A Current View of the State CISO: A National Survey Assessment

NASCIO
Representing Chief Information Officers of the States

www.nascio.org

September 2006

NASCIO Online
Visit us on the web for the latest information on NASCIO's Information Security and Privacy Committee.

www.nascio.org

Who We Are
NASCIO represents the state chief information officers from the 50 states, six U.S. territories, and the District of Columbia. Members include cabinet and senior level state officials responsible for information resource management. Other IT officials participate as associate members and private sector representatives may become corporate members.

AMR Management Services provides NASCIO's executive staff.

Disclaimer
NASCIO makes no endorsement, express or implied, of any products, services or websites contained herein, nor is NASCIO responsible for the content or activities of any linked websites. Any questions should be directed to the administrators of the specific sites to which this publication provides links. All information should be independently verified.

CONTENTS

KEY FINDINGS

The survey results reflect a snapshot of the role of the state CISO (Chief Information Security Officer) as of summer 2006. While not all states have a state CISO position, the results confirm that the position is an important one in which states are willing to invest. ***Eighty-three percent (83%) of the responding states have a CISO or the equivalent of that position.***

Recent NASCIO Research Brief on the Role of the State CISO: For a more in-depth examination of how the state CISO's role has evolved, please see NASCIO's Research Brief "*Born of Necessity: The CISO Evolution — Bringing the Technical and the Policy Together*" at: http://www.nascio.org/nascioCommittees/securityPrivacy/members/#publications.

From the Technical to the Policy: As the role of the state CISO has evolved in the states, state CISOs are now likely to have policy responsibilities that comprise a significant component of their overall duties. ***Sixty-nine percent (69%) of the survey respondents indicated that they have both policy and operational duties, while twenty-nine percent (29%) indicated that they have responsibilities that are more geared to the policy side.***

An Elevated Position within State Government: The survey revealed many factors that indicate the position of the state CISO is becoming a more high-profile position with more authority over enterprise IT security. These factors include the following:

- **Lines of Reporting:** Fifty-four percent (54%) of respondents report to the state CIO.
- **Scope of Authority:** Sixty percent (60%) of the survey respondents indicated that they have authority over executive branch agencies, while an additional thirty-five (35%) reported having statewide authority (including multiple branches of government).
- **Defined Security Budget:** Sixty percent (60%) of respondents have a defined security budget.
- **Enforcement Authority:** Seventy-one percent (71%) of the survey respondents have the ability to enforce IT security policies.

Moving State IT Security Forward—What State CISOs Need To Do Their Jobs: Among the many factors that were identified by the survey respondents, adequate IT staffing and personnel stood out above all others, since it was cited by twenty-seven (27) of the forty-one (41) responding states. ***With the anticipated retirement of a substantial portion of the state IT workforce over the coming years, coupled with a private sector that in many instances provides higher salaries than the public sector, the importance of adequate IT staffing will continue to rise in prominence.*** As always, adequate funding was cited as a common state CISO need. With finite state resources and the drain of ever-rising Medicaid and other state expenses, state CISOs will continue to compete for state dollars and must be able to make a successful business case for ongoing investment in IT security. Finally, other top needs of the state CISO, including the support of the CIO and the Governor or other senior state management leaders, demonstrate that building strong relationships has become the hallmark of the evolving role of the state CISO. The state CISO must educate others as to the vital nature of IT security and bridge gaps in understanding that may exist. While the state CISO alone cannot move the state to its desired IT security posture, the state CISO can lead others in a collective effort toward that goal.

The Role of the CIO Regarding Security: While part of an executive team that may include the CISO, the CIO is ultimately accountable for information security in many cases.

BACKGROUND

Background: An Overview of the World of the State CISO

An Increasingly Complex and Threatening World…
As the world has grown more complex with the advent of technologies that allow for the rapid collection, storage and distribution of vast amounts of information and data, so has the challenge of protecting state IT systems and the information that resides within them. The threats originate not only from external sources but from internal sources, too. The distributed nature of state government with IT systems spread across state agencies, and the possibility of malicious or unaware employees whose IT practices may place the state at risk, are examples of the internal threats that abound. These concerns are in addition to common external threats, such as hackers, viruses, spyware, botnets, and denial of service attacks.

Within this context the citizenry is expecting more and enhanced online applications from state government. The rise of online booksellers, auction houses and other businesses have planted seeds of expectations within citizens that they should be able to conduct business with any entity - whether public or private - on a twenty-four hour, seven-day-a-week basis. However, at the same time, due in part to the many reported data breaches within the past several years in the public, private and educational sectors, citizen trust seems to have grown fragile. Can government be trusted with the ability to protect citizens' personal information that resides within many state IT systems? Adding more layers of complexity to the environmental context are the worries about the security of all types of critical infrastructure in a post-9/11 society and sector-specific IT security and privacy regulatory requirements including HIPAA (the Health Insurance Portability and Accountability Act).

An Increasing Need for a State IT Security Policy and Strategy Leader…
The complexities of state government have spawned the need for a position with an enterprise view of IT security so that there is assurance that all state agencies meet at least minimum, reasonable IT security requirements. An excerpt from NASCIO's recently released Research Brief *"Born of Necessity: The CISO Evolution,"* explains how this complex environment has impacted the state CISO position.

The State CISO's Evolving Role: The state CISO is not merely a technical position involved in the operational aspects of IT security. Instead, the CISO is evolving as an IT security policy leader. The state CISO's responsibilities involve educating others, including those within the Governor's office, state agency leaders, legislators, and others outside of government to help ensure adequate funding for security. The ability of the CISO to form and maintain good relationships with state homeland security and emergency management leaders, and even state auditors, is now a vital part of ensuring that the technology underlying the most basic government function is secured to protect against risks that might reasonably occur.

ABOUT THE SURVEY

In summer 2006, NASCIO conducted a national survey of the state CISOs during the preparation of a Research Brief entitled *"Born of Necessity: The CISO Evolution - Bringing the Technical and Policy Together."*[1] Released in July 2006, the Research Brief highlights that the state CISO is not merely a technical position involved in the operational aspects of IT security, but is evolving as an IT security policy and strategy leader. This National Survey Assessment contains the aggregated results of the survey that was conducted in the preparation of that Research Brief. The survey results are intended to support and elaborate upon the findings of that Research Brief. Relevant excerpts of the Research Brief are highlighted throughout in gray text boxes.

