

COMMENTARY

An Ambitious Approach to Information Sharing: Understanding the Nationwide Suspicious Activity Reporting Initiative

Rick “Ozzie” Nelson
August 31, 2010

In the midst of two major wars and international counterterrorism operations, it may be difficult to recall that the September 11, 2001, attacks had roots not only in Afghanistan but also in Florida and Minnesota.¹ That is a point stressed by developers of the Nationwide Suspicious Activity Reporting (SAR) Initiative, or the NSI.² Begun by the Office of the Program Manager for the Information Sharing Environment (PM-ISE)—which was created by the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA)—the NSI is a partnership that allows federal, state, local, and tribal law enforcement officials to share information on terrorism-related criminal activity. The logic behind the initiative is that terrorism threats to the homeland require the preventive efforts of law enforcement and national security officials across all levels of government.

Policymakers have spent the last few years shaping the NSI. In December 2008, the PM-ISE released the first version of the NSI’s concept of operations.³ The Congressional Research Service described the initiative this way:

When a police officer detects suspicious activity that might be terrorist related, he or she documents that activity in a SAR [Suspicious Activity Report]. That report is reviewed within the officer’s chain of command. Once vetted, it is submitted to a state/local fusion center, where it is reviewed by an intelligence analyst to determine whether it meets the established SAR criteria. If so, the report is entered into the information-sharing environment [sic], where it becomes accessible to authorized agencies at all levels of government and available for analysis and fusion with other intelligence information.⁴

In February 2010, Thomas J. O’Reilly, senior policy adviser in the Bureau of Justice Assistance (BJA) at the Department of Justice (DOJ), was named director of the NSI Program Management Office. Around this same time, a handful of reports described the NSI’s implementation process. In January, the results of a year-long evaluation of SAR initiatives became publicly available. One conclusion was that three different training programs—targeted at line officers, analytic personnel, and agency executives, respectively—helped lay the foundation for improved sharing of terrorism-related suspicious activity reports.⁵

¹ Hijackers Mohamed Atta, Marwan al Shehhi, and Ziad Jarrah received flight training in Florida in the months leading up to the September 11 attacks. Zacarias Moussaoui, the so-called 20th hijacker, received flight training in Minnesota around the same time. Moussaoui’s unusual behavior raised suspicions with his flight instructor, who reported Moussaoui to the FBI. Immigration and Naturalization Service agents later arrested Moussaoui on immigration charges. See National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton, 2004), <http://www.9-11commission.gov/report/911Report.pdf>.

² Nationwide SAR Initiative, “Nationwide SAR Initiative,” http://nsi.ncirc.gov/documents/NSI_Overview.pdf.

³ Program Manager for the Information Sharing Environment (PM-ISE), “Nationwide Suspicious Activity Reporting Initiative: Concept of Operations: Version 1,” Information Sharing Environment, Washington, D.C., December 2008, http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r4.pdf.

⁴ Mark A. Randol, “Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress,” Congressional Research Service, Washington, D.C., November 5, 2009, <http://www.fas.org/sgp/crs/intel/R40901.pdf>.

⁵ Bureau of Justice Assistance, “Final Report: Information Sharing Environment (ISE)—Suspicious Activity Reporting (SAR) Evaluation Environment,” Information Sharing Environment, Washington, D.C., January 2010, p. 45, http://www.ise.gov/docs/sar/BJA_Final_Report_ISE_SAR_EE.pdf.

A February status report also recounted a handful of anecdotes from the evaluation period suggesting that the NSI process might streamline information sharing efforts. Many law enforcement agencies that participated in the evaluation process had reported being overwhelmed by thousands of residual SARs whose relevance to terrorism was unclear. After its officers received training, though, one particular agency “was able to filter out almost 95 percent of its reports” upon concluding that the leftover SARs were unrelated to terrorism.⁶

One police department “added a check-box to its existing field interview forms to specifically denote a report as a SAR,” thus permitting the forms to be “properly routed for processing.” The measure also promised to reduce the burden on line officers by eliminating the need to complete additional paperwork. Such initiatives may seem modest, but even mundane reforms, like consolidating reporting requirements, can improve information sharing.⁷

The February status report is quick to acknowledge that these positive indicators are mostly observational; more research is required to reach quantitative conclusions about the benefits and potential shortcomings of the NSI process.

