BUYER BE AWARE

Integrating Cybersecurity into the Acquisition Process

CIS Center for Internet Security®

NASPO™
National Association of
State Procurement Officials

NASCIO®
Representing Chief Information
Officers of the States

> *"Cybersecurity is seen as 'the CISO's problem' and is almost never considered an integral element to an IT acquisition, although it should be."*

This quote is from a state chief information security officer (CISO) when asked about how cybersecurity is integrated into the state information technology (IT) acquisition process. The importance of cybersecurity in both the public and private sector cannot be overstated and this is even more true for state government. The past several years has demonstrated that disruptions to state services, the supply chain and public trust have a tremendous impact on state governments. While it is impossible to prevent every incident or disruption, there are steps that can be taken to limit them. A very wise woman once said, "let's start at the very beginning, a very good place to start." In this case, the beginning is with the acquisition process—starting with discovering a need and ending with final implementation—and baking cybersecurity into it from the beginning.

As noted in the 2020 Deloitte-NASCIO Cybersecurity Study, cybersecurity functions in state government are increasingly being outsourced. However, confidence in third-party vendors is decreasing. Eighty-one (81) percent of states say they are only somewhat or not very confident in third parties' cybersecurity practices. Additionally, major cyber incidents in the past year have called into question the security of commonly used software and the COVID-19 pandemic reinforced the importance of supply chain security.

In this publication we will address steps state governments should take to ensure cybersecurity is an integral part of the acquisition process. We will also build upon previous acquisition reformation and transformation work and publications from a partnership between NASCIO and NASPO (the National Association of State Procurement Officials) that started in 2016. In this latest iteration, we are excited to have the Center for Internet Security (CIS) join us and bring their unmatched cybersecurity expertise to the effort.

Cybersecurity is a Team Sport

Managing cybersecurity risk should be approached as a team sport. Each employee and contractor in every aspect of an organization touches IT and thus has an important role in the overall cybersecurity posture of the state. The ubiquity of IT throughout the organization implies that only a true whole-of-organization approach can lead to successful cybersecurity outcomes. It is a team task to develop and integrate, patch and maintain and manage end-of-contract and end-of-life transitions. Users must properly utilize and protect resources, administrators must manage, security teams must define and monitor systems and procurement officials must incorporate security into the acquisition process and resulting contract.

Procurement teams, IT teams and IT security teams all have a role to play in making successful IT deployments possible. While these teams may be in the same organization, they may not always see problems in the same way. Together, by focusing on their respective roles, these teams can complete efficient and effective procurements.

Cyber Must be Considered from the Start

In early 2021, NASCIO sought feedback from state CISOs on their involvement in the acquisition process and the responses overwhelmingly indicated a **lack** of involvement. Many CISOs reported they are most often left out of the process until the end and then pressured to "check a box" and sign off on any cybersecurity contract requirements already established.

One CISO commented, "unfortunately, we are regularly seen as the 'roadblock' to services being obtained." Another CISO stated, "we are consulted at the end, after the agency has already chosen the product, negotiated everything to be negotiated and now we are 'holding up' the process by attempting to ensure that security is included." And another CISO said, "I still find myself having to 'push' for security involvement early and in too many cases, being pressured to sign off late in the game."

There is the need for state CISOs, chief procurement officials (CPOs) and other state agencies to share their collective expertise to adequately address cybersecurity issues. Cybersecurity is not, and cannot simply be, a box to be checked. It is critical that CISOs advise agencies on aspects of cybersecurity that must be considered at the beginning of the acquisition process. All parties must work together to create terms and conditions, service level agreements and other components to aid in preventing and responding to cybersecurity issues that might arise.

An Integrated Process for Acquisition

As technology has grown increasingly complex over the last twenty years so has the acquisition process. State CPOs have had to shift from primarily procuring commodities to complex technologies as well as services. This requires a more strategic and integrated approach to managing the entire process. Procurement officials continue to work with their leadership and partners within state government to streamline the procurement process to meet the needs of their agency customers.

As written in the NASPO Practical Guide, successful large-scale technology acquisitions require the expertise, knowledge and active engagement of cross-functional teams throughout the process. Information sharing and cross-departmental education can be used to foster collaboration while building a common understanding of each team's role in cybersecurity. The early engagement of key stakeholders is essential to the procurement process and a team should be formed for each procurement that includes:

- Representatives from the agency requesting the procurement
- The CIO office
- The CISO office
- Technical subject matter experts
- Risk management officers (including privacy officers)
- Legal counsel
- The procurement officer

Each group involved must understand the goals of the project and the roadmap for achieving them.

