TESTIMONY
OF
HUGO TEUFEL III
CHIEF PRIVACY OFFICER
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT

UNITED STATES HOUSE OF REPRESENTATIVES

March 14, 2007

Introduction

Chairman Harman, Ranking Member Reichert, and Members of the Subcommittee, it is an honor to testify before you today on advancing information sharing while safeguarding privacy within the Department of Homeland Security State and Local Fusion Center Program. I am particularly pleased to be appearing with my colleague, Dan Sutherland. As the Subcommittee knows, his office and mine have a statutory responsibility to work together to address privacy as well as civil liberties issues in an integrated and comprehensive manner.

Because this is my first time appearing before the Subcommittee, I would like to introduce myself. I was appointed Chief Privacy Officer of the U.S. Department of Homeland Security by Secretary Michael Chertoff on July 23, 2006. In this capacity and pursuant to Section 222 of the Homeland Security Act of 2002, 6 U.S.C. § 142, my office has primary responsibility for privacy policy at the Department, to include: assuring that the technologies used by the Department to protect the United States sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information; assuring that the Department complies with fair information practices as set out in the Privacy Act of 1974; conducting privacy impact assessments of proposed rules at the Department; evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government; and preparing an annual report to Congress on the activities of the Department that affect privacy.

I also serve as the Department's Chief Freedom of Information Act (FOIA) Officer. In this role, I assure consistent and appropriate Department-wide statutory compliance and harmonized program and policy implementation. As you know, the three pillars of federal privacy law are the Privacy Act, the Freedom of Information Act, and the E-Government Act.

Prior to joining the Privacy Office, I served as the first Associate General Counsel for General Law at the Department of Homeland Security. Before joining the Department of Homeland Security, I served as the Associate Solicitor for General Law at the Department of the Interior. Therefore, I have had the honor of providing advice and counsel on freedom of information, privacy, and civil rights issues at two cabinet level agencies. As Associate General Counsel for General Law at DHS, Dan and my

predecessor as Chief Privacy Officer, Nuala O'Connor Kelly, were my clients, which provided me with the opportunity to understand the issues both offices faced.

There are two other things I should mention. As the Chief Privacy Officer, I currently hold a policy position in the Department, so I limit my practice of law to the weekends, when I serve as a judge advocate in the Army National Guard, within the Legal Support Office, attached to the District of Columbia Army National Guard. Additionally, in my spare time I have been working on a master's degree in National Security Studies through the Naval War College. My studies have aided me in understanding decision-making in the areas of homeland defense and security.

The Privacy Office

I am determined to continue the process of "operationalizing privacy" within the Department and its programs, a phrase described to this Subcommittee by Maureen Cooney, the Acting Chief Privacy Officer before my tenure.

To achieve this, the office forms close relationships with system owners and program managers, along with IT security officials, and senior DHS officials. By placing privacy into the program development and decision-making processes of the Department, we can ensure that DHS not only meets its legal requirements, but stands as a model of how privacy can complement and work with law enforcement and intelligence agencies.

As part of our ongoing operations, our Compliance group works with IT security, budgeting, procurement, and financial professionals Department-wide to complete privacy impact assessments, system of records notices, and other privacy documentation relevant to and required for DHS systems and programs.

Our Office also leverages the considerable experience of our International group to develop and maintain DHS's privacy policy and practices on issues concerning our foreign partners and allies. These issues range from international compliance measures to data sharing initiatives as well as full treaty negotiation and review.

Fusion Centers

State and local authorities have created 42 fusion centers around the country. Fusion centers blend relevant law enforcement and intelligence information analysis and coordinate security measures in order to reduce threats in local communities. They also represent a method for providing first responders with "actionable intelligence"; that is information useful and relevant to the day-to-day mission of state and local law enforcement personnel. As of the end of FY 06, the Department of Homeland Security has provided more than $380 million to state and local governments in support of these centers.

Intelligence Officers from the Department of Homeland Security Office of Intelligence and Analysis currently work side by side with state and local authorities at twelve fusion centers across the country.

This number is about to grow. On September 12, 2006, Secretary Chertoff told the Senate Committee on Homeland Security and Government Affairs that, "Our goal is to have intelligence and operations personnel at every state and major metropolitan fusion center in the United States, sitting in the same room, sharing and analyzing information and intelligence in real time," with a "two-way flow [of information], with every level of government pooling intelligence."

