

Welcome

State and Local Government Cybersecurity Framework Kickoff

MARCH 27, 2014



Michael Daniel

Special Assistant to the President
Cybersecurity Coordinator
The White House



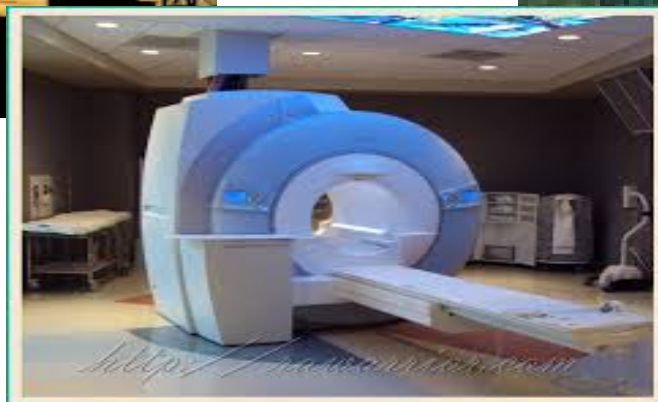
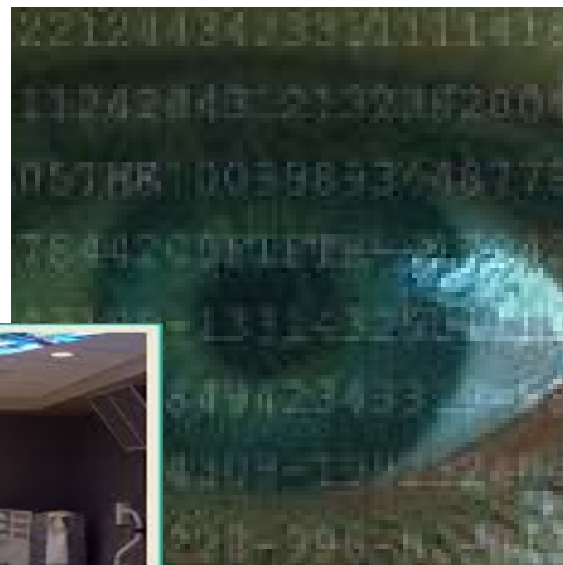
Overview of NIST Cybersecurity Activities

Kevin Stine

National Institute of Standards and Technology

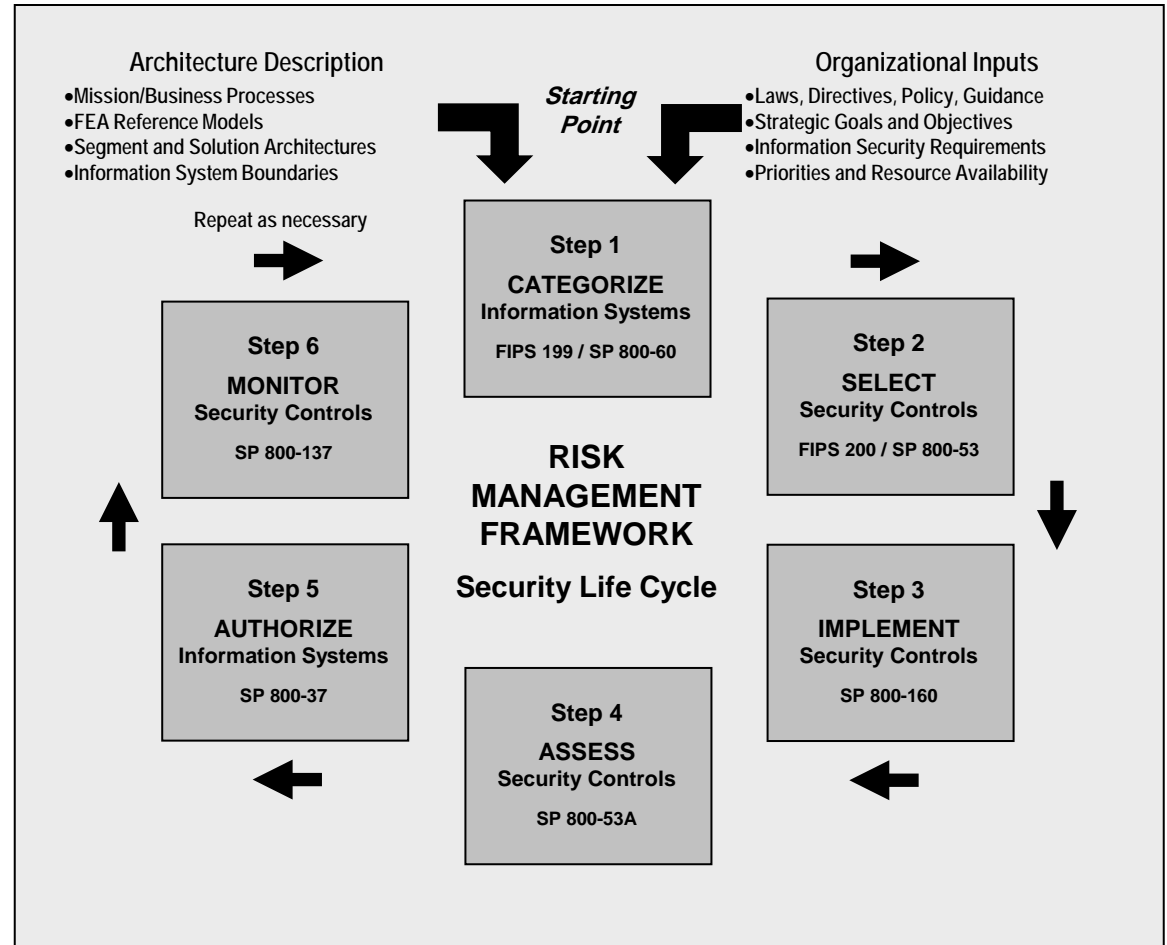
Computer Security Division

Within NIST's Information Technology Laboratory, the Computer Security Division provides standards and guidelines, tools, metrics, and practices to protect information and information systems.