Procurement Strategy

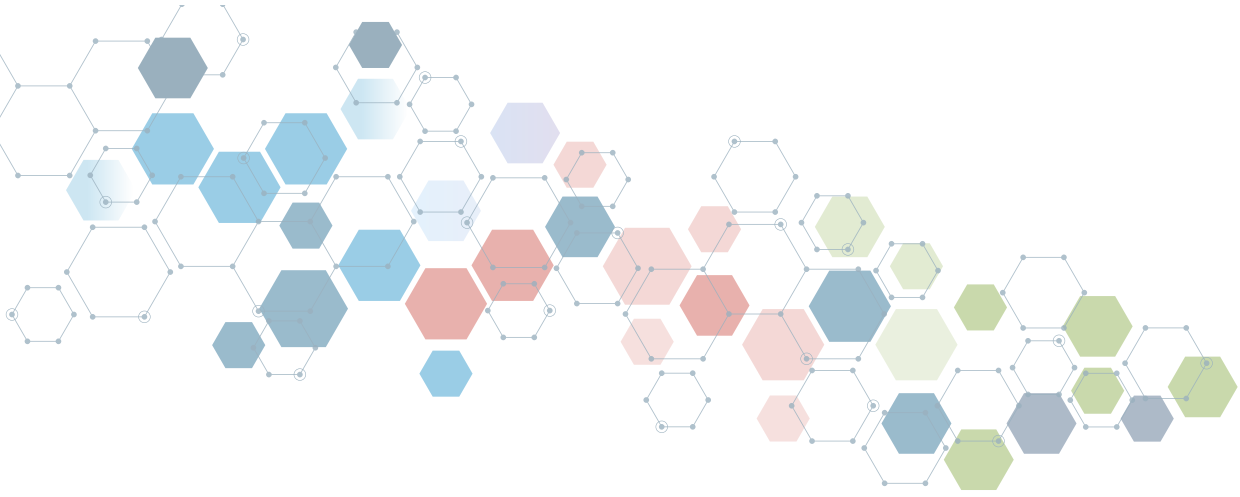
The acquisition process typically begins with the state agency identifying the need or problem to be solved and it is here that the planning and collaboration should begin. Central procurement offices typically provide detailed templates and processes to agencies for identifying a need. This guidance is utilized to develop the business case for the acquisition and to initiate the procurement process. Agencies must examine and outline their need, while guarding against becoming too focused on one solution or vendor. This is also an opportunity for the agency to begin identifying the risks, including cybersecurity, related to the service or product they are seeking.

As the business case is developed and the procurement office is engaged, an integrated procurement strategy should be developed. During this time, stakeholders from different departments should be engaged in the planning. The procurement officer should guide the determination of the procurement strategy and the solicitation method to be used. As the procurement strategy is identified there are several elements that should be addressed:

- Key elements of the procurement methodology selected
- Constraints or risks impacting the procurement
- User agency goals and requirements, such as replacing an old system or purchasing a new one
- Procurement team roles and responsibilities
- Executive and stakeholder oversight

In the case of large-scale IT procurements or procurements that carry a large amount of risk, it is often more beneficial to approach it as a project, rather than a traditional procurement. A formal project process should be implemented to manage the complexity involved and set expectations for all participants. This includes developing a project charter, which serves as an agreement for all parties involved. It authorizes both the project and clearly identifies the different roles. The state CIO, CISO and other technology staff involved should be included as parties to the project charter.

The project team will then develop project plans for the different facets of the projects. These include the activities, processes and procedures that will be used to manage the IT project. They should also identify elements such as constraints, assumptions, organizational structure, IT infrastructure, cost, staffing and communication. Many states have implemented project plans and processes for larger project acquisition and implementation.



Market Research

It is essential to conduct thorough market research as part of the planning process and the development of the solicitation. The project plan should identify who is responsible for conducting this analysis. The project team member serving as the technical subject matter expert (SME) may be best suited to analyze the market, however, the procurement officer should also conduct their own research. Information sharing among the procurement team is crucial. Market research can provide insight into business models/delivery methods, cost structure, potential vendors and key requirements for the solicitation. The CISO and CIO should be actively engaged to provide their industry expertise. This is also the opportunity to begin to identify potential risks and industry practices related to cybersecurity.

