



Information Assurance Post 9-11: Enabling Homeland Security

David W. Carey
Oracle Corporation

STC
Wednesday, 30 April 2003
Industry Plenary: 8:00 - 9:00
Ballroom

The demands of homeland security require information sharing on an unprecedented scale. This includes sharing information among many agencies such as foreign intelligence, domestic law enforcement, the Department of Homeland Security, the Department of Defense, federal, state, local entities, and the private sector. Most of these entities have not worked together before, and those that have will need to work even more closely together in the future. For example, a single bioterrorism incident – or the threat of one – requires that elements in agribusiness, public health, law enforcement, and foreign intelligence work seamlessly. It will take more than legislation to enable this transformation. A host of technology, policy, and cultural issues will need to be addressed. Information assurance will play a pivotal role in establishing the trust that will enable this critical transformation.

Whether the objective is thwarting terrorists beyond U.S. borders, making arrests on U.S. soil, or protecting this country's critical infrastructure, the ability to share information and to do it securely is the key to an effective homeland security regime. This is a staggering undertaking.

In the new Department of Homeland Security alone, a complete information-sharing system will have to encompass some 22 current agencies, many of which are not accustomed to working with one another. These agencies must also be connected to the intelligence community, the Department of Defense (DoD), and other civilian agencies. In essence, most of the federal government needs to be involved. Now add state and local organizations from law enforcement to public health and the private sector, which – after all – controls most of our critical infrastructure.

The need for information assurance is paramount. For organizations that gather critical information – especially the law enforcement and intelligence communities – to be willing to share quality information, the computer infrastructure must be secure. This is particularly true if the information that is to be shared in a time-

ly manner between these federal, state, and local entities and private sector organizations is actionable. If officials in these organizations do not trust that the information they provide will be protected and that it will only be shared appropriately, the information may be either withheld or sanitized to the point of uselessness.

To build this data-sharing infrastructure, a set of technical, policy, and cultural issues must be addressed. The technical issues are complex but in some ways easier to deal with than the policy and especially the cultural challenges.

Information Sharing Architectures

For some time now, the problem for law enforcement and intelligence organizations has not been a lack of information. On the contrary, authorities are often swamped with information, but it resides in separated, isolated, and discrete systems. The problem is exacerbated when the data are stored in different formats in those different systems.

Much of the time the problem is the lack of sufficient capability to establish relationships between these various bits of information. Real knowledge is found in these relationships, often more so than in the data itself. As seen in the days and weeks after 9-11, there were lots of facts about the individual terrorists responsible for the attacks. Because these facts were not brought together, however, no one could see the whole picture.

Of course, there are numerous ways to create the needed information-sharing system. One approach would be to create a single, national, homeland security information system that integrates data from all organizations involved. This is typical of

data warehousing architectures (See Figure 1). Data are first extracted from a system. The data typically undergo some type of sanitization and transformation to normalize structure and meaning. Finally, the finished product is loaded, perhaps also combined with other system data, into a large database called the data warehouse. This process is known as extraction, transformation, and loading.

Whether or not this approach is feasible technically – and many people have suggested it is not – practical realities make it a solution that is not only unwieldy but also unlikely. Persuading all the agencies and organizations involved to defer to some central repository to protect and disseminate their information – with the concomitant loss of control that this implies if not actually entails – would be the equivalent of tilting at numerous cultural windmills in each of the agencies involved. Nor would this approach be without significant political challenges and hurdles.

Another approach would be to allow some central authority – with appropriate certificates and clearances – to reach into the myriad of databases involved and extract just that information needed for the task at hand. This distributed query approach (see Figure 2) also faces significant technical hurdles to ensure that a given query is formatted so that all the databases involved are queried in a like manner. Without that assurance, it would be impossible to have any confidence in any answer produced. Moreover, from a cultural perspective, this approach – which seemingly gives the keys to the kingdom to the enquirer – would likely be just as unpalatable as the first approach, if not more so.