This National Survey Assessment presents a snapshot of the state CISO's world during the summer of 2006. This survey was directed at the fifty states and the District of Columbia and was conducted using a web-based solution. It is intended to establish a starting point for understanding the evolution of the CISO position from technical duties, such as perimeter defense, to that of a state IT security leader. It could serve as a baseline for similar surveys in the future as the position continues to evolve in nature and importance.

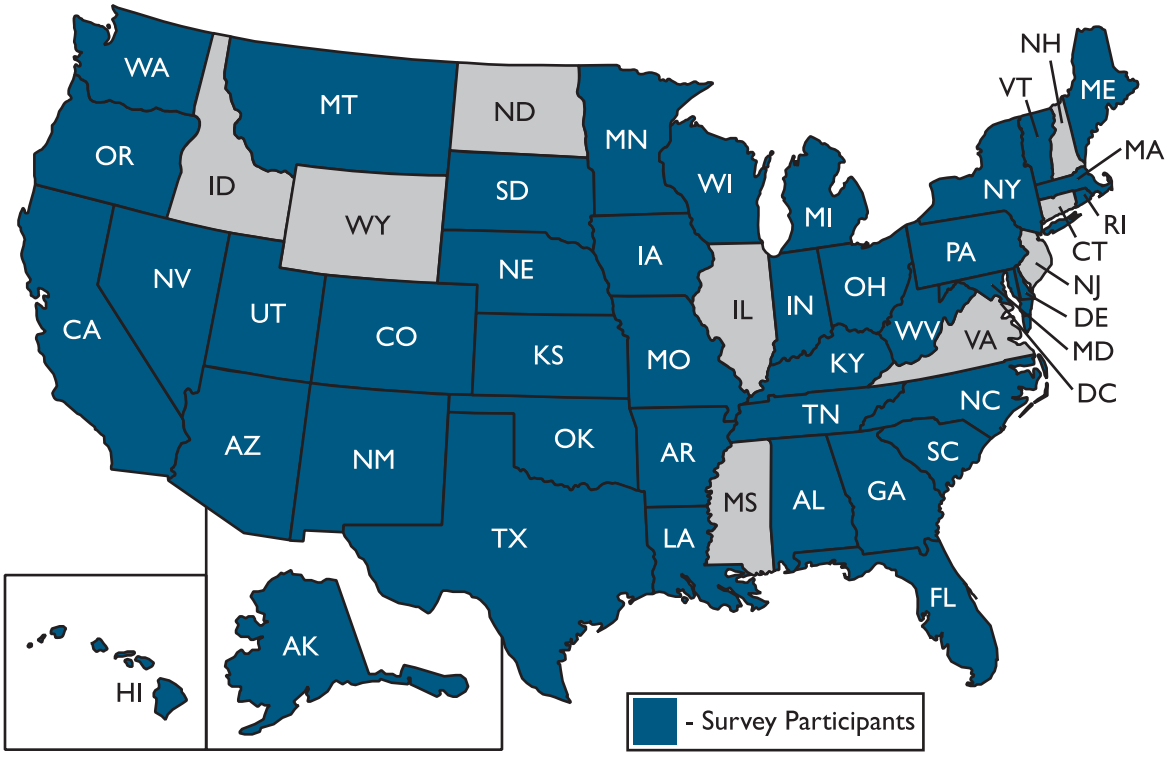
[1]"Born of Necessity: The CISO Evolution-Bringing the Technical and Policy Together," is a product of NASCIO's Information Security and Privacy Committee. To learn more about the Committee and its other publications, please see its webpage at: http://www.nascio.org/nascioCommittees/securityPrivacy/members/.

For most of the states that have a CISO position or the equivalent, the CISO responded to the survey. However, for those states that do not have a CISO, either the state CIO or another appropriate person who is familiar with the way his or her state handles IT security completed the survey.

Survey Participants

Forty-one (41) states responded to the survey. Participation included a wide distribution in geography, population and budget.

Figure 1



Alabama	Iowa	Nebraska	South Dakota
Alaska	Kansas	Nevada	Tennessee
Arizona	Kentucky	New Mexico	Texas
Arkansas	Louisiana	New York	Utah
California	Maine	North Carolina	Vermont
Colorado	Maryland	Ohio	Washington State
Delaware	Massachusetts	Oklahoma	West Virginia
Florida	Michigan	Oregon	Wisconsin
Georgia	Minnesota	Pennsylvania	
Hawaii	Missouri	Rhode Island	
Indiana	Montana	South Carolina	

PREVALENCE OF THE STATE CISO ROLE

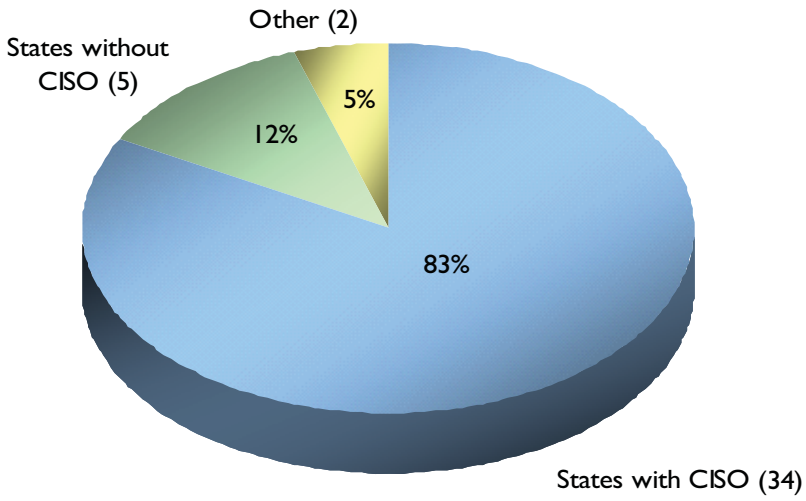
Question 1 - CISO: Are you the designated State CISO (Chief Information Security Officer) or the equivalent of that position?

