

**STATEMENT OF SUZANNE PECK,
CHIEF TECHNOLOGY OFFICER,
DISTRICT OF COLUMBIA GOVERNMENT
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
OF THE
GOVERNMENTAL REFORM COMMITTEE,
UNITED STATES HOUSE OF REPRESENTATIVES
ON FACILITATING AN ENHANCED INFORMATION SHARING NETWORK
THAT LINKS LAW ENFORCEMENT AND HOMELAND SECURITY FOR FEDERAL,
STATE AND LOCAL GOVERNMENTS**

Introduction

Good afternoon, Mr. Chairman and members of the Subcommittee. My name is Suzanne Peck. I am the District of Columbia Chief Technology Officer, leading the Office of the Chief Technology Officer (OCTO), the central information technology and telecommunications agency of the District of Columbia government. I'm pleased to testify today on the District's efforts to develop an enhanced information sharing network that links law enforcement and homeland security for multi-jurisdictional use.

Our initiative in this area is appropriately named SHIELD, and I'll describe it below. It's important, however, that you understand SHIELD in context. It's just one of an integrated suite of District initiatives for local, regional, and federal public safety and domestic preparedness that focus on data exchange, data presentation, data transportation, and data consolidation.

Data Exchange

Our first objective is to build a public safety and criminal justice data sharing system that easily integrates data using only open-standard components and can be easily and quickly replicated by other jurisdictions. This initiative is underway under the name SHIELD (Securing the Homeland by Integrating Existing Local Databases).

We launched SHIELD, with partners in New York City, Pennsylvania, Maryland, and Virginia, to address a long-standing problem that has become more acute since September 11, 2001: Regional homeland security and criminal justice data exchanges are either non-existent or rely on awkward, non-standard, person-to-person communications, even inefficient manual processes. No one can “connect the dots” in a way that helps prevent crime and anticipate terrorist attacks.

SHIELD is designed to solve the problem by connecting existing local criminal justice, public safety, and courts information regionally and nationally, in real time, without compromising the security of the data and without rebuilding existing systems. To give you an idea how SHIELD works, I’ll describe the local data sharing program, JUSTIS, that is one partner in SHIELD and the model for it.

In the District, even before September 11, 2001, data sharing between public safety and criminal justice agencies was essential, but also very complex because local and federal entities operate, literally and figuratively, in the same territory. Before JUSTIS, interagency attempts at sharing arrest and court records were ad hoc. Some were literally by “sneaker network.” To complicate matters, District agencies were at very different levels of technical development; as of early 1999, one had just been weaned off rotary telephones.

In 1999, the heads of several justice agencies drew up a brief agreement that recognized their common need to share data securely. The resulting body, the Criminal Justice Coordinating Council, consists of the heads of 15 District and federal agencies and departments, ranging from Washington Mayor Anthony A. Williams to Kathleen Hawk Sawyer, director of the Federal Bureau of Prisons. The Council sponsored the development of JUSTIS as a secure Web site on which law enforcement agencies could share data regardless of their IT prowess. Today,

participating agencies make a secure browser connection to a dedicated JUSTIS server owned by the District government. JUSTIS pulls data from other agency databases without making any changes to the original data stores. The system automatically highlights two entries that appear to be the same but have some minor differences, such as inconsistent birth dates. JUSTIS flags the later of the two records. The Criminal Justice Coordinating Council provides overall project governance and oversight through monthly meetings. Its IT advisory council handles technical issues.

SHIELD builds on JUSTIS and similar systems in its partner states by allowing them to share public safety, criminal justice, and homeland defense data with each other. The mission of SHIELD is provide access to available, unrestricted public safety and justice data from a partnership of independent city, state and regional information systems, through a secure access methodology, allowing justice and homeland security officials to accomplish comprehensive analyses and to make better informed decisions.

I'll borrow a succinct explanation of the project from the National Governors Association (NGA), which recently described the project this way:

“In response to the terrorist attacks of September 11, 2001, ... States have taken the initiative to partner and develop regional information sharing projects. One of the more innovative and promising regional approaches to information sharing is the ... SHIELD project. SHIELD connected the critical homeland security information of New York City, Pennsylvania, Maryland, Virginia, and the District of Columbia across law enforcement, public safety, and justice agencies.

“The driving assumption of SHIELD is that the majority of necessary components for effective regional information sharing systems already exist within state and local jurisdictions.

“SHIELD project partners link existing information systems from public safety, law enforcement, and justice agencies within their jurisdictions - information that’s not readily available beyond the local level. SHIELD capitalizes on existing local funds, commercial workstations, and Internet browsers/Internet technologies to share data real-time and across multi-jurisdictional boundaries. Since SHIELD leverages existing resources, project partners can expand rapidly at little or no monetary cost.

