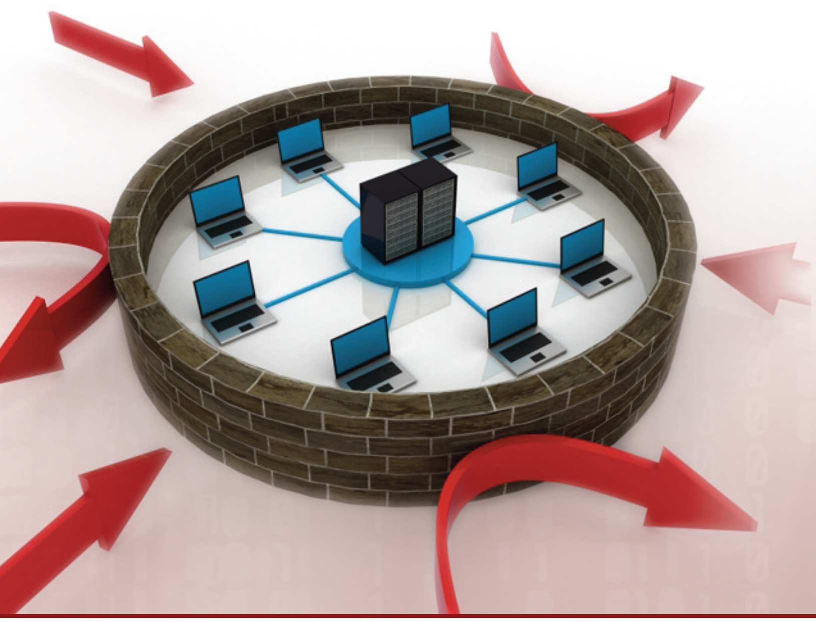


The Heart of the Matter:

A Core Services Taxonomy for State IT Security Programs

NASCIO Staff Contact:
Charles Robb
Senior Policy Analyst
NASCIO

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
NASCIO@AMRms.com
www.NASCIO.org

Why a Security Services Taxonomy?

The fiscal condition of the states is slowly recovering from the great recession, but the security resources, processes, programs, and technology that protect critical assets remain under stress. This brief arises from discussions in NASCIO's Security and Privacy Committee that relate to several factors: the chronic degree of underfunding for IT security programs within state government, in the context of significantly diminished state budgets; the transition of over half of the state CIO positions in the wake of 27 new governors in 2011; and the expanding number of states undertaking IT consolidation across the country. This discussion reflected the compelling need to deliver security adequate to meet current threats and flexible enough to protect against increasingly sophisticated cyber attacks. It also addresses an environment in which sourcing strategies are being rethought as consolidation, reorganization, outsourcing and cloud computing initiatives are being planned and implemented to drive down costs and enhance service delivery.

Whether or not a state CIO has been in his or her position for a long period of time or has just come to the job, state chief information security officers (CISOs) need to be able to communicate quickly with CIOs and high-level policy makers to explain current resource commitments and to articulate new requirements in simple but compelling language.

The seminal Deloitte-NASCIO State CISO survey conducted in 2010 provided strong evidence that state governments were spending significantly less on cyber security than their industry counter-parts.[1] NASCIO followed that survey up with a Call-to-Action in February 2011 that asked governors and other state leaders to respond to the growing threats, fiscal constraints, and to address security requirements in order to protect critical state data and operational capacity.[2] The next step in that process was to enhance the State CIO's and State CISO's ability to assess risks and better understand resource requirements by clearer articulation of the core security services that a state must provide or acquire to ensure appropriate protection of state data and operational capabilities.

Why IT Security is Critical

It is more than just a cliché that state governments run on IT – protection of the integrity, availability, and confidentiality of state data resources is essential to the operation and trustworthiness of government. As the Deloitte-NASCIO 2010 survey report stated, "People put a lot of trust in state governments to collect, maintain, and protect the appropriate information necessary to execute their programs, protect individual rights, and ensure public safety." Protecting this critical resource demands that the core services described in this document be appropriately planned, sourced, and delivered.

Put succinctly, Minnesota chief information security officer Chris Buse enunciated the problem this way: "With the Deloitte Survey and the Call-to-Action, we've basically said to government leadership that states have problems in maintaining adequate IT security, and security programs are underfunded. The issues need to be taken more seriously with greater executive attention. But, executives unfamiliar with the issues would naturally have questions about what the specific security services are, what the recommended delivery model for each service would be, and what the associated costs are. Those are the three foundational questions new CIOs would have, and a tool designed to clarify this picture, in the form of *service identification* would be of significant help to leadership." That is what the core IT security services taxonomy provides.

