



The DHS Domestic Nuclear Detection Office Goes NIEM

FROM A PORTFOLIO OF NIEM SUCCESS STORIES

A vehicle is headed down Interstate 270 south toward Washington, DC. As it passes through Frederick, Maryland, 50 miles north of the capital, it crosses a sensor ring and trips a radiation sensor. At the 45-mile marker, it trips another one; another again at 40. Continuing south, it sets off sensor after sensor. What might at first have appeared to be a false alarm or a nuisance now appears to be a “hot” vehicle speeding toward a highly sensitive location, and is more than likely a real threat.

Is it?

A clock starts ticking: the race is on to make sense of the data being received; to determine the true nature of the threat; to share the data widely, moving it quickly from classified to unclassified, not within minutes but within mere moments, putting the information into the hands of those who will take action.

In such a situation, delays can be deadly. But moving too soon also has its risks. False alarms can be onerous for the many legitimate transporters of radioactive materials on America’s roadways, at its ports, and in its storage facilities, not to mention bulk transporters hauling scrap metal, granite, bananas, and even kitty litter—all of which emit isotope signals that sensors can pick up as “hot.”

Today, there are obstacles that can keep data from traveling from the thousands of sensors planted for chemical, biological, or nuclear detection to analysts, decision-makers, and operations personnel. Disparate message standards, syntaxes, and formats abound. Sensor networks are proprietary, closed, and cannot easily interoperate. Message platforms range from email to telephone to fax—but are almost never machine-to-machine. Humans intervene at almost every handoff, writing on pads, transposing from screens, each time introducing new opportunities for risk and error to be introduced. Domestically, email is the most common method of notification and transmission of sensor spectral files. And in the race to get diverse

messages from sensors to analysts and back to operations, email filters can interrupt the quick and reliable flow of information.

“What we want to do with NIEM,” says Bob Dilonardo, CIO of the Department of Homeland Security’s Domestic Nuclear Detection Office (DNDO), “is to get better technology in place to give first responders better tools for guaranteed delivery, so they’re not interrupted by system filters, human or other, when we’re talking about national security.”

There are plenty of moving parts to this sprawling system of systems, but there is no central oversight or controlling authority that spells out its architecture. State and local law enforcement, the FBI, the Department of Energy, the Department of Homeland Security, and the Department of Defense, for example, all participate in looking for radioactive threats. Dozens of vendors provide solutions, many of them highly innovative.

In an ideal world, machines would move data to machines by messaging—quickly, with minimal error, and across the boundaries of organizations, sectors, and jurisdictions. Data would move, for example, from a sensor on a state trooper’s hip, to the hip display of a Secret Service agent moving a protectee through a complex urban corridor, mediated by secure but open networks, supported by interoperable platforms, and formatted for awareness, decision, and response as necessary.

That world is not here yet, but the concept is: a “global nuclear detection architecture” continuously monitored by the Joint Analysis Center (JAC), a division of the Operations Support Directorate of the DNDO.

JACCIS—the Joint Analysis Center Collaborative Information System—is the JAC’s IT backbone. Support for alarm adjudication across the nation is a key JAC mission, and DHS is the “customer” organization relying on JACCIS and JAC to detect movement within the United States of illicit nuclear material—whether radiological dispersal devices—“dirty bombs”—or conventional nuclear weapons.

“DNDO’s job for this part of its mission,” Bill Wright, DNDO Data Architect, explains, “is to collect the dots and put them together.” Wright has led, supported, and provided insight to initiatives such as DNDO’s for more than 30 years, and with a small group of developers is actively involved in the build-out of the DNDO capability today.

“What we want to do with NIEM is to get better technology in place to give first responders better tools for guaranteed delivery, so they’re not interrupted by system filters, human or other, when we’re talking about national security.”

– Bob Dilonardo, CIO of the Department of Homeland Security’s Domestic Nuclear Detection Office (DNDO)

“The JAC doesn’t control or operate anything in the field, but they’re an important source of knowledge: wiring it all together so the dots can be seen, and then figuring how you’re going to connect the right dots.”

LOOKING BACK

In the aftermath of 9/11, the small DNDO organization faced a daunting challenge: how could they ensure accurate, timely, and complete situational awareness for decision-makers, providing everyone in a variety of agencies and departments with a common operating picture of nuclear threats within the United States?

But at the time, it was the “wild, wild West” out there. For all the diversity of sensor systems deployed (or soon to be deployed), each had its own interface, captured data in its own way, and captured different data records. Standardization of data would be critical for the JAC to gain and generate a common operating picture of threat. Standardization would be essential to bring forward all the value of the many investments already made in sensors and sensor networks—in meaningful, actionable, situational awareness.

Exploring its options, DNDO turned to the National Information Exchange Model (NIEM). The NIEM process and its principal artifact—the Information Exchange Package Documentation (IEPD)—seemed promising to DNDO, partly because DNDO’s network of state and local law enforcement partners had embraced Global Justice XML, a foundational predecessor and building block of NIEM. Whatever move DNDO might

make next, achieving machine-to-machine interoperability with that vast network of state and local message producers and consumers was essential.

Investigating further, DNDO discovered another useful resource: the U.S. Customs and Border Protection (CBP) had already defined and implemented a basic set of messages around the radiological and nuclear (“rad/nuc”) domain, employing what was known as the N.25 protocol. And many of its message sets were consistent with DNDO’s needs.