This ramping up of fusion centers and the two-way information flow to accompany it will require additional effort and vigilance to ensure privacy rights are

protected. As the DHS Chief Privacy Officer, I will strive to make sure privacy concerns are addressed at the beginning of the process, before information is collected and shared. This process begins, in my opinion, with a proposed fusion center utilizing the Department's fusion center guidelines.

Privacy and the Fusion Center Guidelines

The Global Justice Information Sharing Initiative, the Department of Homeland Security, and the Department of Justice collaboratively developed and in August 2006 issued "Fusion Center Guidelines: Developing and Sharing Information in a New Era." These guidelines are intended to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination, strengthened partnerships, and improved crime-fighting and anti-terrorism capabilities. The document offers a comprehensive guide to the development and operation of fusion centers, as well as provides useful resources and document templates to facilitate implementation. I believe this is an excellent first step in ensuring fusion centers integrate privacy protection into their actions.

Implementing these fusion center guidelines provides an important first step in applying appropriate privacy protections as required under the "Guidelines to Ensure that the Information Privacy and other Legal Rights of Americans are Protected in Development and use of the Information Sharing Environment" – otherwise known as the ISE Privacy Guidelines – and is a major focus of the ISE Privacy Guidelines Committee (ISE/PGC), of which I am a member. In fact, the ISE/PGC already formed a working group to deal specifically with privacy issues surrounding the exchange of data with state and local entities. Since the fusion centers will be the primary mechanism for federal government information sharing with our state, local and private sector partners, the successful implementation of appropriate privacy policies will be a critical part of ensuring the success of the Information Sharing Environment.

Privacy concerns and methods of addressing them appear throughout the documents. Fusion Center Guideline 3, for instance, urges the inclusion of a privacy committee in the fusion center governance structure. The purpose of this privacy committee will be to "liaise with community privacy advocacy groups to ensure civil rights and privacy protection." Fusion center governing bodies, moreover, are encouraged in this Guideline to collaborate with the Department of Homeland Security, including the Privacy Office, to establish their operating processes.

Fusion Center Guideline 5 urges fusion center partners to utilize memorandums of understanding (MOUs) to govern interactions between the participants, and commit the parties to the principles and policies of the fusion center. The guideline advises that adherence to privacy and security principles should be specifically addressed within all such MOUs. Where DHS shares personally identifiable information with fusion center partners, the Privacy Office will review and approve a Privacy Impact Assessment that covers the privacy and security controls that the MOU must address.

Fusion Center Guideline 8 is dedicated to promoting meaningful and lawful privacy policies at the fusion centers, and to providing mechanisms ensuring that the centers adhere to these policies. This begins with consideration of the Fair Information Principles which are the worldwide baseline for privacy protection: Transparency, Individual Participation, Purpose Specification, Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing – consideration of

which are also, appropriately, required by the ISE privacy guidelines. The Fusion Center Guidelines provide a useful list of complementary elements for the drafters of the privacy policy, including:

- Add introductory language that clearly states the privacy practices of the center;
- Describe the information collected and how the information is stored;
- Establish a common lexicon of terms for dealing with role-based access;
- Define and publish how the information will be used;
- Draft a clear, prominent, and understandable policy;
- Display the privacy policy for both center personnel and customers;
- Ensure that all other policies and internal controls are consistent with the privacy policy;
- Establish a business practice of notifying government agencies of suspected inaccurate data;
- Adhere to applicable state and federal constitutional and statutory civil rights provisions;
- Partner with training centers on privacy protection requirements and conduct periodic privacy security audits;
- Consult with the privacy committee (established pursuant to Guideline 3) to ensure that citizens' privacy and civil rights are protected;
- When utilizing commercially available databases, ensure that usage is for official business and the information is not commingled with private sector data. To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data; and
- Determine if there are security breach notification laws within the jurisdiction and follow those laws, if applicable.

Having defined the key elements of a sound privacy policy, the rest of Guideline 8 focuses on the steps the leaders of the fusion center should take to ensure the policy is followed. These steps include such prudent steps as ensuring adequate training and information privacy awareness and establishing a policy for tracking and reviewing privacy complaints and concerns. Guideline 8 also recommends seeking legal counsel. I would only add to this list that participants should also consult frequently with their entity's Chief Privacy Officer.