A deeper dive into the Deloitte-NASCIO 2010 survey, ***State Governments at Risk***, makes apparent both the funding problems faced by state IT security and the complexity of the service delivery environment security programs operate in. Fifty percent of states reported that their security budgets were from 1-3% of total IT expenditures, and trending downward, while the average spent in the private sector in the comparable financial services industry was nearer 5% and trending upward.

Perhaps as important is that 17% of the respondents to the survey could not estimate what their expenditures actually were at the time of the survey. That stems from the problem that many state security programs lack enterprise authority and budget visibility, and the CIO or state CISO have inadequate information concerning the security-related expenditures that relatively independent state agencies are making to protect resources. Some have suggested that the funds to appropriately support IT security are actually there, but are embedded in agency line of business budgets and are difficult to identify – that there is a crisis in prioritization. Integrating security programmatic functions is another goal service identification addresses.

Call-to-Action Recommendations

NASCIO's call-to-action for the states drew attention to the criticality of protecting states' data and urged strongly that as states undertake consolidation efforts, they should reexamine decentralized and stovepiped computing models and take advantage of enterprise approaches to reduce redundancies and shared existing or need IT services. This general analysis of services should include IT security requirements, and there is obvious value in identifying and agreeing on a core security services taxonomy, recognizing the benefits of a common vocabulary for describing services that must be provided to meet the requirements of security standards frameworks defined by the Federal government and various standards bodies. In looking at services, it is illustrative to draw from the experiences of several states that have independently looked at security service delivery models from the standpoints of appropriate funding strategies and the development of consolidated/enterprise services.

Core IT Security Services

The core services taxonomy divides security services into two main categories: I – Governance, Risk and Compliance Services, and II – Operational Security Services. Under those primary categories, the taxonomy identifies twelve sub-categories. (See Figure 1.)

The goal of the committee was to develop a list of categories that was inclusive, so that every IT security-related function performed by a hypothetical state IT security program would be on this list or nest under one of the subcategory headings. It was a further assumption that no state security program may do all of these functions or be solely responsible for them — they are, instead, representative of all the functions that need to be performed to ensure adequate information security within the context of appropriate risk assessment.

It was also assumed that some organizations or programs might disagree with some of the categories or consider there to be more or fewer core services. However, it was agreed that NASCIO's identification of this core would facilitate standardization across state programs – a state might disagree with the NASCIO core, while documenting how it mapped its own programs against the taxonomy. This in turn facilitates comparison of state programs, and ongoing reportage of program status, funding levels, etc.

Figure 1

Governance, Risk, and Compliance Services

1. Information Security Program Management
2. Secure System Engineering
3. Information Security Training and Awareness
4. Business Continuity
5. Information Security Compliance

Operational Security Services

6. Information Security Monitoring
7. Information Security Incident Response and Forensics
8. Vulnerability and Threat Management
9. Boundary Defense
10. Endpoint Defense
11. Identity and Access Management
12. Physical Security

The following section provides service categories, defines the scope of the individual services, and describes the key activities and tools employed in the delivery of the service.

Governance, Risk, and Compliance Services

1. Information Security Program Management

Description

Responsible for the planning, oversight, and coordination of all information security activities

Key Activities

- Align security program activities and staff with a generally accepted best practice framework
- Oversee the creation and maintenance of information security policies, standards, procedures, and guidelines
- Create and maintain strategic and tactical plans
- Coordinate the movement of plans, policies, standards, and other authoritative documents through a governance process
- Track information security risk key performance indicators
- Disseminate security metrics and risk information to executives and other managers for decision making
- Coordinate security efforts with local government entities and other branches of government

Tools

- Governance, risk, and compliance software
- Recognized information security program framework, such as NIST or ISO
- Standardized position descriptions

*In numerous publications, calls-to-action, and policy statements, NASCIO has consistently promoted enterprise approaches to IT security oversight and the integration of those into the larger enterprise administration of IT within state governments. More specifically, it has discussed the various security framework standards that CIOs and CISOs must integrate or address in the planning and execution of state IT security programs, most recently in its 2009 publication, **Desperately Seeking Security Frameworks - A Roadmap for State CIOs**.*

2. Secure System Engineering

Description

Responsible for designing appropriate security controls in new systems or systems that are undergoing substantial redesign, including both in-house and outsourced solutions