In the midst of this dialogue, DHS directed all departmental elements—including DNDO and CBP—to become NIEM-conformant. So DNDO helped CPB convert all its rad/nuc messages to NIEM, adding in their own messages. Thus NIEM’s rad/nuc message set was born—dubbed the N.25 IEPD—with CBP to become a major user and DNDO its steward—the first “science” message set to be added to the NIEM core.

ENTER NIEM

DNDO staff had earlier evaluated NIEM’s first release (NIEM Version 1.0) as strong on justice system information exchange, but not yet ready to support DNDO’s science-related mission.

But NIEM Version 2.0 struck DNDO as different—and significantly improved. The introduction of the NIEM “core” and domain structures, for example, seemed to broaden NIEM’s usefulness, away from its historic law enforcement-only roots, welcoming other domains while leaving its law enforcement applications intact. This meant that it would be easy for DNDO to leverage already existing dictionaries while adding its own terms. That would be more than a time and money saver—it would add interoperability across domains.

Moreover, NIEM had been proven in operations. And the NIEM documentation was solid. “I have been either a program manager or a chief architect on more than 200 systems, including for Fortune 500 companies,” Wright said. “All over the map, all different kinds of business disciplines. You can tell what’s good, and what’s just okay. This was good stuff. The NIEM team really did its homework.”

The N.25-to-NIEM conversion work—the goal of which was a NIEM IEPD for rad/nuc messaging—began with CBP. It was arduous work, but the NIEM process provided a useful framework.

The introduction of the NIEM “core” and domain structures [in NIEM Version 2.0] seemed to broaden NIEM’s usefulness, away from its historic law enforcement-only roots, welcoming other domains while leaving its law enforcement applications intact. This meant that it would be easy for DHS’s Domestic Nuclear Detection Office (DNDO) to leverage already existing dictionaries while adding its own terms. That would be more than a time and money saver—it would add interoperability across domains.

The conversion work was complicated by a request from the NIEM Program Management Office to DNDO to steward not just the rad/nuc message set, but to support chemical and biological detection messaging as well—and to create a consolidated “ChemBioRadNuc” (CBRN) domain.

The advantages were clear. The content of the sensor data files—the outputs of a chem/bio, rad/nuc, or geophysical sensor—would be unique to the sensor type. But the information around the file would be the same, regardless of the type: what day it was collected; what the weather was at the time; the temperature; what kind of time was being used—local or GMT; the location of the sensor, its distance from the source. All of this information would be the same no matter what kind of sensor was in use.

The virtue of this approach soon became apparent. In November 2008, the DNDO development team visited a large gathering of state, local, and federal groups at the Naval Post Graduate School in Monterey, California. The DNDO group saw that the chem/bio domain was

making slow progress in its efforts to standardize messaging. DNDO demonstrated an example of its own handiwork—called “the alarm summary” message (one of the messages defined in the N.25 IEPD). Having designed the message so that it might work for any sensor—it contained everything except for the specifics of the chemical data itself—DNDO heard words that would warm the heart of any database developer. “That works for us,” the chem/bio people attending the event told DNDO. “We can use that. We’ll run with it.”

THE SOUTHEAST TRANSPORTATION CORRIDOR PILOT (SETCP)

There was still more proof waiting. The Southeast Transportation Corridor Pilot (SETCP), launched in 2008, was designed to “red team” a sensor web. The idea was to take radioactive material that represented a threat, and see if operators at truck weighing stations could detect it.

Working with DNDO, the SETCP would do more than detect radioactive material at weigh stations: it would test elements of the JACCIS-based message stream by messaging detection alarms from the weigh stations through JACCIS to JAC watch officers, and from there to scientists at Sandia National Laboratory who would analyze, validate, or otherwise characterize the alarms back to the JAC.

Where previously such information might be shared domestically using email and files, the SETCP pilot would ship messages machine-to-machine over JACCIS.

DNDO was tasked to develop the message set for SETCP, using NIEM’s N.25 IEPD-based messages.

Under Dilonardo’s direction, the DNDO team mapped out the message flow from the weigh stations, to the JAC, to Sandia, and working with developers, turned preliminary specifications into operating code in a matter of weeks. Soon, test messages were flowing. When, mid-pilot, exigencies arose that required message revisions, developers used the CBRN IEPD and related NIEM artifacts to crank out revised messages in less than 24 hours—without having to be knowledgeable about NIEM—and made it work for real-world message traffic.

The SETCP demonstrated that the NIEM-based messages DNDO had developed could support the JACCIS-enabled message flow to the JAC, even laden with vital data about the sensor file itself. It proved that, when needed, non-experts could develop NIEM-conformant messages rapidly. It showed, further, that watch officers, analysts, and scientists could read and interpret those messages, even when they were sent machine-to-machine.

The SETCP was therefore an important milestone in proving DNDO’s capabilities, its NIEM development process, and its NIEM CBRN core. Most importantly, perhaps, in SETCP DNDO demonstrated that a vastly distributed network of networks might soon carry messaging alerts from sensors to analysts to operators, no matter where or when they were received, and that they could do so with astonishing speed and accuracy. Which of course, is important in connecting the dots.