To add to this summary, I’d like to emphasize a couple of points. First, SHIELD is easy for participating agencies and officials to use and to learn. The key tool users need – and the only tool they need -- is their web browser. With a single inquiry, an authorized user can access all sets of data from all SHIELD partners’ databases – including both documents and images. Second, SHIELD is a data sharing system and only a data sharing system. SHIELD itself collects no data. Participating agencies individually control the data they contribute and which users may access it.

Finally, the last point in the NGA summary bears repeating: “Since SHIELD leverages existing resources, project partners can expand rapidly at little or no monetary cost.” That means that, although SHIELD’s initial scope is regional, it can easily be expanded to national scope. Secure technology could allow SHIELD to be accessed virtually anywhere in the United States – so SHIELD can easily serve as the first step toward a national network for public safety and justice data sharing.

For that reason, we're seeking a modest investment in SHIELD – \$4.465MM -- from the Department of Homeland Security (DHS). With DHS's help, national information sharing of local criminal justice, public safety, and homeland defense information can occur on an accelerated schedule that calls for an initial 100-day detailed design, blueprint, and user ratification effort, followed by a 3-6-month hub implementation with partners in the National Capital Region. The modest investments we're seeking can and will pay national dividends.

Data Transport

Our second objective is to build a broadband network over which to drive shared criminal justice, public safety, and homeland defense data, both regionally and nationally. We have several programs to address this goal.

One program involves implementing secure Internet connections using existing components such as browsers, ISP connections, and commercially available authentication tokens.

Another key initiative is a pilot broadband public safety network that will allow us to transport real-time video streaming data from incoming sites to central command centers. OCTO has obtained an experimental license from the Federal Communications Commission (FCC) to deploy, on a pilot basis, the nation's first citywide broadband public safety wireless network in the 700 MHz band. The pilot network, to be completed in August 2004, will incorporate 10 broadband broadcast sites distributed throughout the city. The network will be city-owned and will replace current commercial wireless usage. It will provide for the nation's capital, and demonstrate for the nation, next-generation public safety wireless applications such as real-time street crowd monitoring, citywide simulcast emergency alerts, on-line medical consultations and pre-admissions assessments during ambulance trips, video pre-assessment capabilities for police

officers en route to crime and emergency scenes, and chemical and biological alarms in the regional Metro subway system.

Our pilot broadband network will benefit first responders in every city and state in the U.S. by laying the foundation for their access to broadband applications. At the same time, the District's pilot broadband network will provide states and cities across the nation a replicable solution to their needs for more effective and versatile public safety and emergency management capabilities.

In a third and related initiative, OCTO has assembled and is leading a national coalition of states, cities, and counties called the "Spectrum Coalition." Its members are listed in Attachment 1. The coalition's mission is to advocate national legislation that would dedicate spectrum in the 700 MHz band for the use of public safety agencies so that they will have access to enough wireless spectrum to support wireless public safety applications. With the enactment of the Spectrum Coalition legislation, every jurisdiction in the U.S. will have the wireless spectrum necessary to deploy a complete arsenal of public safety, emergency management, and homeland defense communications tools.

Still another District data transportation effort is our participation in the Capital Wireless Integrated Network (CapWIN) project, a partnership between Maryland, Virginia and the District to develop an integrated transportation and criminal justice information wireless network. This unique project will integrate transportation and public safety data and voice communication systems in two states and the District of Columbia and will be the first multi-state transportation and public safety integrated wireless network in the United States. The primary goal of the project is to have multiple mobile data platforms communicating seamlessly across the network regardless of their jurisdiction or geographical location. These CapWIN end-

users include federal, state and local police, fire, and EMS vehicles as well as state Department of Transportation service patrols.

The project is proceeding in multiple phases. The strategic planning phase is completed, and the project's strategic plan can be found on the CapWIN website, www.CapWINproject.com. The implementation phase is currently underway. A continuous development and expansion phase follows.

A pilot test was conducted during the strategic planning phase of the project. The pilot included twenty-two (22) in-vehicle mobile computer systems that allowed messaging between police vehicles in Maryland, Virginia and Washington, D.C., transportation vehicles in Maryland and Virginia, and local fire vehicles. These mobile platforms and other developmental transportation and public safety systems were successfully interfaced during the pilot project.

Like SHIELD and our pilot wireless data network, CapWIN offers national benefits. The project will have national implications in technology transfer, including image/video transmission and the inclusion of transportation applications in an integrated system. National observers will be able to monitor the progress and development of the system during the evolution of the project. Potentially, CapWIN can become the foundation for networks throughout the United States and other countries.