- ❑ Yes (please specify)
- ❑ No
- ❑ Other

Figure 2:

Prevalence of the State CISO Role

(*41 states responding*)



An Evolving IT Security Role:
With eighty-three percent (83%) of responding states confirming that they have a state CISO or the equivalent position, IT security appears to be evolving as a strategic function that must be located at an enterprise level.

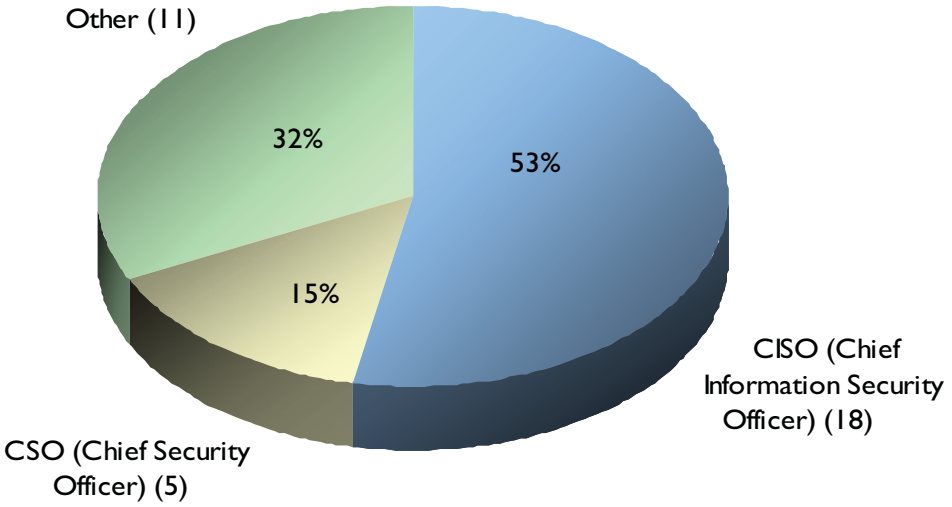
Dual Roles:
Three states indicated that their lead technology official for the state is also the state's CISO.

Note on Survey Question:
The original question asked the survey respondents whether they were the state CISO. The results above reflect those states responding in the affirmative plus those states that have a CISO but had another person (in some cases the state CIO) complete the survey.

VARIATIONS OF CISO TITLES

Variations on a Title:
By a slim majority, "Chief Information Security Officer" (CISO) is the most prevalent title in the states for the lead IT security position. Eighteen (18) survey respondents hold that title. Five (5) survey respondents hold the title of "Chief Security Officer" (CSO). This trend is consistent with similar trends within the private sector. Note that, in some cases, variations in the CISO title can denote variations in duties. For example, a "CSO" title may indicate that the titleholder's duties encompass not only IT security but physical or facilities security as well, which might include responsibilities for building access control and surveillance cameras.

Figure 3:
Variations of CISO Titles
(*34 states responding*)



Unique Titles:
One-third of the survey respondents have an "other" title. Among the more unique titles for the CISO position are the following:

- Information Security Officer
- Director of IT Security
- Homeland Security Technology Manager
- Chief Cyber Security Officer
- Cyber Protection Officer

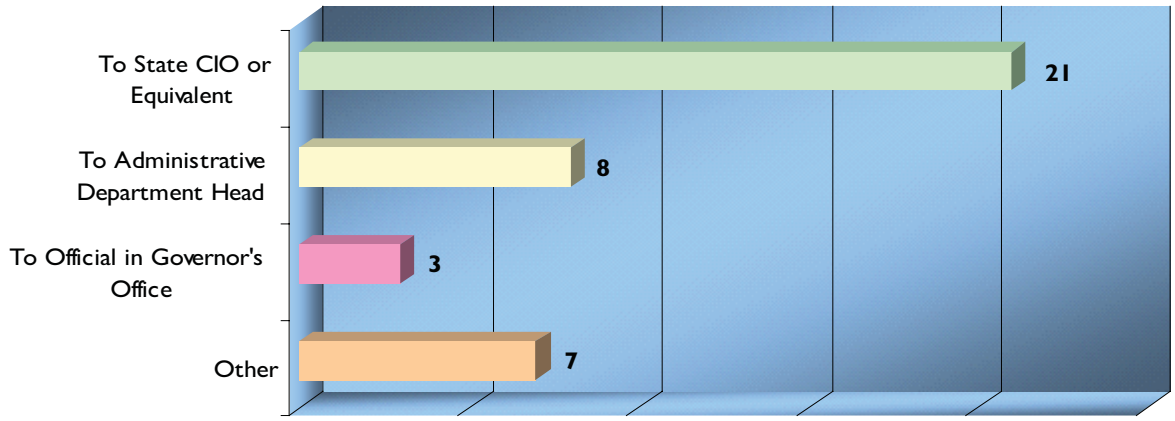
Too Many Chiefs? For states that are attempting to create a CISO position or ensure the continued existence of the position, the state CIO should be prepared for the possibility of encountering concerns from government leaders, legislators or external critics that there are "too many chiefs". The argument stems from the fact that there may be many state positions that are "chiefs," such as the "Chief" Information Officer, the "Chief" Financial Officer, the "Chief" Technology Officer, and the "Chief" Enterprise Architect. In such cases, it may be of assistance to point out that it's the function and authority of the CISO, not the title, that is important in securing state IT resources.

LINES OF REPORTING FOR STATE CISOs

Question 2 - Reporting: To whom do you directly report?

- ❑ State CIO or equivalent
- ❑ Administrative Department Head
- ❑ State Homeland Security Director
- ❑ Official in the Governor's Office
- ❑ Other

Figure 4:
Lines of Reporting for State CISOs
(*39 states responding*)



An Elevated Position:
The majority of survey respondents report to the state CIO or equivalent position, while a lesser number report to an administrative department head. Three (3) survey respondents indicated that they report to an official in the Governor's office. The survey results reflect the fact that the state CISO position has risen through the ranks to the upper-levels of state government, giving the state CISO an enterprise-view of IT security. Elevating the position of the state CISO to report to the state CIO or other high-level state government official has necessitated that state CISOs now embrace the importance of establishing relationships with a variety of stakeholders across the state enterprise, such as state homeland security and emergency management officials.