Figure 1: Data Warehousing



The challenge then is to devise an architecture that deals with legacy systems, which probably have not been fully inventoried yet much less understood, and that does so in a way consistent with the organizational cultures involved. Although we do not have the luxury of starting with a blank piece of paper, we can make it possible for the various organizations involved to build or alter their systems in such a way that they can work in concert. These loosely integrated systems could work together to support a national strategy for homeland security. Each of the entities involved must be able to meet its organization's requirements and fit into its organization's infrastructure while adhering to standards for information sharing.

The resulting architecture would allow each organization to publish to a database that it still controls, allowing that organization to ensure that the data provided meets the requirements levied but does not contain inappropriate material (see Figure 3). Information from such individual repositories could then be amalgamated and made available to appropriate users. For example, if that newly constructed database were a terrorist watch list, then users would have an up-to-date repository of all the watch lists now extant with a pointer system to direct them to the appropriate agency for more in-depth information.

Standards

Above all, creating such an information-sharing system would require a commitment to standards. Those standards fall into three categories: data, integration, and security.

Data

When sharing data, it is not only important to establish data format standards, but also to understand the semantics of data fields and data quality, including how the data were collected. This makes it possible for organizations to compare data and establish relationships.

For example, the Department of Justice has defined a data standard called the National Incident-Based Reporting System (NIBRS). This standard defines guidelines for collecting and storing information related to a criminal incident. For example, it defines a data element for storing a person's eye color: the codes representing the allowed values for eye color, and the color corresponding to each code.

In this way, if two systems are NIBRS-compliant, the data in each can be compared easily because both use the same code to represent blue eyes, for example.

Data standards like this one are critical for ensuring that once connectivity is established between systems, users will be able to compare and interpret the results.

Integration

Integration standards define how a system exposes its data and services to other systems. Web services are the emerging technology area currently being investigated for integration. Web services consist of several technologies that are standards-based. Some examples of standards for Web services include the following:

- Web Services Description Language is an Extensible Markup Language (XML) for describing Web services.
- The Universal Description, Discovery, and Integration is an open framework for describing services, discovering businesses, and integrating business services using the Internet.
- The Simple Object Access Protocol is an XML/HTTP-based protocol for accessing services, objects, and servers in a platform-independent manner.

These standards define how a system wraps up and publishes its data to other systems along with what services it provides and how to interact with these services. A system can use these standards to, in effect, say the following:

I know all about licenses for airplane pilots in the state of Virginia. If you give me a social security number, I will check your credentials and then give you XML in the following format that includes that person's license information.

With this approach, the user does not care how the system was built, only that it