Data Presentation

We can enhance the uses, and usefulness, of the data we share and transport by presenting it in innovative ways. The District's DCSTAT system meets this need. DCSTAT offers both daily and near real-time capabilities to collect, organize, report, and map data for use by local, regional, and federal agencies in the National Capitol Region (NCR). DCSTAT presents data from many sources, spanning numerous agencies, and has been designed with a

particular focus on targeted users and opportunities, using a novel blend of technologies including: EAI-based database linkage, data warehousing, Geographic Information Systems, and business intelligence. DCSTAT serves many regular government management functions; here's how the system can be enhanced to support emergency preparedness and management.

At the outset of an emergency event, there is often a time gap between reporting of seemingly unassociated incidents and recognition by public safety officials that they form a pattern of broader public threat. The more rapidly the awareness of a threat and its nature emerges, the faster we can launch an appropriate response. The goal of DCSTAT is to improve the speed at which government agencies recognize and react to public threat events. This project will transform real time information into actions by: accelerating the flow of information between many surveillance sources and recipients, applying spatial proximity analysis to analyze incoming incidents, and using meaningful presentation techniques to reveal subtle patterns.

Currently DCSTAT provides forensic-oriented analysis, collecting and publishing data sets on a 24 hour basis suitable for assisting management of day-to-day city services. For domestic preparedness and emergency management, we'll incorporate a much shorter data refresh time interval. Fortunately, incorporating real time data collection from emergency surveillance systems is a natural extension of existing DCSTAT capabilities. For example, by connecting to and aggregating real-time information, DCSTAT will be able to expand its existing "Watch and Alert" functions into monitoring incident data and triggering notifications to senior management when a pre-identified risk threshold is reached.

The DCSTAT architecture uses state-of-the-market technologies in an information systems model that supports homeland security and domestic preparedness goals by providing an early warning system for detecting and managing unfolding incidents as they emerge. Users will

be better able to predict, recognize and manage major emergency events, more efficiently deploy emergency management resources, and ultimately reduce loss of life and property.

Like the other initiatives described here, DCSTAT can be replicated by other jurisdictions for emergency preparedness and management – and a multitude of other day-to-day management purposes.

Data Coordination

It's critical to effective homeland defense that first responder and emergency management agencies coordinate data, planning, and deployment. Our Unified Communications Center (UCC) will serve this goal. The UCC is a 127,000-square-foot building on the East Campus of St. Elizabeths Hospital in Ward 8 where the District will consolidate the emergency communications functions of the District's police, fire/EMS, and emergency management agencies, our traffic management function, and our 911 emergency, 311 non-emergency, and 727-1000 citizen service call centers. In addition, the UCC will play a key homeland defense role, serving as the District's Emergency Operations Center during major local events and emergencies, as well as the Regional Incident Communication and Command Center (RICCC). The RICCC will facilitate communication and coordination among local, state and federal authorities for effective and timely response to regional and national emergencies.

Because of its vital public safety and homeland defense functions, the UCC is equipped with a state-of-the art telecommunications infrastructure and security features appropriate to our status as the nation's capital. The UCC is designed to GSA security standards, incorporating features such as a 100-foot setback and berms, blast- and bullet-resistant glass, monitors and security cameras, controlled access, security check points, turnstiles, bollards, and tamperproof exterior windows and doors.

Conclusion

Together, the District of Columbia initiatives I've described address the public safety and criminal justice data sharing, transportation, presentation, and coordination needs that have become critical and urgent for the nation's capital since September 11, 2001. Most important, as the nation's capital, we have designed each of these programs to be quickly, easily, and inexpensively expanded to local, regional, and federal agencies and jurisdictions throughout the nation.

SPECTRUM COALITION MEMBERS

City of San Diego
U.S. Park Police
State of Delaware
Washington, D.C.
City of Phoenix
City of Denver
CapWIN
Montgomery County, MD
Region 25 (Montana)
700 MHz Regional
Planning Committee
State of Texas
State of Arizona
City of Philadelphia
Broward County, FL
Rocky Mtn. EDACS User Group
· Aurora, CO
· Westminster, CO
· Arvada, CO
· Lakewood, CO
· W. Metro Fire District, CO
· Denver International Airport
· Rocky Flats, CO
Fairfax County, VA
State of Oregon (SIEC)
State of Washington (SIEC)
San Mateo County, CA
State of Ohio
State of Ohio (SIEC)
State of Rhode Island
Los Angeles Co. Sheriff's Dept.