



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

JUN 15 2005

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
(ATTN: ACQUISITION EXECUTIVES)
DIRECTORS, DEFENSE AGENCIES

SUBJECT: Release of Purchase Card Data to the Public Domain

In response to the terrorist attacks on the United States in the Fall of 2001 the Department revised its policies which implement the Freedom of Information Act. At that time, the decision was made to withhold lists of names and other personally identifying information of Department personnel in response to requests under the FOIA. In terms of the Department's purchase card program, this policy revision meant that the names of all program officials (to include cardholders, billing officials, and agency program coordinators) would not be released under a FOIA request.

However, this policy revision did not address the potential exposure of classified programs and organizations within the Department through non-name specific FOIA requests. In May of 2003, I requested a review by the Office of the Under Secretary of Defense for Intelligence to determine if the public availability of the organizational names and telephone numbers of all Departmental cardholders could pose a security risk to classified operations. The August 7, 2003 response provided by the Deputy Assistant Secretary of Defense (Security and Information Operations), attached, makes a persuasive case regarding the Operational Security risk posed by the release of detailed aggregated purchase card information provided by the Office of the Secretary of Defense.

Notwithstanding this guidance, the Department has a legal responsibility to provide a limited amount of publicly accessible information associated with each Departmental purchase card account. To this end, this memorandum authorizes the release of a limited amount of purchase card transactional detail to the public domain. Effective immediately, the Purchase Card Program Office is authorized to release the following transactional data at the installation, base, or activity level for non-classified card accounts:

- merchant category code
- transaction amount



- merchant name
- merchant city, state, zip, and phone
- transaction date (releasable 90 days after date)

The transaction date is not to be released until 90 days have passed from this date. This mirrors identical Department policy governing the release of DD350 data to FPDS.

Additionally, base commanders are reminded of the security risk created if unnecessary personnel information (e.g. card holder's names) is publicly available. If you have any questions, my point of contact for this matter is Mr. Dennis Hudner and he can be reached at dennis.hudner@hqda.army.mil or (703) 681-3315.



Deidre A. Lee
Director, Defense Procurement
and Acquisition Policy

Attachment:
As Stated



INTELLIGENCE

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

August 7, 2003

DPAP
LB 8/18
10: Purchase
Card Program
[Signature]

MEMORANDUM FOR DIRECTOR, DEFENSE PROCUREMENT AND
ACQUISITION POLICY

SUBJECT: Freedom of Information Request (FOIA)—Purchase Card Data

This memorandum responds to your May 27, 2003 memorandum, same subject, to the Under Secretary of Defense for Intelligence, asking if an exemption from the release of information on all DoD purchase cardholders could be justified by governing Departmental policy. The Department's policy on operations security (OPSEC) provides justification for an exemption in this case, as the release of organizational addresses and associated phone numbers of all DoD purchase cardholders could significantly increase the risk of adversaries being able to derive information about sensitive organizational elements and useful indicators of DoD intentions, capabilities, operations, or activities.

OPSEC is the systematic process by which the U.S. Government denies potential adversaries information by identifying, controlling and protecting unclassified information that provides evidence of sensitive Government activities. OPSEC in the Department of Defense is governed by DoD Directive 5205.2 and is based on policy established by National Security Decision Directive 298.

Given the size of the Joint Purchase Card database, redaction of information concerning cardholders in sensitive positions is not an acceptable option, in our view. Some of the risk of disclosing sensitive data comes from the ability to compare the data requested here with compilations of purchase card data that the recipient could obtain or develop from other sources. The differences identified by such comparisons could identify redacted data directly or could then be subject to further investigations from which information about sensitive organizational elements might be derived. Additional risk derives from the potential for incomplete or inconsistent redaction.

Further risk is associated with the fact that the databases that contain purchase card account and transaction information are vulnerable to collection and exploitation. Having information that identifies users, their organizations and their phone numbers would allow an adversary to target those specific operations and activities in which they have an interest. Data mining techniques could be utilized to identify deviations from previous or typical purchasing patterns or to recognize a pattern across multiple organizations. As the Joint Purchase Card is used in every part of DoD to support ongoing operations as well as garrison activities, some types of purchases may reveal

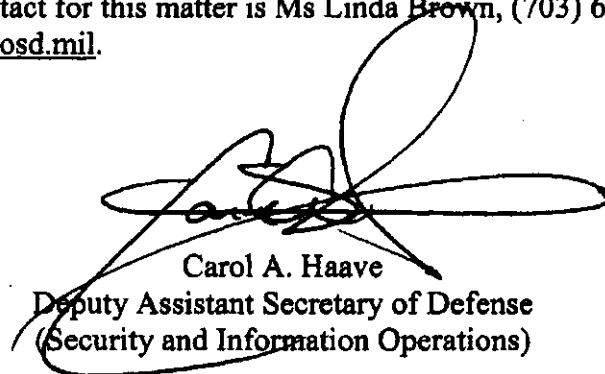


ongoing operations as well as garrison activities, some types of purchases may reveal sensitive or classified missions, intentions, limitations, or plans even though the individual purchases are not classified. When specific purchases can be connected to a specific organization and, by default, to a specific mission or location, those purchases may provide the adversary with enough information to refine their intelligence analysis of U.S. operations in a given area or regarding a specific mission.

Transactional risks can arise when financial institutions hire foreign nationals who in turn have access to account data; when accounting functions are moved to lower cost overseas locations; and when accounts are managed over networks that may also be vulnerable to exploitation. Additionally, some foreign countries require companies conducting credit transactions to provide copies of all transactions as a condition of operating in that country.

Even if much of the requested information is available by other means from other unclassified sources, from an intelligence point of view the information collected in that manner may lack credibility and may not be actionable. The same information provided directly by DoD not only has credibility, but also would be regarded by an adversary as reliable and could be actively used to gain insight into sensitive U.S. operations.

My point of contact for this matter is Ms Linda Brown, (703) 602-0929, or via e-mail at Linda.Brown@osd.mil.



Carol A. Haave
Deputy Assistant Secretary of Defense
(Security and Information Operations)