As mentioned earlier, engaging the vendor community can also provide powerful insight and feedback. Issuing a request for information (RFI) is one approach to obtaining this input. A carefully structured RFI early in the planning process can provide information that can be incorporated into the project plan and the solicitation itself. Engagement with vendors can also occur through "industry days," state procurement conferences and other appropriate venues.

Managing Risk

The procurement team should utilize the information gathered to conduct a complete risk assessment and mitigation framework. This assessment should take a team approach and include all relevant types of risk: IT security, privacy, financial, legal, procurement, technology and others. The team, particularly the CISO and legal counsel, must thoroughly analyze the potential security threats and the impact. The team must strategize about how to identify, weigh and reduce the risk related to the procurement. This should result in the determination of the tolerance for risk and how it might be mitigated. This will then inform the development of the requirements of the solicitation, the determination of terms and conditions, and eventually post-award contract monitoring.

In addition to the state's minimum-security requirements, the solicitation lists other requirements as dictated by the risk assessment and mitigation framework. In addition to asking vendors to address these risks, they should identify what they perceive as the significant risks posed by the contract. Vendors should be required to provide a plan to reduce or manage the identified risks. This should be factored into the evaluation criteria included in the solicitation. The CISO typically oversees compliance with these requirements and can help with their incorporation into the solicitation. Additional security requirements may be determined necessary through the risk analysis and the mitigation framework.

Determining the appropriate set of security requirements is one of the most difficult tasks that an organization faces in cybersecurity risk management—and mistakes can have severe consequences. Eighty (80) percent of states have implemented some subset of the controls set forth by the National Institute of Standards and Technology (NIST) in its Special Publication (SP) 800-53. The NIST guidance includes a catalog of security and privacy controls to protect against a variety of threats.

For example, the State of North Carolina has implemented the NIST Standards as part of their security requirements and includes them in a Vendor Readiness Assessment for State Hosted Solutions. This document establishes a limited set of baseline controls determined through an analysis within the State of North Carolina. To properly implement NIST SP 800-53, an organization has to conduct a risk assessment and determine which of the various control families and enhancements are applicable to its systems. This is a valuable exercise but is often beyond the level of expertise of even sophisticated organizations.

Another option is the CIS Controls® coupled with the CIS Benchmarks. The Implementation Groups in the Controls were developed through a baseline risk assessment conducted across a wide variety of industries for a wide range of organizational types and sizes. Based on the size and sophistication of an organization, it can select one of three Implementation Groups, tailor if necessary, and implement them. To aid implementation, organizations can use the CIS Benchmarks to properly configure a variety of well-known operating systems, cloud providers and other products. State, local, tribal and territorial governments can get these and other security tools for free from CIS.

As security requirements are included in the solicitation and vendors craft their proposals to demonstrate that they comply, state agencies must verify that prospective contractors meet the requirements. The state CISO should oversee the validation process and work with the procurement team to ensure that the vendors meet the requirements. States have, in some cases, required third party verification that includes a detailed risk assessment of the vendor's cybersecurity practices.

Often one of the biggest mistakes in drafting solicitations is being overly prescriptive in defining the specifications for a solution and how to deliver the solution. Requests for Proposals (RFP should encourage solutions from the private sector to solve the problem identified within the statement of work. Opening the ability for the vendor to innovatively address the issue, while meeting the requirements, can create a more comprehensive solution. Moreover, states are encouraged to embrace agile development methodologies, employing rapid iterations with users to refine requirements and accelerate the delivery of early capabilities. The procurement officer can foster this approach and mentality within the procurement team throughout the process. The representatives from the different departments involved in the development of the procurement should comprise the evaluation committee to ensure a successful award.

StateRAMP

An independent, nonprofit organization, StateRAMP, has recently been established with the goal of "verifying the cybersecurity of cloud service providers for state and local governments." StateRAMP's security verification model is based on the National Institute of Standards and Technology (NIST) publication 800-53 Rev. 4—the same publication the Federal Government used to develop FedRAMP, a similar cybersecurity program for federal entities.

