, including a chaplain, in dress uniform always arrive to tell the family in person. The Army never makes notifications over the telephone.

Fort Stewart spouses have been spreading news of the latest hoax, said Army wife Michelle Dombrowski, who received an e-mail more than a week ago reporting the incident.

"I can't believe that someone would do that," said Dombrowski, whose husband, Staff Sgt. Joe Dombrowski, is deployed with the 3rd Infantry. "I know the protocol, though."

Military police described the suspected hoaxer as being 6-feet, 1-inch tall and about 180 pounds with black or brown hair and a pale complexion. He was reported to be driving a blue or green pickup truck with chrome wheels, oversized tires and a Georgia license plate.

By Russ Bynum

©MMV The Associated Press. All Rights Reserved. This material may not be published, broadcast, rewritten, or redistributed.

[Feedback](#) [Terms of Service](#) [Privacy Statement](#)

*Exhibit 2*