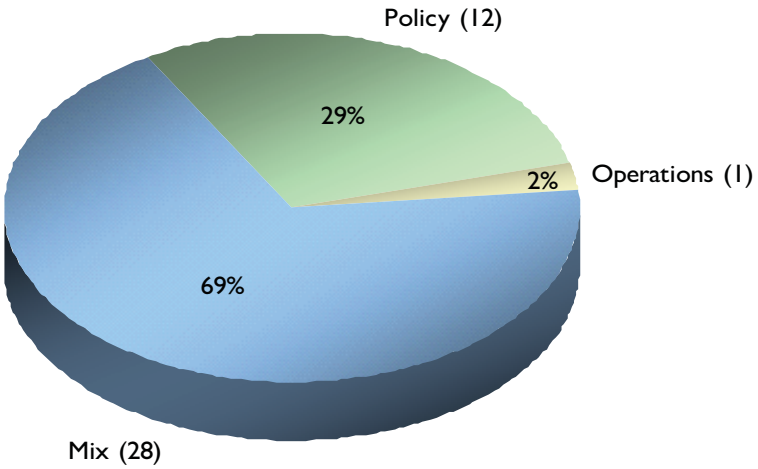
Relationships Matter: As a result of the increasingly prevalent role of the CISO as a strategist for state IT security, it has become important for CISOs to develop strong relationships with many stakeholders inside and outside of state government. In particular, state CISOs are likely to become more involved in state homeland security, critical infrastructure, protection and emergency management efforts as they relate to state IT systems and cybersecurity. In addition, the state CISO may also need to leverage relationships with other state agencies and processes, including procurement, budget and human resources.

THE PRIMARY FOCUS OF STATE CISO DUTIES

Question 3 - Duties and Responsibilities: Are your duties and responsibilities focused more on which of the following?

- ❑ The policy-side (planning, business strategy, enterprise architecture, policy formulation, budgeting)
- ❑ The operational-side (network monitoring, perimeter defense, threat analysis, training)
- ❑ A mix of both?

Figure 5:
The Primary Focus of State CISO Duties
(*41 states responding*)



Policy Duties are a Part of the Mix:
Over two-thirds of the survey respondents indicated that they have a mix of both policy duties (planning, business strategy, enterprise architecture, policy formulation, budgeting and related activities) and operational duties (network monitoring, perimeter defense, threat analysis, and training). When taken together with the other twenty-nine percent (29%) of respondents who indicated having primarily policy-related duties, the picture becomes apparent. State CISOs generally have policy-related duties, although they likely are balanced with operational duties. The survey results confirm that, as the state CISO position has become elevated within many states, the position has taken on policy-related duties. State IT security no longer focuses solely on perimeter defense and other operational duties, but also now includes the formulation of enterprise policies to help protect IT systems across the state.

Other Duties:
Other duties listed by the survey respondents included:

- Physical security for government infrastructure
- Statewide 911 services
- Forensic investigations
- Enforcement role with respect to state homeland security.

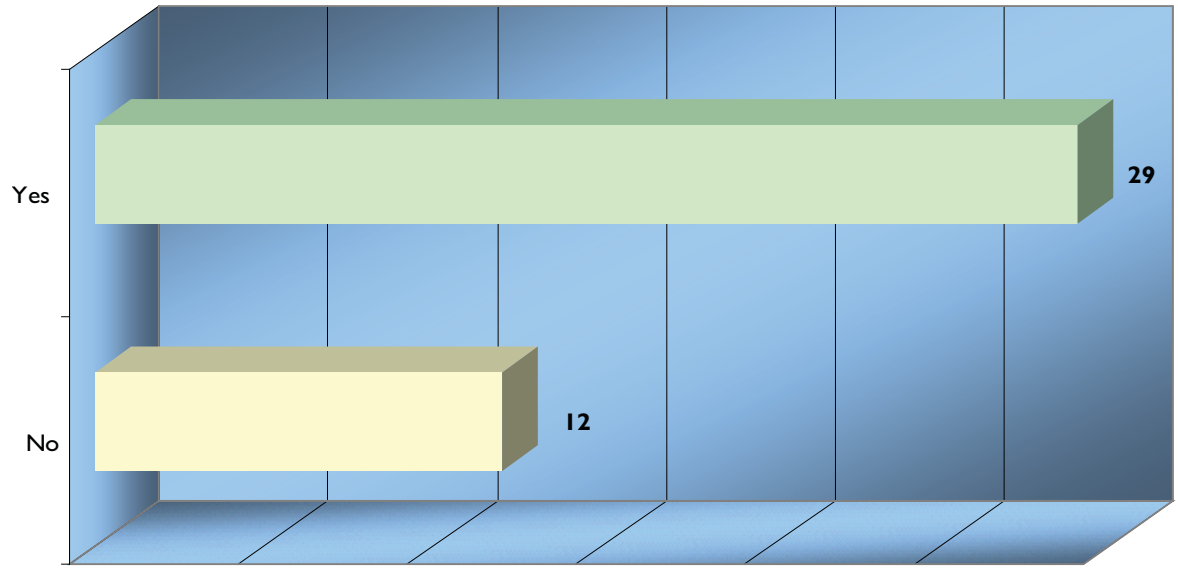
The Emerging Role of the CISO as Security Strategist and Business Enabler: As IT security has increased in importance, so have the policy and strategy-related duties of the state CISO. The position has evolved from operations to more of a policy and security-strategy position. The state CISO may also seek to build support from others within the state by demonstrating how IT security can actually enable improved business processes and services.

AUTHORITY TO ENFORCE ENTERPRISE IT SECURITY POLICIES

Question 4 - Enforcement/Compliance: Do you have authority to enforce compliance with enterprise IT security policies?

- ❑ Yes
- ❑ No, policies formulated by the CISO are primarily enforced by: [please specify which agency or entity holds enforcement authority]
- ❑ No, my duties do not include policy development

Figure 6:
Authority to Enforce Enterprise IT Security Policies
(*41 states responding*)



A Majority with Enforcement Authority:
Over two-thirds of the survey respondents indicated that they have authority to enforce enterprise IT security policies.