In March, for instance, the PM-ISE issued a report outlining the information sharing technologies available to agencies involved in the NSI process.⁸ Once fusion centers, police departments, and other NSI stakeholders are able to implement these technologies, officials will gain a better sense of what works and what needs revision. The same goes for guidelines on privacy and civil liberties protections. As the July 2010 ISE report to Congress noted, numerous ISE stakeholders had developed draft privacy guidelines.⁹ These are positive developments, but until such policies are fully coordinated and codified, it is difficult to determine their effectiveness.

A few additional, more subtle measures are unlikely to gain as much attention as technological implementation or civil liberties guidelines, but they may prove no less important to the success of the NSI. One is the Building Communities of Trust Initiative, a joint endeavor by BJA, DOJ’s Community Oriented Policing Services (COPS), the Department of Homeland Security, and the PM-ISE. Four pilot programs—located in Miami, Boston, Seattle, and the state of Texas—hosted workshops with police, fusion center leaders, and community representatives. The goal was to increase trust and interaction between law enforcement officials and local residents, especially racial, ethnic, or religious minorities.

This type of measure—one that aims to develop relationships, build trust, and improve communication—is an often-overlooked but critical component of effective information sharing. Even the most efficient procedures for channeling SARs from frontline officers to fusion centers to federal agencies will suffer if local law enforcement officials neglect to build relationships with local communities. The family and friends of suspected terrorists, after all, are often the best source of information for local police. This was true in the case of the five young men from Northern Virginia who traveled to Pakistan in an attempt to join the Taliban in late 2009. Through an intermediary, their families contacted the FBI, which then worked with Pakistani authorities to locate the young men before they could harm anyone.

The February status report lauded the Building Communities of Trust Initiative and said that guidance for law enforcement, fusion center personnel, and community representatives, to be based on findings from the four pilot programs, would be released early this year.¹⁰ The PM-ISE’s July report to Congress similarly praised the initiative and said that the findings would be released this summer.¹¹ As of this writing, the report is in the final prepublication stages.

Another low-profile aspect of the NSI is its applicability to an “all-crimes environment,” as described in the February status update. According to the report, the NSI cycle, while focused on terrorism, can be applied just as readily to other criminal activity. This feature is likely to appeal most especially to local law enforcement officials, for whom terrorism is one of many concerns.

⁶ PM-ISE, “Nationwide Suspicious Activity Reporting Initiative: Status Report,” Information Sharing Environment, Washington, D.C., February 2010, p. 11, http://www.ise.gov/docs/sar/NSI_Status_Report_FINAL_2010-02-03.pdf.

⁷ Ibid., p. 10.

⁸ PM-ISE, “Nationwide Suspicious Activity Reporting Initiative (NSI): Technical Implementation Options,” Information Sharing Environment, Washington, D.C., March 2010, http://www.ise.gov/docs/sar/NSI_Tech_Impl_Options_Version_1_FINAL_2010-03-09.pdf.

⁹ PM-ISE, “Information Sharing Environment: Annual Report to The Congress,” Information Sharing Environment, Washington, D.C., July 2010, p. 51, http://www.ise.gov/document/ISE_AR-2010_Final_2010-07-29.pdf.

¹⁰ PM-ISE, “Nationwide Suspicious Activity Reporting Initiative: Status Report,” February 2010, p. 17.

¹¹ PM-ISE, “Information Sharing Environment: Annual Report to The Congress,” July 2010, pp. 58–59.

The February status report suggested that changes to the NSI's concept of operations may be necessary to ensure that the program functions according to an "all-crimes" paradigm.¹² The PM-ISE's lengthy July report to Congress made no mention of such potential alterations. Going forward, it will be interesting to see whether the NSI's Program Management Office, in consultation with the PM-ISE, decides to reshape the concept of operations to better address non-terrorist threats. Such a move would likely prove useful for state and local law enforcement agencies forced to deal with crime tied to drugs, gangs, and other non-terrorist activities.

The numerous programs tied to the Nationwide SAR Initiative and the broader Information Sharing Environment signal an important step toward alleviating what the 9/11 Commission recognized as a major flaw in the country's national security apparatus. And with the recent uptick in "homegrown" extremism, programs like the NSI, which explicitly reaches out to state and local law enforcement officials, will prove especially important. How these initiatives are implemented—and how they evolve—will ultimately determine their success.

Rick "Ozzie" Nelson is director of the Homeland Security and Counterterrorism Program at the Center for Strategic and International Studies in Washington, D.C. This Commentary is being published as part of a series of events on information sharing in counterterrorism and law enforcement, sponsored by IBM.

Commentary is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2010 by the Center for Strategic and International Studies. All rights reserved.

¹² PM-ISE, "Nationwide Suspicious Activity Reporting Initiative: Status Report," February 2010, p. 5.