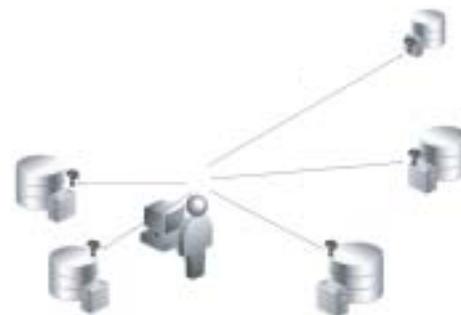


Figure 2: *Distributed Query Infrastructure*

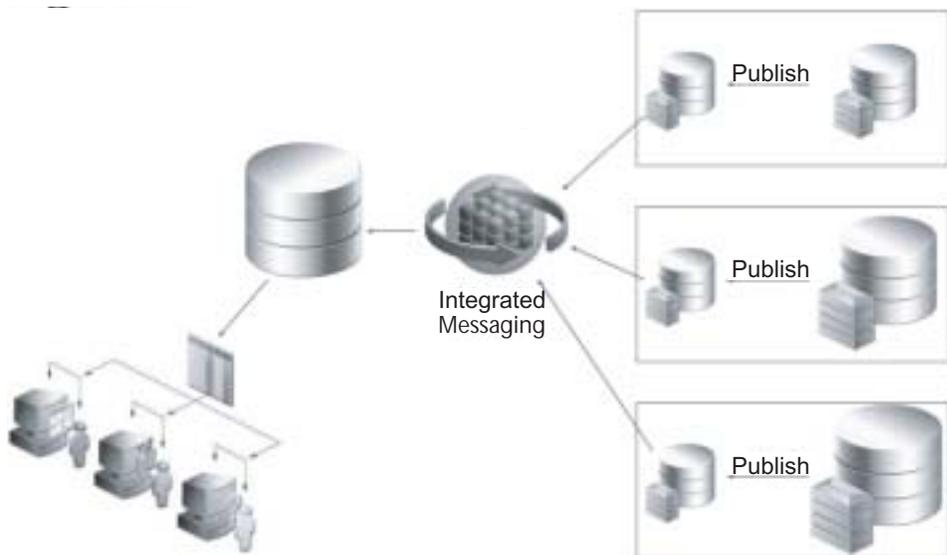
can accept and answer the question. Because the federal, state, and local systems are all going to be built independently, integration standards are required for them to effectively share information.

Security

Perhaps the most important information standards are those related to security. Again, the most significant barrier to information sharing will not be the technical issue; it will be the concerns that organizations have about exposing their data to potentially insecure systems. This means that the organizations have to establish trust relationships.

To do so, at least four basic tenets of security need to be honored. First, security has to be part of the design. That is, security has to be built into the system and not bolted on afterward. When a bank is built, for example, the architects and construction personnel have thought about how people will try to break in. They will have gone through extra measures to ensure the bank's security is sound and robust. The same attention should be focused on security in information-sharing systems. Trying to secure an insecure system after it has been built simply does not work – at least elegantly.

Figure 3: *Selected Information Sharing*



Second, defense in depth is needed. By providing layers of security, assurance is given that a failure in any single defense measure does not compromise the entire system. Returning to the bank example, the architect is likely not only to use locked doors but also a time-operated bank vault, security cameras, and bulletproof glass. The bank managers are likely to add vetting procedures for bank personnel and guards.

Third, it is important to the security process that people realize risk has to be managed. While maximum security is a laudable goal, achieving that goal has to be balanced with other competing factors such as system performance, usability, administration, and even cost. A system with every possible safeguard generally suffers such performance problems that the system is not used. The workarounds devised generally sacrifice security entirely. Security is the delicate balance in risk management to secure our assets while still maintaining a usable, cost efficient, and manageable system.

Fourth, it is important to be careful about the products used. Just as there are different qualities in building materials, there are different qualities in security products. While it is largely accepted that most security is centered in the process of configuring and properly using the products, they are the foundation by which everything is built. As with most endeavors, if the foundation is weak, then it does not matter what else has been done; the system will not function appropriately.

Within the U.S. government, a level of trust is established in an operational system through the certification and accreditation process. System certification is the technical and non-technical evaluation of a system that produces the necessary evidence that is presented to the accrediting authority. The evidence needs to be comprehensive enough so that the accrediting authority can make a decision about the risk of allowing a system to be operational and to connect to other systems.

Within the government's executive and civil branches, the National Institute of Standards and Technology (NIST) is taking the lead in establishing standards and guidelines for system certification and accreditation. For the executive branch, the NIST recently released the draft publication "Guidelines for Security Certification and Accreditation of Federal Information Technology Systems."

For the DoD, the Defense Information Systems Agency (DISA) has established the "DoD Information Technology Security Certification and Accreditation

Process (DITSCAP)" [1]. The DITSCAP defines both the secure design and certification process and requirements, and applies to systems within the DoD that do not include special intelligence data. Systems that process special intelligence data are certified by the Defense Intelligence Agency against the Director of Central Intelligence Directive 6/3 [2] that is similar to the DITSCAP but more stringent in its requirements.