Architecting for Success: Mitigating Risk through Good Architecture

The NASCIO publication, Leveraging Enterprise Architecture for Improved IT Procurement, states that "state leaders should consider the benefits of aligning IT procurement and enterprise architecture not only as a way to deliver IT services more effectively, but also as a way to finding savings through streamlined investments." It is also true that aligning IT procurement and enterprise architecture can mitigate a state's cybersecurity risk.

Enterprise architecture (EA) serves the purpose of formally describing the envisioned structure, relationships and characteristics of a system. EA serves as the 'blueprint' for the organization and its supporting systems. Defining the architecture for the desired end state of an IT system helps ensure that those defining the IT system requirements and those who will build the system have a common understanding of what is expected. Architectural descriptions are essential for IT systems due to the enormous complexity of modern IT solutions. The absence of solid EA to guide an IT procurement or development effort greatly increases the risk of program failure.

EA provides an enterprise-wide perspective for an organization defining the components and the relationships among the processes, information and systems to meet the mission of an organization. EA reflects the logical relationships and information flows among the system components within the enterprise. Thus, EA is very useful, for example, in enabling the evaluation of potential business process improvements as well as the examination of alternative technical solution options, such as use of commercial components rather than developing new components. Armed with an EA, state and local government organizations can then reduce cybersecurity risk with rigorous planning, careful implementation and thorough testing.

Securing the Supply Chain

A supply chain is a network of organizations, individuals, resources and information that, together, create and move a product or service to its final customer or end-user. Supply chains are a fact of modern life. No organization develops everything itself, and nearly all IT used in government is sourced externally. Even IT products purportedly developed in-house likely leverage software development toolkits, workstations, removable media and other technology that are subject to supply chain risks.

Managing supply chain risk is notoriously difficult. Organizations involved in large complex supply chains—from major retailers to the defense industry—struggle with appropriately making investments and accepting the risks that remain after these investments—known as residual risks. Smaller organizations often lack the resources to make appropriate investments and the leverage to influence their suppliers.

Not all IT components are critical or carry the same risks, requiring a careful risk assessment of each component and a logical approach to mitigating it. Broadly speaking, organizations can significantly lower their supply chain risk by taking three steps to manage cybersecurity risk:

1. A **cybersecurity risk management program** to address broad cybersecurity risks, regardless of whether they are supply chain risks.
2. A targeted **supply chain risk mitigation program** for identifying and mitigating the most consequential supply chain risks.
3. A **supplier risk management program** to reduce the risk from emerging threats and more elusive attacks.

For the first step, organizations can build cybersecurity risk management programs through existing frameworks and controls developed through the experiences of many organizations and the input of many experts. As discussed earlier, one good example is the CIS Controls®.

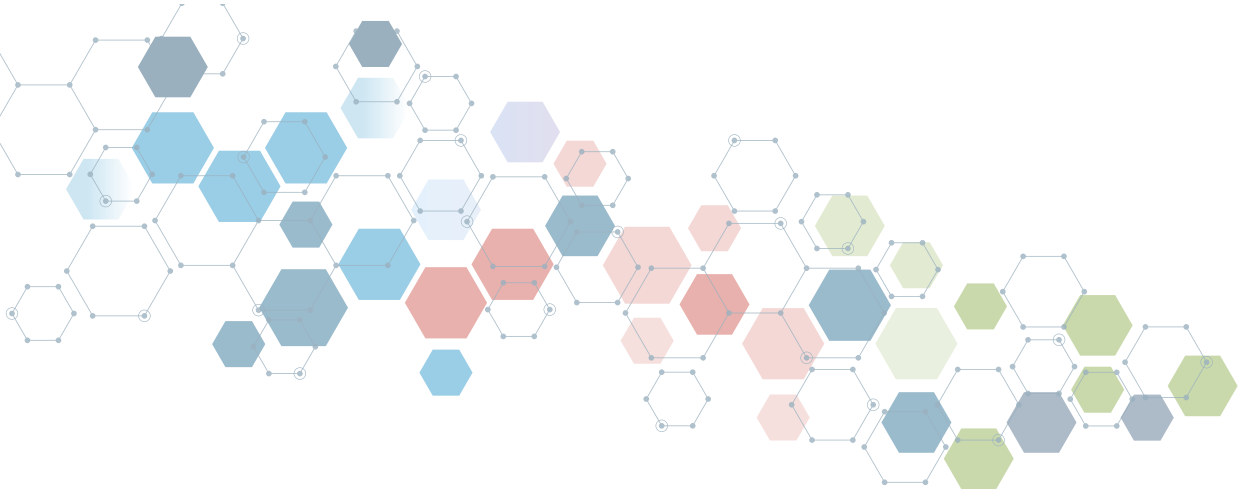
The second step involves a deep understanding of cyber threat actors and how they may attack your supply chain. This process of threat modeling is complex and requires specialized cybersecurity training. Its contribution to reducing supply chain risk can be significant but most organizations will require experienced threat modelers either from a cybersecurity team or, in most state and local governments, through contracts.

The final step requires a careful understanding of your suppliers and how they manage their risk and the risk of their own suppliers. The upshot is to identify from whom you get things, ensure that you have the right type of relationship with them and properly manage that relationship. Managing relationships with suppliers can be costly and time intensive. There are several triggers for how concerned you need to be about your supply chain partners. Four important triggers are size, diversity, criticality and customization.

The SolarWinds Incident—a Game Changer

In December 2020, the world learned of an unprecedented supply chain attack on a company called SolarWinds. The consequences of this serious compromise are not yet fully known, and likely won't be for some time. The introduction of malicious code into the SolarWinds product was a particularly effective approach, as most network management systems are viewed as trusted and given significant access privileges to network and system components in an enterprise.

This highly successful attack begs a question for all organizations deploying in complex IT environments: if a large, well-resourced supplier like SolarWinds cannot prevent such an incident, how can I possibly keep these sorts of things from impacting my environment?



The answer, however unfortunate, is that there is very little most purchasers of the SolarWinds Orion product could have done to prevent the initial introduction of this vulnerability: they downloaded updates from a trusted site, installed, signed and verified updates with valid hashes and used the products as intended. SolarWinds has some 300,000 customers across a wide range of industries and agencies at all levels of government. Because of its size, few state or local governments would have any ability to influence SolarWinds's risk management practices. However, the criticality of the SolarWinds Orion product could have a dramatic impact on an organization's operation.

Disheartening as this may seem, there is hope. It is certainly not reasonable to expect to catch or dissuade every possible attack—and you don't have to. Organizations can implement security principles that lower risk even—especially—when facing the reality that some initial attack vectors will be successful. Examples of these include:

- Separation of duties
- Strong network segmentation
- Standard security configurations
- Zero trust architectures
- Regularly updating assessments of suppliers
- Identifying changes in supplier practices that might alter an organization's security posture toward
- Notification of operational changes that impact security, such as if operations begin in certain countries.

The baseline cyber hygiene activities discussed above can lower the consequence of an attack like the one against SolarWinds. This is where defense-in-depth comes in by layering different risk mitigation approaches to stop attacks that might overcome any single hurdle. This increases the chance that, at some point, a threat actor will be tripped up and thwarted, or at least isolated to limit damage.

A good defense-in-depth strategy will thoughtfully implement controls of different natures to mitigate risk more thoroughly. This is, in essence, the idea behind control "families" seen in most major control guidance, like NIST Special Publication 800-53 and the CIS Controls. It also underscores the importance of implementing basic cyber hygiene to stop the most likely sets of attacks, and then build upon that foundation.

The Private Sector's Role

In 2018, NASCIO convened the NASCIO Roundtable on IT Procurement Innovation and partnered with NASPO, the National Association of State Chief Administrators (NASCA) the Computing Technology Industry Association (CompTIA) SLED Council and the IT Alliance for Public Sector (ITAPS). The Roundtable included state chief information officers, state procurement officials, state chief administrators and representatives from private sector companies. The resulting publication, A View From the Marketplace, included several recommendations that highlight the importance of the private sector in the acquisition process. Some of the

Supply Chain EO

On February 24, 2021, President Biden signed an Executive Order, "Securing America's Critical Supply Chains." The Executive Order includes a mandated review of the information and communications technology sector in the wake of the SolarWinds breach. Additionally, the order directs the numerous Federal agency secretaries to provide an assessment of cyber risks within key industry sectors that could disrupt the U.S. supply chain.

recommendations can be used or modified to demonstrate the important cybersecurity role the private sector has in the acquisition process.

One of the most applicable recommendations is:

> *Look for partners and not just vendors or suppliers. If you are in the private sector, be a partner instead of simply a vendor or supplier.*

States can be good and trusted partners by having clear cybersecurity governance and policies that third parties and vendors must adhere to and transparent ways to measure compliance. States can also be good partners by planning and budgeting for cybersecurity requirements from the beginning of the process.

Vendors can be good and trusted partners by demonstrating that a culture of information security exists in their companies; understanding and respecting state cybersecurity risks; sharing internal cybersecurity assessments with the state; and agreeing to state standards and practices to measure security compliance.

Recommendations for Improved Cybersecurity and Acquisition Integration

Cybersecurity must be viewed as an integral part of the acquisition process by CIO, CPO, agency staff and the private sector. Neither the acquisition process nor cybersecurity are trivial components of state government which makes it all the more important that the two are integrated. Anything less than full integration and acceptance of the importance of the two quite simply puts states at a much higher risk. Below is a list of recommendations aimed at assisting state governments in this task.

- Educate the budget office on the importance of cybersecurity and the potential risks for the state. Cyber is a lifecycle and not project with a start and end.
- Ensure that cybersecurity is planned into and budgeted for at the beginning of the acquisition process.
- Cross-educate all stakeholders to ensure an understanding of cybersecurity concepts, priorities, objectives, defined roles and terminology.
- Ensure alignment between the acquisition process and the state's cybersecurity standards and architectures.
- Vendors and contractors must be required to provide an attestation that their security practices are in line with the state's cybersecurity practices as a requirement to bid on a state contract. Vendor attestations should be verified and the state CISO should oversee this process.

- States should establish a rigorous third-party (vendor) assessment and accountability system via terms and conditions, the project management process and implementation.
- States should establish a process to regularly monitor security practices of all third parties involved in current state contracts via SOC2 (system and organization controls) reports, periodic assessments, service level agreements, etc.
- States must pay close attention to supply chain risk management. In addition to implementing a broad supplier risk management program to reduce the risk from emerging threats and more elusive attacks, for each procurement, states should conduct a targeted supply chain risk assessment for identifying and mitigating supply chain risks. The National Counterintelligence and Security Center (NCSC) has produced an excellent primer on the importance of supply chain risk management HERE.
- Thorough market research should be conducted to identify risks, industry trends and solicitation best practices.
- States should utilize a risk-based approach to negotiating terms and conditions to allow for flexibility where possible.
- States should educate state procurement offices and user agencies on the state's risk assessment/risk mitigation framework that includes an inventory of threats and risks to the state and how they are applicable to the acquisition process.
- States should follow federal government (GSA, FCC, etc.) directives and guidelines on banned products and software.

Resources

CIS Controls. Available at https://www.cisecurity.org/controls/.

CISA Information and Communications Technology Supply Chain Risk Management. Available at https://www.cisa.gov/supply-chain.

NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations. Available at https://csrc.nist.gov/publications/detail/sp/800-161/final.

Leveraging Enterprise Architecture for Improved IT Procurement https://www.nascio.org/resource-center/resources/leveraging-enterprise-architecture-for-improved-it-procurement/

A View from the Marketplace: What They Say About State IT Procurement https://www.nascio.org/resource-center/resources/a-view-from-the-marketplace-what-they-say-about-state-it-procurement/

State IT Procurement Negotiations: Working Together to Reform and Transform https://www.nascio.org/resource-center/resources/state-it-procurement-negotiations-working-together-to-reform-and-transform/

Cyber Liability Insurance 101 https://www.naspo.org/cybersecurity-is-a-complex-issue-and-naspo-is-not-alone-in-recognizing-its-importance/

State of California templates and planning documents for each phase of an IT project: https://capmf.cdt.ca.gov/Templates.html

Primary Authors

Mike Garcia
Senior Advisor for Cybersecurity
Center for Internet Security
Mike.Garcia@cisecurity.org

Matt Oyer
Acting Chief Learning Officer
National Association of State Procurement Officials
moyer@naspo.org

Meredith Ward
Director, Policy & Research
National Association of State Chief Information Officers
mward@nascio.org

About CIS

The Center for Internet Security, Inc. (CIS®) is a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

About NASPO

The National Association of State Procurement Officials (NASPO) is a non-profit association dedicated to advancing public procurement through leadership, excellence, and integrity. It is made up of the directors of the central purchasing offices in each of the 50 states, the District of Columbia, and the territories of the United States. NASPO is an organization that helps its members as public procurement leaders through promotion of best practices, education, professional development, research, and innovative procurement strategies.

About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit www.NASCIO.org.