Enforcement Responsibilities of Other State Entities:
Although less than one-third of the respondents do not have enforcement authority, other entities in those states primarily handle that responsibility. Examples of state entities with that authority include:

- Agency Directors
- Auditor/Department of Audits
- Legislative Auditor
- State IT Security Council
- Department of Administration.

DEFINED SECURITY BUDGET SUPPORTING STATE CISO DUTIES

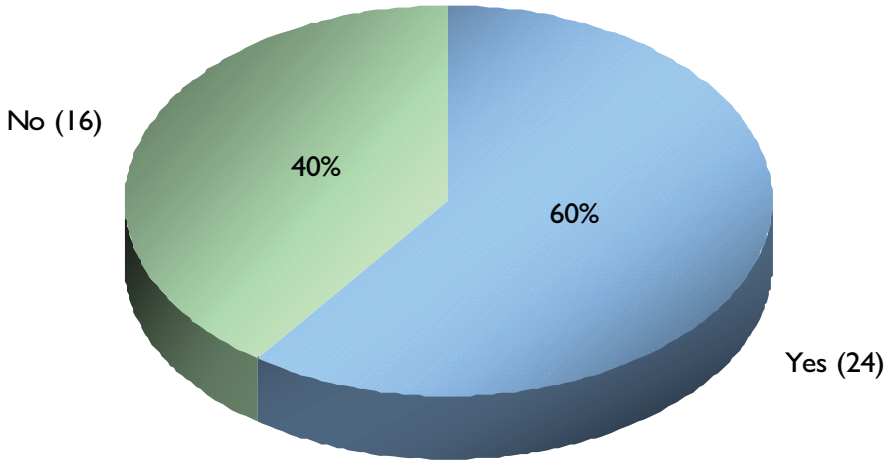
Question 5 - Security Budget: Do you have a defined budget to support your CISO duties?

- ❑ Yes
- ❑ No

Figure 7:

Defined Security Budget Supporting State CISO Duties

(*40 states responding*)



The Benefits of a Defined Security Budget:

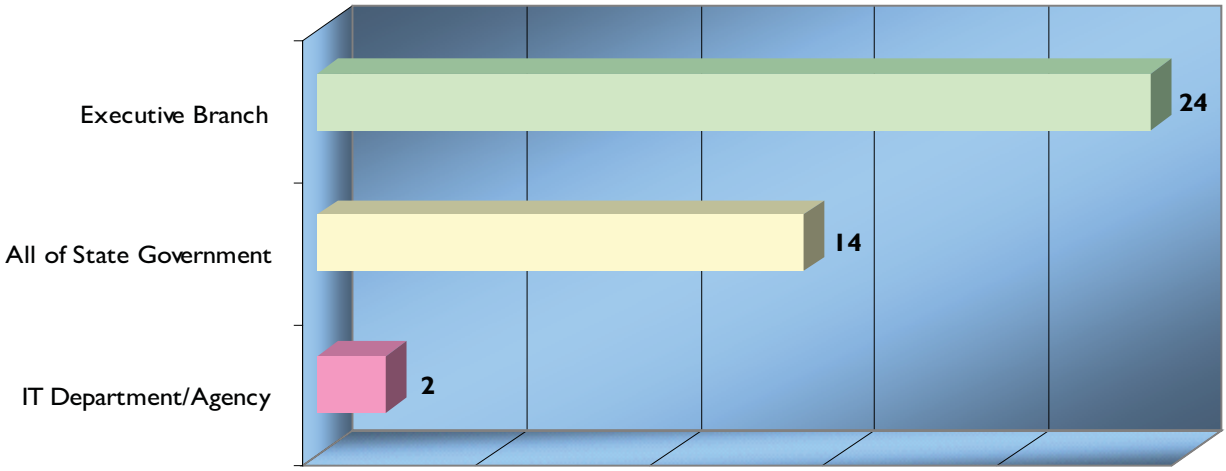
Sixty percent (60%) of the survey respondents have a defined security budget supporting the duties that they carry out to protect state IT systems. With allocated funds that are dedicated to securing state IT systems, the CISO has increased control to ensure that resources are being properly divided in order to achieve the state's desired short-term and long-term IT security posture. It also serves as an indicator that state leaders place importance on IT security.

SCOPE OF CISO AUTHORITY

Question 6 - Scope of Authority: For which of the following do you have responsibility?

- ❑ Your IT Department/Agency Only
- ❑ Executive Branch
- ❑ All State Government (Executive, Legislative and Judicial branches)

Figure 8:
Scope of CISO Authority
(*40 states responding*)



Extent of CISO Authority in State Government:
The state CISO is taking on an enterprise-wide span with sixty (60%) of respondents reporting authority over the executive branch and in excess of one-third of respondents reporting authority that extends to all state government (including multiple branches). With this type of enterprise view, the state CISO must build relationships across agencies and even branches of government. As many states pursue consolidation efforts, it is likely that this trend will continue into the future with increasingly consolidated CISO authority.

Depth and Breadth of CISO Authority: State CISOs normally have authority at least with respect to the executive branch of government, if not for the entire state government enterprise, including other branches of government. Regarding state agencies, many states take a "federated" approach, with state agencies having an information security officer or an IT security point of contact that may report to the agency head.