Key Activities

- Integrate information security design requirements in the system development life cycle
- Participate as a security consultant on significant technology projects
- Assist with the creation of system security plans, outlining key controls to address risks
- Assist with the creation of residual risk documentation for management acceptance
- Integrate security requirements into contracts for outsourced services
- Assist with the creation of information security policies, standards, procedures, and guidelines
- Assist with the creation of secure configuration standards for hardware, software, and network devices
- Integrate security requirements into contracts for outsourced services

Tools

- Standardized system security planning template(s)
- Governance, risk, and compliance software
- Various operational security tools
- Best practice frameworks for the management of IT, such as ITIL

3. Information Security Training and Awareness

Description

Responsible for providing employees at all levels with relevant security information and training to lessen the number of security incidents

Key Activities

- Coordinate general security awareness training for all employees and contractors
- Coordinate security training for groups with specialized needs, such as application developers
- Provide persistent and regular messaging relating to cybersecurity threats and vulnerabilities

Tools

- Learning management system

*NASCIO participates annually in Cyber Security Awareness Month activities to promote greater awareness for both public officials and citizens. It coordinates these activities with the Department of Homeland Security, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and StaySafeOnline.org. For the 2011 awareness campaign, NASCIO has updated its **Cyber Security Awareness and Resource Guide**, which describes cyber awareness training and education initiatives taking place in state governments across the country. See the NASCIO website at NASCIO.org for further details.*

4. Business Continuity

Description

Responsible for ensuring that critical business functions will be available in a time of crisis

Key Activities

- Coordinate business impact analysis
- Development of appropriate recovery strategies for services
- Develop disaster recovery plans for identified key technologies
- Coordinate testing to ensure that services can be recovered in the event of an actual disaster

Tools

- Business continuity planning software
- Business impact analysis software
- Governance, risk, and compliance software
- Automated contact tool
- Incident management tool

5. Information Security Compliance

Description

Responsible for validating that information security controls are functioning as intended

Key Activities

- Coordination of ongoing assessments of key security controls in both in-house and outsourced systems
- Completion of independent "pre-production" assessments of security controls in new systems or systems that are undergoing substantial redesign
- Coordination of all IT audit and assessment work done by 3rd party auditors
- Monitoring of 3rd parties' compliance to state security requirements

Tools

- Generalized audit and data analysis software
- Various operational security tools
- Configuration compliance management software

Operational Security Services

6. Information Security Monitoring

Description

Responsible for gaining situational awareness through continuous monitoring of networks and other IT assets for signs of attack, anomalies, and inappropriate activities

Key Activities

- Create and implement an event logging strategy
- Place sensors, agents, and security monitoring software at strategic locations throughout the network
- Monitor situational awareness information from security monitoring and event correlation tools to determine events that require investigation and response
- Disseminate potential security events to the information security incident response team

Tools

- Host and network-based intrusion detection and prevention systems
- Security information and event management system
- Network traffic flow analysis (Netflow) system
- Email and messaging security gateway software
- Web content filtering software
- Data loss prevention software

7. Information Security Incident Response and Forensics

Description

Responsible for determining the cause, scope, and impact of incidents to stop unwanted activity, limit damage, and prevent recurrence

Key Activities

- Manage security incident case assignments and the security investigation process
- Mobilize emergency and third party investigation and response processes, when necessary
- Consult with system owners to help quarantine incidents and limit damage
- Consult with HR on violations of appropriate use policy
- Communicate with law enforcement, when necessary

Tools

- Information security forensic investigation software
- Various operational IT and security tools, as situations dictate
- Case management software

8. Vulnerability and Threat Management

Description

Responsible for continuously identifying and remediating vulnerabilities before they can be exploited

Key Activities

- Strategic placement of scanning tools to continuously assess all information technology assets
- Implement appropriate scan schedules, based on asset criticality
- Communicate vulnerability information to system owners or other individuals responsible for remediation
- Disseminate timely threat advisories to system owners or other individuals responsible for remediation
- Consult with system owners on mitigation strategies

Tools

- Host vulnerability scanning software
- Web application vulnerability scanning software
- Database vulnerability scanning software
- Commercial or government threat advisory service

9. Boundary Defense

Description

Responsible for separating and controlling access to different networks with different threat levels and sets of users to reduce the number of successful attacks

Key Activities

- Assist with the development of a network security architecture that:
  - □ includes distinct zones to separate internal, external, and DMZ traffic
  - □ segments internal networks to limit damage, should a security incident occur
- Participate in the change management process to ensure that firewall, router, and other perimeter security tools enforce network security architecture decisions
- Periodically recertify perimeter security access control rules to identify those that are no longer needed or provide overly broad clearance