The supplemental materials available on the Guidelines' companion CD are particularly useful. They include the Justice Department's *Privacy and Civil Rights Policy Templates for Justice Information Systems*, Privacy Policy Templates, and a *Privacy Policy Development Guide*.

The *Privacy Policy Development Guide* recommends that in addition to the development of a comprehensive privacy policy, fusion centers complete privacy impact assessments to understand the effect that technology and operation choices have on privacy. The Privacy Office developed a detailed methodology to analyze the impact any new or update system will have on an individual's personal information, including reviewing:

- What information is to be collected;
- How will be it stored, managed, and used;
- What means of individual access is available;

- What means of redress for informational errors has been provided; and
- What security is in place to protect the information.

The Privacy Office's official guidance on the writing of privacy impact assessments to shepherd the different system programs safely through the privacy protection process serves as an appropriate addendum to the Fusion Center Guidelines.

Furthermore, it is often said that "security concerns become privacy problems." Privacy protection principles are only meaningful if they exist in tandem with a robust security regime. Fusion Center Guideline 9 provides a framework for ensuring adequate security measures are in place. This includes, of course, security for facilities, data, and personnel. A fusion center's Privacy Officer and Civil Rights Officer must have close working relationships with its Chief Information Officer as well as the Chief Security Officer.

As a whole, I believe these guidelines provide an invaluable resource for the principals to utilize when founding and operating a fusion center, and will also be helpful to me, as a member of the ISE Privacy Guidelines Committee, in monitoring how privacy is safeguarded in this crucial aspect of the Information Sharing Environment. The Fusion Center Guidelines encourage consideration of privacy interests from the very moment of formation – a critical step.

Privacy Office's Review of the MATRIX Program

Information sharing, of course, is at the heart of fusion center activities. The Privacy Office has had an opportunity to review a pilot information sharing program among a number of state governments called MATRIX, the Multistate Anti-Terrorism Information Exchange. The program accessed only state-owned or publicly available records that were already available to law enforcement without a subpoena or court order. DHS became involved in the pilot in July 2003, when (what is now) Grants and Training entered a Cooperative Agreement with a non-profit entity to administer the project. The funding was intended to assist with testing the system for data analysis and integration of terrorist threats and other intelligence information, as well as to provide funding to establish user accounts for MATRIX participants and to create a secure website for each participating state to facilitate information sharing.

The Privacy Office reviewed the program following a request by the American Civil Liberties Union and published its findings in a report entitled, "Matrix Report – DHS Privacy Office Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project," which is available on the Privacy Office website.

We found that the project lacked a privacy policy that clearly articulated the project's purpose, how it would use personal information, the types of information covered, and the security and auditing safeguards governing the project. The MATRIX Board of Directors did not issue a privacy policy of any kind until four months after the pilot began. It was nearly a year before the Board approved an audit requirement and then it merely called for a self audit.

The Privacy Office believes, however, that the MATRIX pilot project was undermined, and ultimately halted, in large part because it did not have a comprehensive privacy policy from the outset to provide transparency about the project's purpose and practices and protect against mission creep or abuse. The recommendations of the Privacy Office rest on the basic premise that information programs such as the MATRIX

pilot project can protect privacy, while securing the homeland. Building privacy into the architecture of an information program can help ensure that such programs achieve their objectives while at the same time safeguarding individual privacy. This is more than just a compliance issue. The Privacy Office understands that sound and effective privacy practices maximize the utility of the information collected, processed, and maintained by DHS to facilitate and improve performance, while minimizing the cost to agencies and to the public.

I note that the MATRIX program was initiated and failed before the fusion center guidelines were issued. If the MATRIX participants had had the benefit of these guidelines and followed their plan for implementation and the creation of a comprehensive privacy policy, I am confident that the program would have stood a much better chance of success. Looking forward, I hope parties entering future information sharing agreements, especially in support of fusion centers, read the MATRIX report for its lessons learned and then review and adopt the Fusion Center Guidelines. And of course they should consult their Privacy Office.

Conclusion

I thank the Subcommittee for this opportunity to testify. My office looks forward to working with the Department and our fusion center partners to ensure they maximize their effectiveness by establishing sound privacy practices.

I look forward to hearing my colleagues' testimony and to answering your questions.