In developing accreditable systems, it has become increasingly important to use products that have been evaluated against the security standards. This is especially true for products that support system security or provide cryptographic services. In the United States, the National Information Assurance Partnership, a collaboration between the National Security Agency and NIST, manage product evaluation. They manage the standards and independent evaluation processes required to ensure that technology providers are implementing secure products. Security products are evaluated against standards promulgated by the ISO, specifically ISO 15408, and the "Common Criteria" [3]. Encryption technology is evaluated against Federal Information Processing Standards 140-2 [4].

These evaluation standards should be enforced across this information-sharing system. To ensure that every possible step is being taken to secure data at its source, the government has taken steps to do just that for national security information systems. In July 2002, a National Information Assurance Acquisition policy went into effect for systems that contain information related to national security. National Security Telecommunications Information Security Systems Policy No. 11 [5] requires that products that have undergone independent security evaluation be used on these systems. It is imperative that policies like this one be strengthened and, more importantly, enforced through procurement policy. This policy was reiterated in DoD Directive 8500.1 [6] in October 2002.

The good news is that, in essence, the technology to build a secure information-sharing system is available today. Information can be shared widely with assurance that only the people who should see the information are granted access. Systems can be protected and users audited. And systems can be configured so that they will be available even in the event of a catastrophe. Some of the technology is already robust while other technology will become so with demand and high expectations.

In describing these secure systems, security clearances and national security classifications have not been mentioned. These protections are especially important within the intelligence community and other parts of the federal structure that are required to protect sources and methods. But it is possible to get actionable information to the people who need it without worrying about whether or not they have a national security clearance. In this case, the secure in secure information sharing means that only appropriate users are accredited to the system and that they only have the access needed to discharge their responsibilities.

Building a system that will meet these requirements is not cheap or easy, but it is doable. While reality in the information technology industry sometimes falls short of claimed performance, there are ways to ensure that does not happen. As noted, independent evaluations provide a measure of assurance that actual functionality lives up to a vendor's claims; moreover, employing evaluated products makes certification and accreditation of information technology systems easier.

It is important to buy commercial off-the-shelf products and to limit the urge to customize. Too often such customization is justified because *we are special*. This is invariably an expensive trap; the mission of homeland security is special but often the information sharing and information assurance needs are not. Point solutions or those that require 20/20 hindsight should be avoided; rather, the infrastructure to enable solutions should be created.

Other Challenges

Of all the impediments and hurdles, the technical challenges – while far from trivial – may be the easiest. As with any massive change, the principal challenge will be policy and culture.

A major policy challenge has already been met; the president has said, "Do it." Of course, myriad policy issues will have to be addressed to get it done. Setting the standards that have been discussed involves a number of key decisions. Even deciding who makes the decisions may be controversial. Who will fund and control the coordinating systems and mechanisms? Who will fund the upgrades and migration programs for the legacy systems involved, remembering as noted earlier that in the critical infrastructure community most of these entities are in the private sector? There will also be the policy decisions regarding who has access to what information.

Next are the cultural issues. At least the

technical and policy issues can be identified and worked directly. The challenge that must be faced is to build a trust relationship, frequently a challenging task when the parties know each other well. Dealing across cultural divides is often problematic in part because of the difficulty in defining the specific issues that need to be addressed.

The intelligence and law enforcement communities at the federal level work more closely together than they ever have. But there are still distinctly different cultures forged by the nature of the work. There is a common language with different definitions. For example, at the Federal Bureau of Investigation an agent is a government employee; at the Central Intelligence Agency (CIA), an agent is someone you recruit to provide intelligence or access to a foreign target; whereas in the public health arena an agent is a pathogen.

The same issues are associated with the use of acronyms. Within the CIA the National Intelligence Council – NIC – produces assessments called NIEs or National Intelligence Estimates. While within the Drug Enforcement Administration there was at one time the National Narcotics Intelligence Coordinating Committee – NNICC – which issued NIEs or Narcotics Intelligence Estimates. And, of course, CI means counterintelligence to one group in the CIA, current intelligence to another, confidential informant to most law enforcement organizations, and a computer incident within the IT community. These are purposely trivial examples, but they are symptomatic of the different mindsets forged by different missions.

These different cultures and mindsets come to the forefront when information sharing is on the table. Some of what people see as resistance to sharing is based on legal requirements. As stated earlier, by law the director of Central Intelligence is charged with protecting sources and methods. The issue of how much information can be released without revealing either source or method is legitimate. Against that backdrop though, a risk avoidance culture will ensure that less rather than more is shared. Each agency has its own security vetting process, and at present there does not appear to be a shared appreciation for what information needs to flow where.

The Task

Despite these challenges, progress can be made. Indeed, it must be made. The key is found in two old saws that fit today's chal-

lenge. The first is “think big, start small, and scale fast.” Assuming that the new Department of Homeland Security will be tasked to develop this integration capability and given the appropriate authority and budget, a number of things need to happen under their auspices to start small, recognizing that in this instance small is a relative term; the task is enormous. If some other entity is given this responsibility, the tasks remain the same:

- A pilot program needs to be defined that identifies the first set of information that must be shared across organizations. This pilot must be large enough to cross organizational boundaries but small enough to allow results to be accomplished quickly. To facilitate the pilot, no more than three organizations should be involved. This also keeps to a minimum the number of security accrediting authorities that would need to be involved.
- Memorandums of understanding between the organizations need to be established along with a trust relationship at the personnel.
- Several efforts need to be started in parallel:
 - Development of system integration and data-sharing standards.
 - Design of a system architecture.
 - Definition of the security accrediting authority, process, and requirements, and the definition of the security policy and architecture.
 - Development of a prototype system to shake out the interoperability, security, and system functionality issues.

The lessons learned from this effort can then be used to *scale fast*, that is to move the prototype system to operational status and then to start a phased effort to integrate additional organizations and systems. Again, the task is huge, but it is imperative to bite off something that can work and can be done rapidly – both to get things moving and to model the culture and behavior you will need to get the bigger job done. Then scale fast.

The other old saw that is appropriate is, “the perfect is the enemy of the good.” In other words, it is important to get something good started and make it better as we move along.

Both of these old saws contain an underlying note of urgency that is relevant to the task of enabling data sharing for homeland security. The formation of the new Department of Homeland Security has been likened by many to the formation of the DoD in the post-World War II era because of the enormity and otherwise

daunting nature of the two undertakings. The main difference, of course, is that the DoD was formed in the aftermath of war while the new department is being formed during what unfortunately is in all likelihood the early phase of a war. The only acceptable result is success. ♦

References

1. DoD Information Technology Security Certification and Accreditation Process <<http://iase.disa.mil/ditscap>>.
2. Director of Central Intelligence Directive 6/3 <www.fas.org/irp/offdocs/DCID_6-3_20Policy.htm>.
3. Common Criteria/ISO 15408 <www.commoncriteria.org> and <<http://csrc.nist.gov/cc/index.htm>>.
4. Federal Information Processing Standards 140-2 <www.itl.nist.gov/fipspubs/index.htm>.
5. National Security Telecommunications Information Security Systems Policy No. 11 <http://niap.nist.gov/ccscheme/nstissp_11.pdf>.
6. DoD Directive 8500.1 <<http://iase.disa.mil>> and <<http://niap.nist.gov/cc-scheme/d850001p.pdf>>.

About the Author



David W. Carey is vice president of Information Assurance at Oracle Corporation. He built and currently directs Oracle's Information Assurance Center, located in the company's Reston, Va., facility. The center provides a venue to demonstrate Oracle's security-related technology and for Oracle customers and partners to address a wide array of information assurance and security challenges. Before joining Oracle, Carey worked for the Central Intelligence Agency. During his 32-year career there, Carey held several senior positions, including executive director. He is a graduate of Cornell University and the University of Delaware.

Oracle Corporation
1910 Oracle Way
Reston, VA 20190
Phone: (703) 364-2126
Fax: (703) 734-1374
E-mail: dave.carey@oracle.com