

# Public Safety

FIRE • POLICE • EMS • JUSTICE • COMMUNICATIONS

TECHNOLOGY SOLUTIONS FOR EMERGENCY MANAGEMENT & HOMELAND SECURITY

## Interagency data sharing in a secure environment evolving

By Debra Cohen

The public safety data information sharing arena, from the local level to the federal level, has truly evolved. Local law enforcement agencies are sharing more information with neighboring jurisdictions, regional, state and federal justice agencies. Federal grant-making agencies, once funding data-focused projects implemented in information silos, are mandating that grant recipients creating or expanding data-sharing systems use XML. The development of IEPDs (Information Exchange Package Documentations) has allowed federal, state and local agency data-sharing initiatives to expand exponentially. Global Justice XML Data Model (GJXDM) has grown into the National Information Exchange Model (NIEM). Fusion centers warrant their own annual conference. This short list represents a mere tidbit of the many changes we've seen in interagency data sharing over the past 10 years. The message is clear: Share and share alike with all of your stakeholders for the common good of public safety and national security.

Yet, we have many miles to go before we sleep securely. The complexities of multi-agency data sharing have left open an array of data security and privacy issues that need to be addressed in order for the full capabilities and maximum benefits of data sharing to be realized. Take, for example, NIEM. The value of NIEM as an information-shar-

ing framework grows proportionately with the number of agencies that use it. However, if agencies do not feel secure in sharing their data, then no amount of "for the common good" persuasion is going to convince them otherwise.

Secure data sharing was the subject of one of the presentations given at the recent International Association of Chiefs of Police 33rd Annual Law Enforcement Information Management Training Conference and Exposition (LEIM) held in Dallas. In a joint presentation by the U.S. Department of Justice Office of Community Oriented Policing Services (COPS Office) and SEARCH, the National Consortium for Justice Information and Statistics, "Options for Interagency Data Sharing in a Secure Environment" examined ways that law enforcement agencies could securely share data locally, regionally and nationally. The session focused on efforts and initiatives being undertaken to help agencies ensure that their data's integrity, privacy and security remain uncompromised as they join the data pool filled with information from partner agencies.

After a presentation by the COPS Office on technology resources, Jim Douglas, the justice information specialist for SEARCH and chairman of the Global JRA Service Task Team, began to share best practice recommendations that his organization had provided to recipients of COPS FY07 Technology Program grants.

In FY07, the COPS Office awarded 37 jurisdictions a total of \$159 million in grants under its Technology Program for the procurement of technology that could increase the ability to share data and enhance voice interoperability with regional, state and federal partners. These multi-jurisdictional and multidisciplinary projects ranged from those focusing on CAD, RMS, and mobile data systems to radio systems and data sharing.

To support its FY07 Technology Program grantees and help make their projects successful, the COPS Office also provided a series of training and technical assistance opportunities through SEARCH, its non-profit training and technical assistance provider. The offerings included a post-award Kickoff Conference, Advanced Training Workshops, and tailored, direct onsite and remote technical assistance. Part of this assistance includes SEARCH working directly with grantees and recommending techniques that can help them overcome challenges in data sharing, particularly those regarding information security and privacy.

The COPS Office views training and technical assistance efforts as benefiting grantees and other agencies as well through the lessons gleaned from grantee experience. Conferences such as this year's LEIM provide one vehicle for sharing lessons learned with all agencies engaged in multi-agency data-sharing projects.

## Interagency data sharing in a secure environment evolving *(continued)*

Douglas said information sharing means that information gets to the right people at the right time securely and honors privacy requirements. Further, he said that clearly defined and institutionalized rules, roles, responsibilities, and standards are necessary to ensure effective information sharing. He discussed several options to minimize vulnerabilities in multi-agency data sharing, including strategies to ensure information privacy and security.

For example: Plan, plan and then plan some more. Conducting information technology risk assessments and developing sound information security policies governing who uses the data and toward what purpose are minimal steps you can take. The Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies (2006) is one of many resources freely available and designed to assist agencies in developing security policies for protecting sensitive data such as case reports, confidential investigative data, agency intelligence, crime data and personnel information. This guide includes tips, checklists and risk assessment tools, such as how to organize a security policy development team, conduct an IT security risk assessment, and develop risk-mitigation strategies. The guide emphasizes the importance of integrating security policy development into an IT strategic planning process, rather than developing policy post-system deployment.

In addition, the Global Justice Reference Architecture (JRA) and Global Federated Identity and Privilege Management (GFIPM) are national initiatives coming to a data system near you, seeking to improve the state of information sharing between state and local law enforcement agencies. In particular, the GFIPM initiative seeks to eliminate the need for authorized personnel to have multiple accounts. It does this through an authentication and authorization process based on open

standards (pilots are ongoing among JNET, HISN, RISS and CISA).

Douglas also discussed the guidelines applying to all multi-jurisdictional intelligence systems promulgated by 28 CFR Part 23. When discussing intelligence and information sharing, there is a distinction between the two terms, although their relationship is unavoidably symbiotic. Information includes raw data that, once analyzed, may yield intelligence. When gathering information or intelligence, there are provisions governing and requiring the protection of civil liberties and privacy. As we have seen, today's information becomes tomorrow's intelligence. For more information, see the National Summit on Intelligence: Gathering, Sharing, Analysis, and Use After 9-11, (2008).

Finally, creating governance structures through the use of service level agreements can provide a means of making sure all of the stakeholders have a consistent view of what information needs to be secure. They can also ensure that all stakeholders hold the same view on the measures that will need to be taken by each agency in order to meet security and privacy requirements.

This presentation was one of many discussions on data-sharing security held throughout the conference. Vance Hitch, U.S. Department of Justice CIO and co-chairman of the newly formed Information Security and Identity Management Committee, noted cyber security as being a top priority by the current administration with identity management and data access control undergoing significant changes over the next few years. David Kunkle, the Dallas police chief and a fusion center champion, shared this philosophy with the LEIM audience: "If every cop knew what every cop knew, there would be no crime."

Will implementation of these data-sharing security initiatives bring us one step closer to having every cop "know?" That was a central focus of the LEIM conference this year, and we expect it

will be the focus of many upcoming law enforcement gatherings, as well.

To learn more about the COPS Office, its resources and programs, or order any of its publications or products, visit [www.cops.usdoj.gov](http://www.cops.usdoj.gov) or contact the COPS Response Center at (800) 421-6770 or [askcopsrc@usdoj.gov](mailto:askcopsrc@usdoj.gov). ■

*Debra Cohen, Ph.D., is the senior social science analyst at the U.S. Department Justice Office of Community Oriented Policing Services (COPS). She can be reached at [debra.cohen2@usdoj.gov](mailto:debra.cohen2@usdoj.gov).*