PREVALENCE OF CERTIFICATIONS FOR STATE CISOs

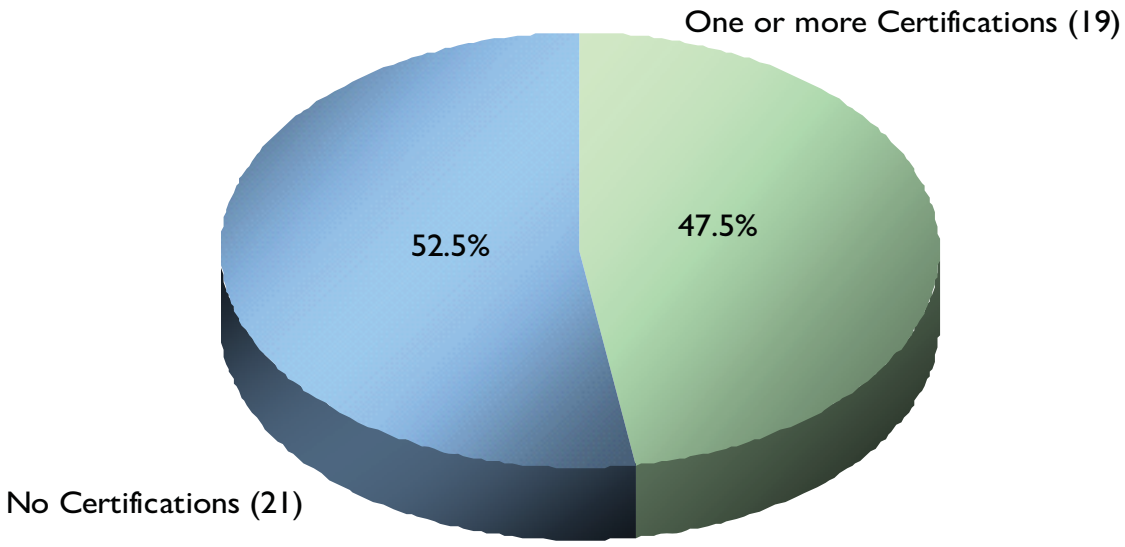
Question 7 - Certifications: Do you have an IT security certification (check as many as apply)?

- ❑ Yes, CISSP (Certified Information Systems Security Professional)
- ❑ Yes, CISM (Certified Information Security Manager)
- ❑ Yes, CISA (Certified Information Security Auditor)
- ❑ Yes, SANS Institute GIAC (Global Information Assurance Certification)
- ❑ Yes, Other [please specify]
- ❑ No

Figure 9:

Prevalence of Certifications for State CISOs

(*40 states responding*)



Certifications:

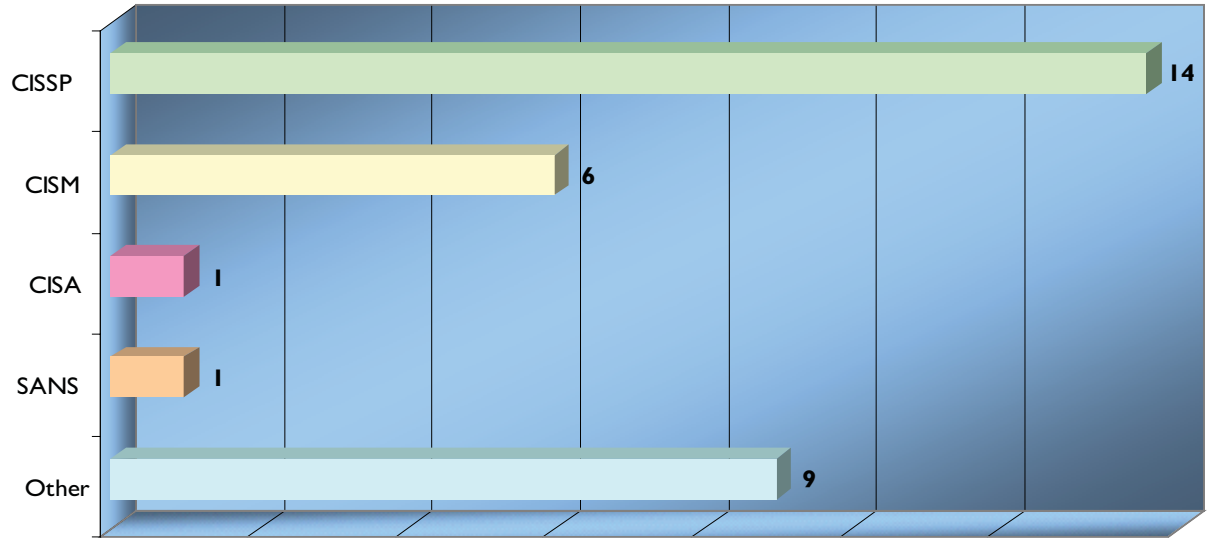
A very slight majority of state CISOs do not hold a certification that is related to IT security. However, 47.5% hold at least one certification. It should be noted that, generally, those state CISOs who do not hold certifications have gained their IT security expertise through years of "hands-on" work in IT security or closely related fields.

CISO Skills: As opposed to a purely technical position, state CISOs now have a balance of technical, policy and "business" related skills. Important skills are communications, building relationships, and understanding security and security management.

TYPES OF CERTIFICATIONS FOR STATE CISOs

One Certification vs. Many:
Interestingly, of those state CISOs holding certifications, just less than half hold one certification, while just over half hold multiple certifications (two or more).

Figure 10:
Types of Certifications for State CISOs



Many Types of Certifications:
While the Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) are the most popular state CISO certifications, other certifications of the survey respondents included:

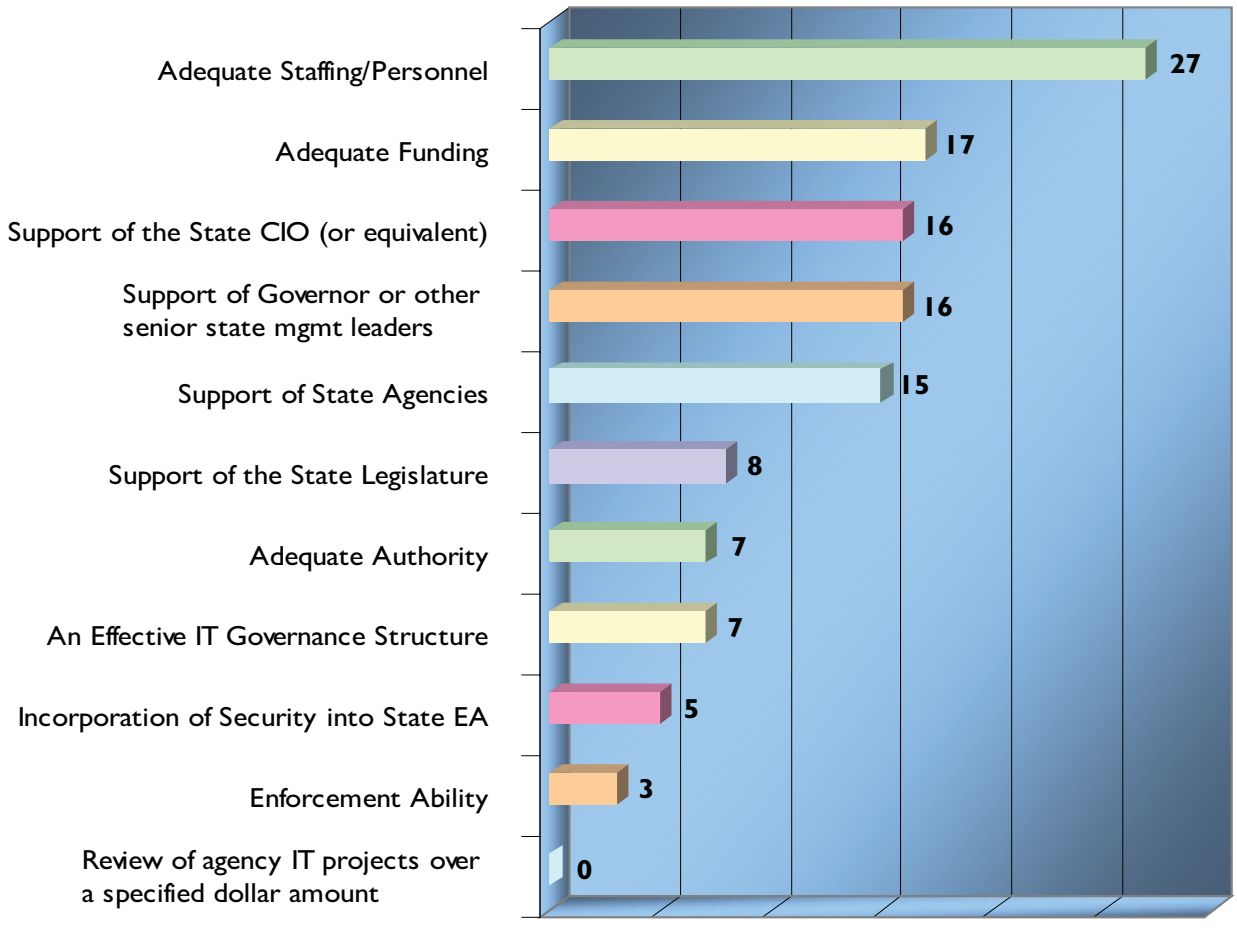
- Certified Fraud Examiner (CFE)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Network Associate (CCNA)
- Security+
- Continuity of Operations Planning (COOP) through FEMA
- Certified Business Continuity Planner (CBCP)
- Systems Security Certified Practitioner (SSCP)
- EnCase Certified Examiner (EnCE)
- Certified Information Forensics Investigator (CIFI)
- Microsoft Certified Systems Engineer (MCSE)
- Red Hat Certified Engineer (RHCE)
- Certified Information Privacy Professional/Government (CIPP/G).

WHAT STATE CISOs REALLY NEED TO DO THEIR JOBS

Question 8 - State CISOs: What Do You Really Need? What are the top three items/resources that you need in order to do your job (please check three)?

- ❑ Support of the State CIO (or equivalent)
- ❑ Support of the Governor or other senior state management leaders
- ❑ Support of state agencies
- ❑ Support of the State Legislature
- ❑ Adequate authority
- ❑ Adequate funding
- ❑ Adequate staffing/personnel
- ❑ Enforcement ability
- ❑ Incorporation of security into state enterprise architecture
- ❑ An effective IT governance structure
- ❑ Review of agency IT projects over a specified dollar amount

Figure 11:
What State CISOs Really Need to do their Jobs



Tier 1 Priority—The Importance of Adequate Staffing:
The state CISOs were asked to select from a list of 11 items the top three that they needed to do their jobs. According to the responding states, the overwhelming majority of state CISOs need adequate staffing/personnel in order to perform their jobs. The prevalence of this response far exceeded all others.

Tier 2 Priorities—Funding and the Support of Stakeholders:
After adequate staffing, adequate funding is the next most important item followed by the support of the CIO and the support of the Governor or other senior state management leaders in a tie. Close behind those, the state CISOs listed the support of state agencies as a priority. Since sufficient funding is an ever-present necessity, NASCIO published a recent Research Brief on that topic entitled, "*The IT Security Business Case: Sustainable Funding to Manage the Risks.*" Moreover, as the state CISO position is elevated in importance, the value of relationship-building increases as well as the need for support from a variety of stakeholders, including the Governor, CIO and state agency leaders.

Tier 3 Priorities:
The need for the support of the state legislature leads the Tier 3 state CISO priorities. Slightly behind that priority are the need for adequate authority and an effective IT governance structure in a tie. Incorporation of security into a state's enterprise architecture and enforcement ability follow in that descending order. This reflects the fact that the state CISO position is becoming established in many states. Hence, state CISOs now do not have to justify the need for their positions as much as they now have to forge relationships within the state and with external stakeholders in order to carry out their duty to secure state IT systems and infrastructure.

Training & Continuing Education: It is important for state CIOs to have the resources for ongoing, specialized training for state CISOs and IT security staff members.

The Compensation Challenge: Compensation for CISOs can be a challenge. One option is to pay them as close to commensurate with the private sector as possible. Other options include an emphasis to potential job applicants on quality of life and good retirement packages.

HOW DO CISOs SPEND MOST OF THEIR TIME?

Open Comment Question 9 - How You Spend Most of Your Time: On what activity or issue do you spend most of your time?

Policy and Strategy:
Many state respondents spend a significant portion of their time working on policy development. A few respondents also identified the importance of protecting citizens' information privacy as part of their role and determining where the linkages are between security and privacy. The policy aspect of state CISO duties is also closely related to strategic planning tasks that have a goal of moving the state toward its desired long-term security posture.

Maintaining Ongoing IT Security Investment:
Since continuing the investment of funds and other resources is needed to support IT security activities and measures, many CISOs are involved in making the IT security business case to various state government stakeholders, including state legislators and high-level executive branch leaders.

Day-to-Day Management:
State CISOs spend significant portions of their days dealing with staffing issues, including recruiting and staff management. For some states, this also includes the initial establishment of a statewide cyber-security office.

Building Bridges:
State CISOs also spent time coordinating and consulting with state agencies on the implementation of IT security policies, training and awareness, and risk mitigation. In some cases, this also may include policy enforcement and compliance. As the role of the CISO has been elevated within the state organization, CISOs likely spend increased amounts of time working with others across the state, including with state homeland security and emergency management officials, as well as with the federal and local levels of government and the private sector.

Technical Issues:
In addition to these duties, many CISOs still have operational responsibilities ranging from regular log review and monitoring to providing network security to risk assessments.

THE LIFE OF THE BUSY STATE CISO

Below is a list of the types of activities on which many state CISOs spend most of their time.

Policy-Related Activities:

- Developing and formalizing security policies, guidelines and standards
- Developing privacy policies and procedures
- Policy assessments for new and existing applications
- Policy and governance issues

Enterprise Planning and Strategy Activities:

- Addressing technology planning issues
- Strategic direction and planning
- IT planning for state agencies
- Enterprise-wide disaster recovery/business continuity planning
- Working on the state's long-term security posture and goals
- Issue prioritization
- Statewide technology procurements

IT Security Business Case:

- Developing a business case strategy for implementing an enterprise-focused CISO
- Developing a business justification for strategic security functions
- IT security budget issues

Administrative Activities:

- Establishing a statewide cyber-security office
- Creating positions that will bring the right mix of employees to the IT security team
- Recruiting
- Security staff/team management
- Program management

Relationship-Building with State Agencies and Others:

- Developing a federated model to work with state agencies
- Building partnerships and getting buy-in from state agencies on security
- Consulting with state agencies (including agency CIOs and ISOs)
- Consulting with enterprise architecture
- Education and awareness at all levels
- Educating agencies that security is a business issue, not just a technology issue
- Helping agencies drive enterprise IT security
- Communicating threat mitigation strategies
- Security standards compliance
- Policy enforcement
- Building relationships with state homeland security and emergency management officials and those at the federal and state levels as well as the private sector

Technical/Operational Activities:

- Prevention-based consulting and analysis regarding IT technical infrastructure
- Operational support
- Equipment configuration
- Generalized "firefighting"/running from one technical fire to another
- Research
- Threat assessment
- Risk assessments
- Risk mitigation/management
- Answering questions related to access control policies and implementation of controls
- Incident response
- ISP and content filtering
- Review and monitoring of logs
- Network monitoring
- Forensic investigations
- Security architecture.

What's Privacy Got To Do with It? States are still determining where best to address the information privacy function regarding personal or sensitive information within state IT systems. Some state CISOs may handle privacy-related issues, while others may not. As the privacy function emerges and takes shape within the states, so will the CISO's relationship with state privacy officers or the equivalent.

Accountability: Collecting and analyzing state data is an important way to measure CISO success and outcomes.

SUMMARY OBSERVATIONS

The role of the CISO has matured to become highly prevalent in state government. Eighty-three percent (83%) of the states that responded to this survey have a CISO or the equivalent of that position. Yet, the state CISO role has evolved in recent years from a technical position dealing with perimeter security and related activities to a position of state IT strategy and policy leader. As that transformation has occurred, there has been a growing appreciation for the value of the state CISO's enterprise-wide view and ability to harmonize IT security policies and practices. With the increased importance of technology to almost every vital government operation, the state CISO has assumed responsibility for translating technical security issues for state policy officials as well as the state officials who execute those policies. In this way, the state CISO has become an educator on IT security. State CIOs also have a heightened level of reliance on the state CISO due to the position's expertise in dealing with the ever-mutating IT threat environment.

In the coming years, the role of the state CISO will continue to evolve in response to environmental factors that include the changing nature of threats facing state IT and growing citizen demands for enhanced online state services. Pressures created by a retiring state IT workforce and higher average salaries available in the private sector are likely to motivate states to find innovative and creative ways to compensate and retain state CISOs and supporting IT security staff members. Finally, state CISOs are likely to become more involved in homeland security and critical infrastructure protection initiatives, since much of government and private sector operations rely on properly functioning technology.

Through its Committee work, NASCIO will continue to monitor the evolution of the state CISO and the important part that role plays in ensuring that citizens and state employees have the technology they need while ensuring the security of state IT systems and infrastructure.

APPENDIX 1: ADDITIONAL RESOURCES

NASCIO:
“Born of Necessity: The CISO Evolution — Bringing the Technical and the Policy Together”, NASCIO, July 2006,
http://www.nascio.org/nascioCommittees/securityPrivacy/members/#publications.

"The IT Security Business Case: Sustainable Funding to Manage the Risks," NASCIO, May 2006,
http://www.nascio.org/nascioCommittees/securityPrivacy/members/#publications.

NASCIO Security and Privacy Committee Webpage:
http://www.nascio.org/nascioCommittees/securityPrivacy/members/.

Other Publications and Resources:
"Effective Management of Information Security and Privacy," Alicia Anderson, Educause Quarterly, November 1, 2006,
http://www.educause.edu/ir/library/pdf/EQM0614.pdf.

"The National Strategy to Secure Cyberspace," A White House Report, February 2003,
http://www.whitehouse.gov/pcipb/.

United States Computer Emergency Readiness Team (US CERT):
http://www.us-cert.gov/.

National Institute of Standards and Technology (NIST), Computer Security Division:
http://csrc.nist.gov/.

The Federal Information Security Management Act (FISMA):
http://csrc.nist.gov/policies/FISMA-final.pdf.

Sarbanes Oxley Act:
http://www.sec.gov/spotlight/sarbanes-oxley.htm.

Infragard:
http://www.infragard.net/.

Multi-State ISAC:
www.msisac.org.

IT ISAC:
https://www.it-isac.org/#.

International Systems Security Association (ISSA):
http://www.issa.org/.

Global Security Working Group:
http://it.ojp.gov/topic.jsp?topic_id=58.

Internet Education Foundation:
http://getnetwise.org/.
National Cyber Security Partnership:
http://www.cyberpartnership.org/.

SANS Technology Institute:
http://www.sans.edu/.

CSO Magazine:
http://www.csoonline.com/.