Tools

- Firewall rules
- Router access control lists
- Virtual private networks

10. Endpoint Defense

Description

Responsible for protecting information on computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft

Key Activities

- Manage processes and tools to detect malicious software
- Manage processes and tools that only permits trusted software to run on a device, commonly referred to as white listing
- Manage processes and tools to prevent certain software from running on a device, commonly referred to as blacklisting
- Manage processes and tools to identity unauthorized changes to secure configurations
- Manage processes and tools to encrypt sensitive data

Tools

- Malicious software protection (Anti-virus)
- Host-based intrusion detection and prevention systems
- White and Black Listing Software
- Configuration compliance software
- Data encryption software

*The IT security community has recognized for years that mobile devices create extraordinary vulnerabilities for states. NASCIO addressed mobile device security in a July 2009 publication, **Security at the Edge - Protecting Mobile Computing Devices**. This document was supplemented with **Security at the Edge Part II** in 2010, to address policy concerns more specifically. The increased penetration of powerful consumer-based devices in the workplace continues to challenge state IT programs and is a trend the Security and Privacy Committee continues to monitor and discuss.*

11. Identity and Access Management

Description

Responsible for managing the identities of users and devices and controlling access to resources and data based on a need to know

Key Activities

- Maintenance of identities, including both provisioning and de-provisioning
- Enforce password policies or more advanced multifactor mechanisms to authenticate users and devices
- Manage access control rules, limiting security access to the minimum necessary to complete defined responsibilities
- Periodically recertify access control rules to identify those that are no longer needed or provide overly broad clearance
- Restrict and audit the use of privileged accounts that can bypass security
- Define and install systems to administer access based on roles
- Generate, exchange, store, and safeguard encryption keys and system security certificates

Tools

- Identity and access management software
- Operating system and application-based security software
- Multi-factor authentication solutions, including smart cards

NASCIO's State Digital Identity Work Group has provided a consensus based forum that enables State Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Enterprise Architects and line of business stakeholders to collaborate on developing recommendations on federated identity management initiatives. This working group has served as a focal point for discussion of state-level IAM issues and the developing trust frameworks being promoted by the federal government through the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative. See archived workgroup webinars and the NASCIO website for further details.

12. Physical Security

Description

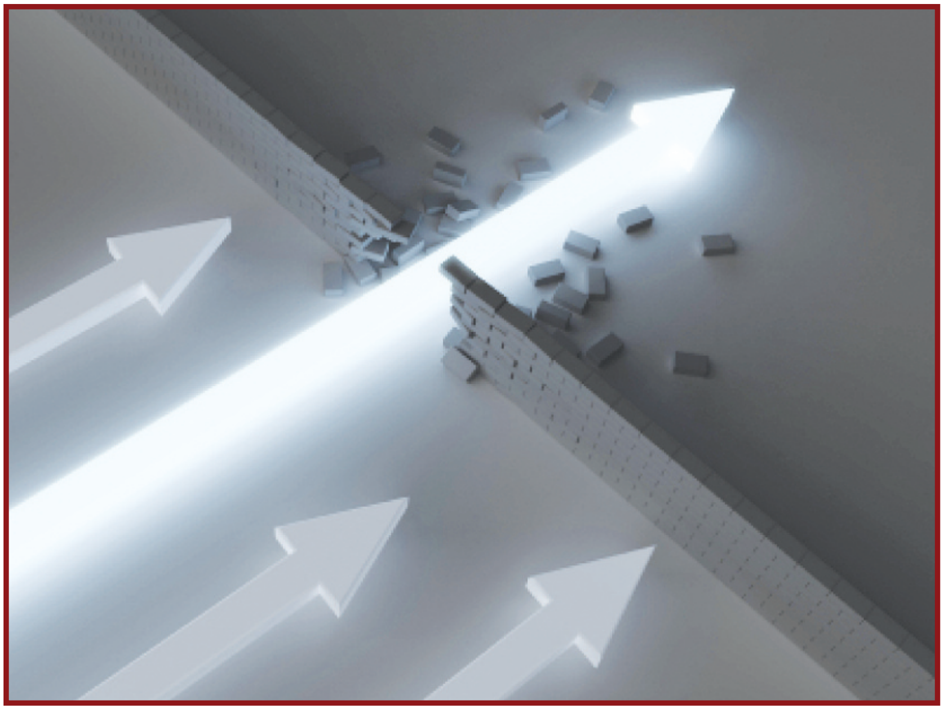
Responsible for protecting information systems and data from physical threats

