Privacy Impact Assessment
for the

COMMUNITY POLICING DISPATCH

Office of Community Oriented Policing Services

August 29, 2008

Contact Point
Chau Miles
Associate General Counsel, Legal Division
Office of Community Oriented Policing Services
(202) 616-9608

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Kenneth P. Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

The Community Policing Dispatch ("the Dispatch") is a monthly e-newsletter that will be freely available to the public on the COPS Office web site. The Dispatch will contain brief articles examining how community policing relates to different issues, overviews of promising practices from the field, and links to additional reading and resources. The Dispatch will also highlight upcoming events and trainings, and keep the public up to date about what is new and noteworthy at the COPS Office. The public will have the option to subscribe to the Dispatch e-mail list to receive e-mail reminders from the COPS Office notifying them that a new issue of the Dispatch is available online.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The COPS Office collects e-mail addresses directly from the public through a mail-to-link function on the Dispatch homepage. The submitted e-mail addresses will be included on the Dispatch e-mail list, and the COPS Office will send a monthly e-mail reminder to current subscribers.

1.2 From whom is the information collected?

E-mail addresses will be collected from members of the public who voluntarily subscribe to the Dispatch e-mail list on the COPS web site.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

E-mail addresses are being collected so that subscribers can receive monthly e-mail reminders from the COPS Office about the availability of new issues of the Dispatch e-newsletter on the COPS web site.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The COPS Office will use the e-mail addresses to generate a Dispatch e-mail list in order to send monthly reminders to subscribers notifying them about the availability of new issues of the Dispatch e-newsletter on the COPS web site. The e-mail reminders will also include a link to the Dispatch e-newsletter.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Access to information is limited to authorized COPS Office users responsible for managing the Dispatch e-mail list.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

None. Information will not be shared with external recipients.

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. Subscribing to the Dispatch e-mail list is voluntary and the public may unsubscribe at any time. The COPS Office will act promptly to honor unsubscribe requests. The public does not have to provide their e-mail addresses to access the COPS web site or the Dispatch e-newsletter

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Yes. Subscribing to the Dispatch e-mail list is voluntary. The public may subscribe to the Dispatch e-mail list by clicking on the subscribe icon on the Dispatch homepage, which will automatically direct the user to an e-mail screen. The user can then provide an e-mail address and send it to the Dispatch Outlook mailbox. By submitting the subscribe request, the user is consenting to the use of the e-mail address for e-mail reminders from the COPS Office about new issues of the Dispatch e-newsletter.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

The Dispatch e-mail list is a process of the existing certified and accredited COPS Management System (CMS), which includes our general support system. Access to the Dispatch

e-mail list is granted to internal users only and is limited to the Dispatch Group (Editor-in-Chief plus three Editors) and CMS Administrators.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes. The only contractors with access to the Dispatch e-mail list are authorized CMS Administrators. Their level of access is controlled by their assigned roles. Contractors are part of the general Department of Justice ITSS-3 support contract for IT services with Keane Federal Systems.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Roles are assigned according to a user's function and need. The Dispatch Group and CMS Administrators will have write-access to the Dispatch e-mail list based on their user roles and permissions.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The Dispatch e-mail list is covered by the Certification and Accreditation documentation for CMS which include: designating a managerial point of contact (Dispatch Editor-in-Chief) with authority to grant or remove users' (Dispatch Editors) access to the e-mail list; only CMS Administrators, subject to managerial approval, can change the security settings to allow or remove user access to the e-mail list; access to the e-mail list is promptly removed when a user leaves the organization; CMS Administrators conduct periodic review, verification and re-authorization of access rights to the e-mail list.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Roles, rules and access rights are verified manually by the Dispatch Editor-in-Chief and CMS Administrators (see Section 8.4 above) as well as automatically by the COPS computer operating system. Microsoft Windows Server allows COPS to designate groups and assign access rights to members of a group. The Dispatch Group will be added to the group account that is allowed to view the Dispatch e-mail list. Users who are not members of the Dispatch Group that attempt to access the Dispatch e-mail list will receive an error message.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Role-based privileges prevent the misuse of the Dispatch e-mail list and event logs are reviewed regularly according to the Certification and Accreditation documentation for CMS.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

There is no specific privacy training for the Dispatch e-mail list, but all internal COPS users undergo annual Computer Security Awareness Training (CSAT) and Rules of Behavior (ROB) training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. CMS, which supports the Dispatch e-mail list, has been Certified and Accredited. The last Certification and Accreditation was completed for CMS in July 2007 and will be valid until July 27, 2010.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The only potential privacy risk associated with the Dispatch is the unauthorized disclosure and use of e-mail addresses. This risk is mitigated by the following:

- Restrict access to information to a limited number of authorized personnel.
- Utilize password-protected systems requiring complex passwords with alpha-numeric and special characters that must be changed regularly.
- Provide annual Computer User IT Security and Rules of Behavior training.
- Maintain information in secured facilities with access limited to authorized users and escorted visitors.
- Limit physical access to the system through the use of guards and locked facilities requiring identification badges.
- Conduct robust anti-virus software management.

- Perform timely installation of security patches.
- Monitor network activity by reviewing event logs regularly.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

The Community Policing Dispatch ("the Dispatch") is a monthly e-newsletter freely available to the public on the COPS Office web site. The Dispatch provides information about community policing issues, upcoming events and trainings, and the latest COPS Office news. The COPS Office gives the public the option of subscribing to the Dispatch e-mail list in order to receive monthly e-mail reminders about new issues of the Dispatch online. Subscribing to the Dispatch e-mail list is voluntary and is not required to access the COPS Office web site or the Dispatch. The COPS Office protects subscribers against the unauthorized disclosure of their e-mail addresses through the use of appropriate physical and technological safeguards including restricting access to the information to a limited number of authorized personnel, collecting the information in password-protected systems and maintaining the information in secured facilities.

Responsible Officials

Deborah Spence
COPS Dispatch Program Manager

Darren Neely
COPS Chief Information Officer

Approval Signature Page

_____/s/_____

Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice