



Call for Action

May 2005

A Blueprint for Better Government: The Information Sharing Imperative

The Issue

Government information is a critical asset that must be held in trust and effectively managed by state government. Government institutions, at all levels, must place greater emphasis on the exchange of data between and among its trusted partners. In order to meet the growing demands and service expectations, information must be leveraged and supported by coordinated, integrated solutions. Information sharing or exchanges among agencies, the federal government and local jurisdictions are obstructed in the current “stove piped” environment. Where information sharing is required with federal agencies, the lack of common data vocabularies is costly and confusing for state governments. Although some progress has been made, more effort is needed to detail how information sharing responsibilities and relationships, including appropriate federal incentives, will advance this task.

The Challenge

NASCIO recognizes the challenges of cross boundary information sharing initiatives. By definition, any cross-boundary project requires cooperation across traditional boundaries. These boundaries can be administrative, cultural, technological, geographic, organizational or, most likely, all of the above. A major barrier is the federal funding model and lack of incentives to collaborate. State governments have their own set of unique challenges; however barriers to effective information sharing are being addressed. State chief information officers (CIOs) are actively promoting the enterprise perspective for information management with initiatives in several program areas including criminal justice, public health and education.

Our Position

The information sharing environment is complex and innovative solutions and partnerships are necessary to harvest shared benefits. Information exchange modeling is a difficult undertaking, especially if multiple layers of government are involved. A shared understanding and well-defined blueprint (or information architecture) is the key to success. Part of the enterprise architecture (EA) approach includes an understanding of the necessary inter-agency business processes from federal to state, state to state, and state to local. It provides guidance for re-designing those processes to remove inefficiencies and redundancies. In short, this approach promotes information sharing between governments at each level and identifies the points and processes for sharing, while being mindful of the security and privacy implications.

How Congress and the Administration Can Help

To achieve seamless delivery of citizen services, safeguard citizens and protect our infrastructure, information sharing among all levels of government is a necessity. Government agencies are increasingly exploiting technologies to integrate their geographically diverse workforce, to break down bureaucratic barriers and to share pertinent information. Partnerships between all levels of government are imperative

to develop a strategic, unified national approach to sharing information. NASCIO calls on Congress and the Administration to take the following actions:

1. REQUIRE A COMMON FRAMEWORK FOR INFORMATION SHARING: NASCIO supports moving from an ongoing dialogue to a clear, jointly prioritized, cross-boundary action agenda involving state, federal, local governments and partnering with the private sector. We advocate a meaningful and collaborative approach to **information sharing** with enterprise architecture standards for commonly used data and harmonized vocabularies across federal government agencies.

- Seek input from state CIOs on proposed Congressional action regarding information sharing and include states on federal information sharing advisory committees. NASCIO requests the federal government **work with the state CIOs** to clearly articulate information sharing frameworks, policies and best practices, and where possible, provide technology guidance, methodologies and funding to the states.
- To improve information sharing, a unified national approach with "joint consensus" is necessary. Defining core shared data and harmonized vocabularies across agencies will promote better information exchange models. We urge an approach which leverages the re-use of existing standards and technology – federal agencies should strive to define a “location” in the same way. Specifically, there is already a well grounded solution for enabling information exchange within the justice community, but that does not preclude its value to other aspects of government. Rather than create agency or program-specific data dictionaries – *use the Global Justice XML Data Model and Data Dictionary* – and continue to build its utility. In addition, the recent partnership agreement between the Department of Justice and Department of Homeland Security to create the National Information Exchange Model (<http://www.NIEM.gov>) is an excellent first step. NASCIO respectfully requests a position on the NIEM governance body to represent state technology interests. Most importantly, to avoid the continued proliferation of new data schemes, Congress should require federal funding requests for information sharing projects to demonstrate how they are **leveraging existing capabilities** for enabling information sharing.
- As Congress contemplates the reauthorization of the **Paperwork Reduction Act** (PL 104-13), the opportunity to reduce the burdens on state government, and create a common and consistent approach for information collection and exchange, is available. Solicit comments from the states and their information technology leaders. If requested, NASCIO is prepared to testify and propose language on this issue.

2. ENERGIZE INTERGOVERNMENTAL CYBERSECURITY: Information sharing for securing the homeland is a classic intergovernmental effort involving multiple federal agencies and layers of government. As a crucial tool in fighting terrorism and cyber crime, federal leadership in all aspects of cybersecurity is critical. Efforts at intergovernmental cybersecurity need to be energized now because protecting critical information assets requires a focused, organized government effort at all levels. Therefore, “cybersecurity” should be integrated into the current homeland security strategy-setting and funding process in order to secure governments’ critical information assets – especially those that support homeland security functions – from both physical and Internet-based threats, as well as to prevent the rise of cyber-terrorism. Regardless of whether Congress (or the Administration) chooses to create an “Assistant Secretary of Cyber Security” as proposed in H.R. 285 or not, NASCIO would like to recommend the following language become law:

- “The Secretary of Homeland Security, through the Office of State and Local Government Coordination, shall work closely with state homeland security officials, the National Association of State Chief Information Officers, and other stakeholders with respect to cyber security and critical infrastructure protection, to develop a state cyber security assessment and strategy process focusing on

continuity of operations and disaster recovery strategies for the critical information and communications technology systems and other technology related assets that support emergency services at the state and local levels as well as related operators in the private sector.”

3. THE URGENCY OF PRIVACY PROTECTION: The rash of recent security breaches and exposure of personal data underscore the necessity for privacy policies and protection. As massive storehouses of citizen information, state governments face similar threats. Federal legislation with privacy provisions, such as HIPAA, can have substantial state compliance costs and complex business process implications across state agencies and branches. Given the wide variety of citizens’ personal information that states collect, store and distribute, a state impact is likely from most types of federal privacy legislation, including driver’s license and voting reform laws. With more government programs involving information sharing, each level of government needs a consistent privacy-protection structure in place. Privacy needs to be more fully integrated in federal agency operations through the Federal Enterprise Architecture (FEA), the consistent use of thorough Privacy Impact Assessments (PIAs), and ensuring that all federal agencies have strong privacy-protection functions in place.

- NASCIO urges Congress to carefully weigh the pros and cons of **pre-empting state law** on privacy notifications and privacy-enhancing policy. Given the level of consumer worry over identity theft, phishing, spyware and database breaches, many states have been active in proposing and enacting legislation to protect citizens. Proposed federal legislation may pre-empt state provisions dealing with these privacy threats. A set of federal threshold requirements may be adequate; however, states are generally better positioned to pursue enforcement action in these matters.
- Create a “seat at the table” for states when considering the enactment of federal privacy legislation or the creation of agency privacy councils or workgroups that address emerging technologies, such as data-mining, or programs that will impact state government IT, such as the Driver’s License Rulemaking Committee.
- Both state and federal governments are challenged to create and maintain strong information privacy protection functions and defend personally identifiable data from exposure. Vulnerabilities from intentional and unintentional intrusions or violations need to be guarded against at an architectural level. NASCIO urges the federal government to continue its work on the security and **privacy profile** in the Federal Enterprise Architecture Framework. We are aware that the Office of Management and Budget (OMB) is advancing the privacy domain work and the outcome will certainly be beneficial to state governments. As a result, we believe a Congressional request to OMB on the status of this effort and the expected timeline for a final issuance is appropriate.

4. PROMOTE AND SUPPORT HEALTH INFORMATION EXCHANGE: Health information exchange has the potential to correct the fragmentation of healthcare delivery and improve communication between healthcare decision-makers. States are key stakeholders in the policy and funding discussions related to this sharing, supported by healthcare networks and electronic medical records. Public health monitoring, bio-terror surveillance and quality of care monitoring require data that depends on health information technology. However, many of the challenges and opportunities in this area are not solved by technology - major business process transformation and workflow improvements are needed. In addition, there are many legal and privacy concerns affecting health information exchange that are controlled by state law.

Medicaid spending now accounts for over twenty percent of total state spending and has become the second-largest item in most state budgets, after elementary and secondary education. Medicaid spending growth has crowded out funding for other important programs delivered by states and technology

investments by CIOs. The potential for health information sharing and health care information technology to bring about improvements and efficiencies in the health system must drive more rapid adoption of proven IT strategies. NASCIO urges the following actions:

- Jointly financed by states and the federal government, Medicaid is the largest source of federal funds to the states, accounting for 43 percent of all federal grants in aid. Through the adoption of health information technology (HIT) there are significant cost saving and quality of care benefits to be realized in the public health arena. As Congress undertakes **Medicaid reform**, it should provide incentives for states to adopt current technologies, like health information systems, quality tracking and review, provider report cards, and other methods to measure and improve quality through the use of technology.
- With the challenge to reduce health costs overall and Medicaid costs in particular, NASCIO **supports fully funding** the Office of the National Coordinator for Health Information Technology (ONCHIT). This office must be supported in pursuit of its goal of executing the actions ordered by President George W. Bush in his April 2004 Executive Order which called for widespread deployment of health information technology within ten years to help realize substantial improvements in safety and efficiency.
- State CIOs are aggressively implementing enterprise technology architecture and standards as a blueprint for better government. Funded by a federal grant from the Bureau of Justice Assistance, NASCIO has five years of demonstrated program experience, products and services advancing enterprise architecture in the public sector. In healthcare, the federal government must continue to lead this effort and **drive adoption of standards** to promote an interoperable, interconnected system. Interoperability and open standards are important factors for successful adoption of life-saving and cost effective technologies such as electronic medical records and electronic prescribing. With additional resources, NASCIO is ready, willing and able to expand our educational efforts to advance public health architectures in state government.