Key Activities

- Maintain facility entry controls and badging systems
- Manage equipment and media destruction processes
- Maintain building emergency procedures
- Perform screening/background checks on job applicants
- Implement controls to mitigate facility vulnerabilities

Tools

- Card readers and badging systems



Use of the Services Taxonomy

Agreeing upon and using this set of terms for describing core IT security services creates an opportunity for state CIOs and CISOs to do several things:

- Most critically, the taxonomy should be used by individual states to assess current programmatic capabilities, expenditures, and weaknesses within each of the core IT security service areas. This analysis, in the context of risk-based IT security frameworks like the Consensus Audit Guidelines (CAG), will provide clear decision points for state leadership as budgetary constraints create continuing pressure to reduce expenditures.

- In light of the number of IT consolidation initiatives that are active across the states, it can be used to inform discussions of the services that are ideally performed centrally versus those which are distributed. Figure 2 below provides an illustration of how the states of Florida and Minnesota have used comparable service identifications and analysis to establish or strengthen enterprise security programs.

- In decentralized environments, the taxonomy can be used as a common vocabulary across lines of agency authority and allow better assessment of the total costs being expended to fulfill the service requirement. In the current fiscal environment most states find themselves in, it is vital that every dollar invested in IT security be visible to decision-makers, and that it be spent appropriately and its impact maximized. As referenced above, many state CISOs have difficulty determining the level of aggregate security spending. This common vocabulary should make it simpler for agencies to identify and report their security expenditures.

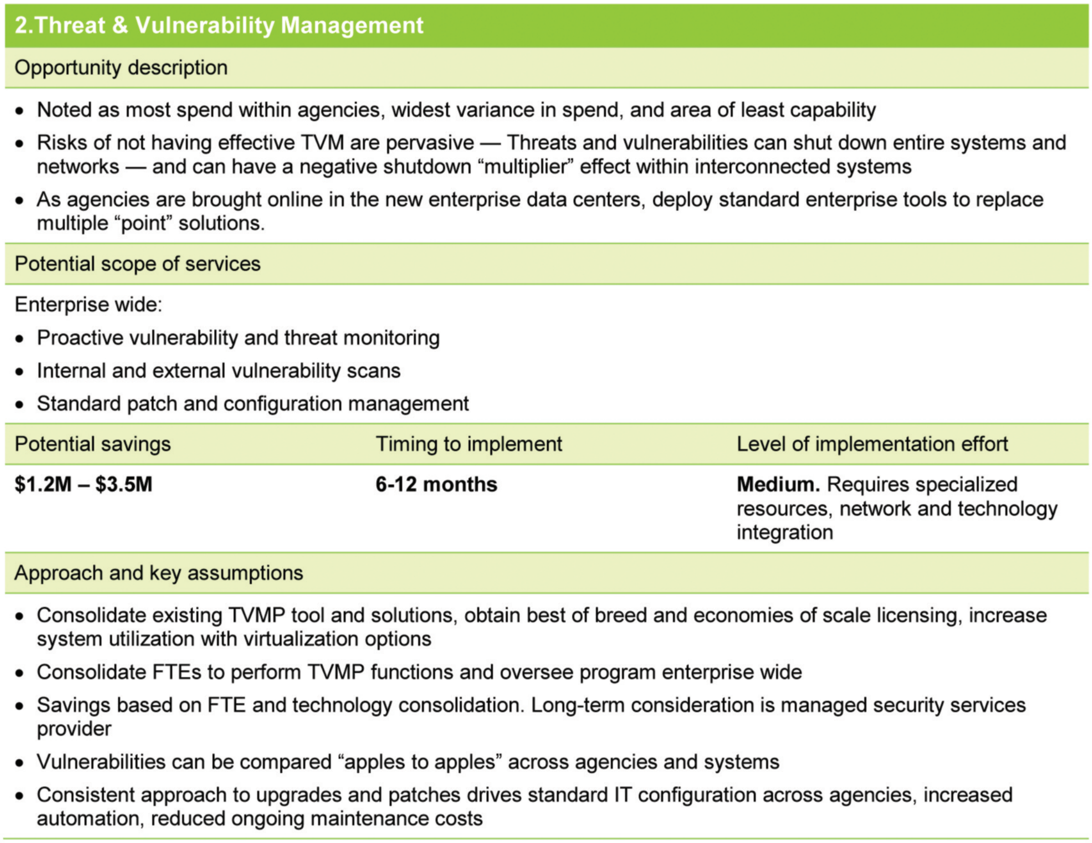
- It can be used to enhance the assessment of programs against those of other states and to identify potential services that can be performed consortially through multi-state collaboration.

