



WORLD **PRIVACY** FORUM

COMMENTS OF THE WORLD PRIVACY FORUM TO THE DEPARTMENT OF
HOMELAND SECURITY, OFFICE OF SECURITY

VIA FAX AND POSTAL MAIL

September 25, 2006

Hugo Teufel III,
Chief Privacy Officer
601 S. 12th Street
Arlington, VA 22202-4220

Marc E. Frey, Senior Advisor
Office of Security
245 Murray Lane, SW.,
Building 410, Washington, DC 20528

Re: Notice of Proposed Rulemaking for Department of Homeland Security Office of Security Implementation of Exemptions, ``Office of Security File System,' Docket Number 2006-0027.

Pursuant to the notice published in the Federal Register on September 12, 2006 regarding the Notice of Proposed Rulemaking ``Office of Security File System," the World Privacy Forum respectfully submits the following comments. These comments are focused on the proposed implementation of an exemption for the proposed new system of records.

The proposed system of records is the Office of Security File System. The docket numbers for the two Federal Register notices are DHS-2006-0025 and DHS-2006-0027. The Department of Homeland Security (DHS) agency proposing the system and accompanying exemption is the Office of Security.

The World Privacy Forum is a non-profit, non-partisan public interest research organization. It focuses on in-depth research and analysis of privacy topics, including topics in medical privacy, financial privacy, and other aspects of privacy.

I. Objection to a Commingled System of Records

According to the September 12, 2006 published notice:

This system contains records pertaining to numerous categories of individuals including DHS personnel who may be a subject of a counterterrorism, or counter-

espionage, or law enforcement investigation; senders of unsolicited communications that raise a security concern to the Department or its personnel; state and local government personnel and private sector individuals who serve on an advisory committee and board sponsored by DHS; and state and local government personnel and private sector individuals who are authorized by DHS to access sensitive or classified homeland security information, classified facilities, communications security equipment, and information technology systems that process national or homeland security classified information. The information in this system also relates to official Security investigations and law enforcement activities.¹

The principal objection to the proposed system is the establishment of a single system that combines records and functions that are not sufficiently similar and that are eligible for different exemptions and different routine uses. It would be more appropriate for the activities to be separated into two distinct systems.

Records in the proposed system fall into two broad and distinct categories. First, the system includes records about subjects of law enforcement investigations for several types of law enforcement investigations. An exemption for these records under (k)(1) [classified information] and (k)(2) [investigatory material compiled for law enforcement] is reasonable and appropriate.

Second, the system includes records of investigatory material compiled *solely* for the purpose of determining suitability, eligibility, or qualifications for federal employment, access to classified information, and other related activities. An exemption for these records under (k)(5) that protects the identity of a confidential source is reasonable and appropriate.

The problem is that the law enforcement records are not eligible for exemption under (k)(5). Even the Department of Justice's *Privacy Act Overview*² observes that "subsection (k)(2) does not include material compiled solely for the purpose of a routine background security investigation of a job applicant." (original emphasis). Records compiled for suitability purposes are not likely candidates for exemption under (k)(2). The Office of Security has one component responsible for personnel security, and that component does not engage in law enforcement activities. If it finds information that requires review by law enforcement officials, the personnel security component can refer the information to the law enforcement officials who operate a separate system of records eligible for the (k)(2) exemption.

Because the two activities are distinct, the commingling of the records in a single system will only result in confusion on the part of DHS staff and – especially – on the part of individuals who are the subjects of records in the system. That confusion may result in the denial of rights that the Privacy Act of 1974 was intended to grant. The obvious solution here is to have two distinct systems. Two separate notices will clarify for everybody the application of the available exemptions.

¹ 71 Fed. Reg. 53,609 (September 12, 2006).

² U.S. Department of Justice, *Overview of the Privacy Act of 1974, Ten Exemptions*, 2004 edition. <<http://www.usdoj.gov/04foia/1974tenexemp.htm>>.