- It can be used as states move to use of cloud computing services to ensure that security requirements are well-articulated and understood both on the provider side and the business side.

Figure 2

Two state programs, in Florida and Minnesota, have been asked by their legislatures to assess enterprise security requirements as part of IT consolidation efforts. Minnesota developed a core services list that included a larger number of services, and this formed the basis of NASCIO's initial discussions of the security services taxonomy. Minnesota's service identification was used as a part of the legislative report, and its analysis was extended to assess FTI costs for each service and to make recommendations about the sourcing of each service, which series were better handled centrally, and which were best left distributed.[3]

Florida conducted a very similar analysis of core security services and the following figure is an example of how Florida used the core services to assess potential enterprise savings:



2.Threat & Vulnerability Management

Opportunity description

- Noted as most spend within agencies, widest variance in spend, and area of least capability
- Risks of not having effective TVM are pervasive — Threats and vulnerabilities can shut down entire systems and networks — and can have a negative shutdown "multiplier" effect within interconnected systems
- As agencies are brought online in the new enterprise data centers, deploy standard enterprise tools to replace multiple "point" solutions.

Potential scope of services

Enterprise wide:

- Proactive vulnerability and threat monitoring
- Internal and external vulnerability scans
- Standard patch and configuration management

Potential savings	Timing to implement	Level of implementation effort
$1.2M – $3.5M	**6-12 months**	**Medium.** Requires specialized resources, network and technology integration

Approach and key assumptions

- Consolidate existing TVMP tool and solutions, obtain best of breed and economies of scale licensing, increase system utilization with virtualization options
- Consolidate FTEs to perform TVMP functions and oversee program enterprise wide
- Savings based on FTE and technology consolidation. Long-term consideration is managed security services provider
- Vulnerabilities can be compared "apples to apples" across agencies and systems
- Consistent approach to upgrades and patches drives standard IT configuration across agencies, increased automation, reduced ongoing maintenance costs

The assessment in Florida allowed its security program to identify core enterprise services that have become the basis of their strategic plan for IT security going forward.

The recently published 2011 State CIO Survey reported that 94% of State CIOs are considering security consolidation initiatives.[4]

The Heart of the Matter . . .

The states are slowly moving from a system-centric view to a services-centric view of their IT world and making important investment decisions on this journey. Fundamentally, the use of standard terminology to describe security services allows the CIO and the State CISO to articulate service requirements clearly and accurately whether their environments are centralized, federated, de-centralized, or a hybrid. The large-scale IT consolidation efforts that many new CIOs are leading create significant opportunities for states to more effectively match resources to risk through an enterprise approach to IT security. Similar taxonomies have proven useful in past state consolidation efforts, and many more states should be able to take advantage of the model the NASCIO taxonomy affords.

Creating greater awareness of cyber security funding problems in the states has been an important element of NASCIO's advocacy agenda over the last half decade, and in August 2010 NASCIO and the Multi-State Information Sharing and Analysis Center (MS-ISAC) co-signed a letter to the Department of Homeland Security urging that greater federal funding be applied to states through the mechanism of DHS's Homeland Security Grant Program. Related to that program, Congress in 2009 requested that the DHS develop an assessment of state cybersecurity vulnerabilities, and this month the National Cyber Security Review survey was launched. This survey will provide the first national assessment of cyber security programs at state and municipal levels, and will lead to a report early next year that is likely to address critical cyber weaknesses and opportunities. It is imperative at that point that state programs have clear and accurate pictures of their cyber security capabilities, funding needs, and expenditures. The core services taxonomy will play a critical role as CIOs conduct that analysis.

[1] State Governments At Risk: A Call to Secure Citizen Data and Inspire Public Trust. Deloitte-NASCIO 2010 Cybersecurity Study, August 2010.
[2] NASCIO Call to Action: Cybersecurity and the States, February 2011.
[3] Minnesota Comprehensive Information Security Funding Strategy, March 2010. See particularly Appendix A – Detailed Security Services Descriptions.
[4] See "Enterprise Information Technology Security Implementation Plan," Florida Agency for Enterprise Information Technology, Office of Information Security, December 2010, and "The 2011 State CIO Survey: a new C^4 agenda" NASCIO, TechAmerica, GrantThornton; October 2011.