II. The Proposed Exemption

The proposed exemption in its current form is inconsistent with the system notice. The system notice indicates that the proposed system of records will be exempt under (k)(1), (k)(2), and (k)(5). However, the proposed rule only mentions exemptions (k)(1) and (k)(2). The system notice and the proposed rule implementing the exemption are inconsistent. That inconsistency is legally fatal to the rule. Because of the deficiency, DHS will be obliged to go back to the start and to republish the rule in its entirety as a proposed rule. The deficiency cannot be corrected through adjustment of the final rule.

III. Routine Uses

We offer comments on two proposed routine uses. The first proposed use, routine use H, allows disclosure to congressional offices in response to an inquiry made at the request of the individual to whom the record pertains. Disclosure to a congressional office of the sensitive information likely to be contained in the proposed system of records (whether covering law enforcement or suitability records) should be made only with the written authorization of the data subject. Of course, if written authorization is obtained, then there is no need for the routine use at all. We propose that routine use H be eliminated in its entirety.

The second proposed routine use, routine use I, allows disclosures to contractors, grantees, experts, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records. Given the sensitivity and potential classification of the law enforcement information in this system of records, we cannot conceive of a circumstance in which a disclosure to a student would be appropriate.

We propose that the authority to disclose to students be eliminated from the system of records that includes investigatory material compiled for law enforcement purposes. Whether disclosure of suitability information to students can be justified appears to be a closer question, and we cannot assert with the same degree of assurance that students should also be eliminated from a suitability system. However, unless the Department has affirmative reason to know that disclosure of suitability records to students is a common practice, then the authority should be dropped from a suitability system as well.

The broader point suggested by the *student* language in the routine use is that the unthinking application of commonly employed routine uses to new systems of records is something that should be actively avoided. A second point is that commingling systems of record that should be separate and that should have separate routine uses often results in routine uses that are overly broad, inappropriate, or legally deficient. That appears to be the case here.

Every authority to disclose for this system of records should be intensively reviewed and only included if both *appropriate and necessary* to carry out an agency function. This suggested test should be over and above the statutory *compatibility* requirement for routine uses. Every routine use that is compatible may not be appropriate or necessary. A review of routine use I might also

find that disclosures of investigatory material compiled for law enforcement purposes to those working under grants and cooperative agreements are inappropriate.

IV. Proposed Exemption from Civil Remedies

The proposed rule would exempt the system from subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act. This exemption is only available by law to a system of records that is exempt under the (j) exemptions in the Act. No system of records subject only to any of the (k) exemptions is eligible for an exemption from the civil remedies in subsection (g). It makes no difference that an agency may exempt a system from some provisions of the Privacy Act under the provisions of subsection (k). The agency can still be held accountable under the civil remedies. The Department is without any statutory authority for the claim of an exemption from the civil remedies under subsection (g) for this proposed system of records.

Even though an exemption from civil remedies is available for some systems of records – albeit not this particular system – the Department should demonstrate its commitment to accountability and transparency by not invoking the exemption to subsection (g) for any system of records that is actually eligible to be exempt from the civil remedies. If the Department has violated the privacy rights of any individual, it should be willing to allow that individual to pursue the limited remedies provided by the Privacy Act of 1974. Any substantive exemption will still protect the Department against liability for the exemption provision, but an aggrieved individual will nevertheless have his or her day in court otherwise.

The claim of exemption is also deficient in another way. The proposed rule fails to offer any justification for the exemption as is required. This defect does not matter since the exemption is legally unavailable, but we note the deficiency anyway.

While the proposed exemption from civil remedies for the Office of Security File System is improper, we nevertheless note that the Department limited the exemption so that it applies only to the extent that the system is exempt from other specific subsections of the Privacy Act. While even this limited exemption is not available, we do applaud the Department for restricting the scope of the exemption as it has. It would be a bolder and better step to disclaim the exemption in its entirety.

Thank you for considering these comments.

Respectfully submitted,

Pam Dixon
World Privacy Forum
www.worldprivacyforum.org