NIST Risk Management Framework

- A process, based on an integrated suite of standards and guidelines, to help Federal agencies manage cybersecurity risk.
- Frequently voluntarily adopted by non-Federal organizations
- Complementary to the *Framework for Improving Critical Infrastructure Cybersecurity*



Executive Order: Improving Critical Infrastructure Cybersecurity

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

President Barack Obama

Executive Order 13636, Feb. 12, 2013

- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a [voluntary framework for reducing cyber risks to critical infrastructure](#)
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a [roadmap for future work](#)

As Directed in the EO, the Cybersecurity Framework ...

- Includes a set of existing standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks
- Provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Identifies areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations

Framework Components

Framework Core

- Cybersecurity activities and informative references common across critical infrastructure sectors and organized around particular outcomes

Framework Profile

- Aligns industry standards and best practices to the framework Core in a particular implementation scenario

Framework Implementation Tiers

- Describes how cybersecurity risk is managed by an organization

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Key Points about the Framework

- It's a **framework**, not a prescription.
- The framework is a **flexible**, highly **adaptable** tool.
- It's a demonstration of a strong **private-public partnership**
- The framework is a **living document**.



What's Next: Using the Cybersecurity Framework

- Organizations should **use the framework** and provide feedback to NIST
- Industry groups, associations, and non-profits can play key roles in assisting their members to understand and use the framework by:
 - Building or **mapping sector specific standards, guidelines, and best practices** to the framework
 - Developing and **sharing examples** of how organizations are using the framework
- NIST is committed to helping organizations understand and use the framework
 - NIST is **expanding its outreach** and will work with the Department of Homeland Security on its “C³” Voluntary Program ([http://www.dhs.gov/about-critical-infrastructure-cyber-community-c³-voluntary-program](http://www.dhs.gov/about-critical-infrastructure-cyber-community-c3-voluntary-program))

What's Next: Roadmap Areas for Development, Alignment, and Collaboration

- The Executive Order calls for the framework to “identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations”
- High-priority **areas for development, alignment, and collaboration** were identified based on stakeholder input:

Authentication

Automated Indicator Sharing

Conformity Assessment

Cybersecurity Workforce

Data Analytics

Technical Privacy Standards

International Alignment

Supply Chain Risk Management

Federal Agency Cybersecurity Alignment

<http://nist.gov/cyberframework/upload/roadmap-021214.pdf>

Where to Learn More and Engage...

- *Framework for Improving Critical Infrastructure Cybersecurity*, available at www.nist.gov/cyberframework
 - Share your framework experiences at cyberframework@nist.gov
- Participate in our cybersecurity workshops and comment on our standards and guidelines
- Participate through the National Cybersecurity Center of Excellence (NCCoE) at <http://csrc.nist.gov/nccoe/>
- Follow our cybersecurity activities at <http://csrc.nist.gov>

Questions?

Please identify yourself and your organization as you ask your question.

National Cybersecurity Center of Excellence

Nate Lesser, Deputy Director

State and Local Government Cybersecurity Framework Kickoff
March 27, 2014



VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs



GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

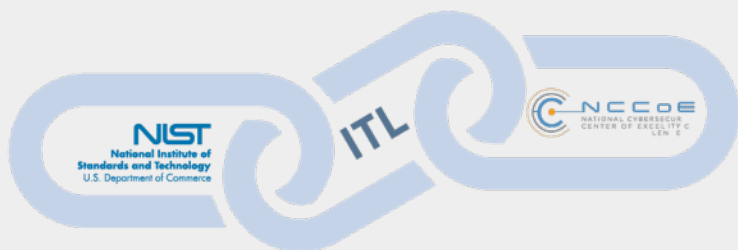
INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

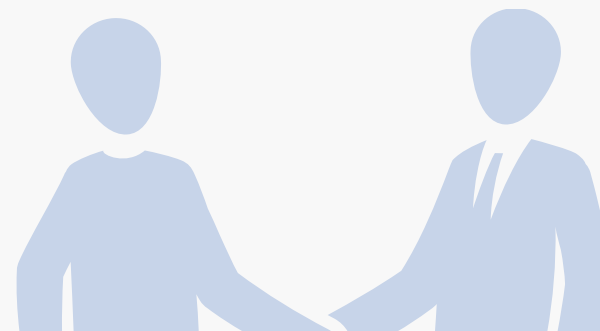


NIST ITL





The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.





PARTNERSHIPS





Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.



NIST CYBERSECURITY THOUGHT LEADERSHIP

-  Cryptography
-  Identity management
-  Key management
-  Risk management

-  Secure virtualization
-  Software assurance
-  Security automation
-  Security for cloud and mobility

-  Hardware roots of trust
-  Vulnerability management
-  Secure networking
-  Usability and security



Standards-Based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards



Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications



Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions



Commercially Available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry



Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations



Open & Transparent

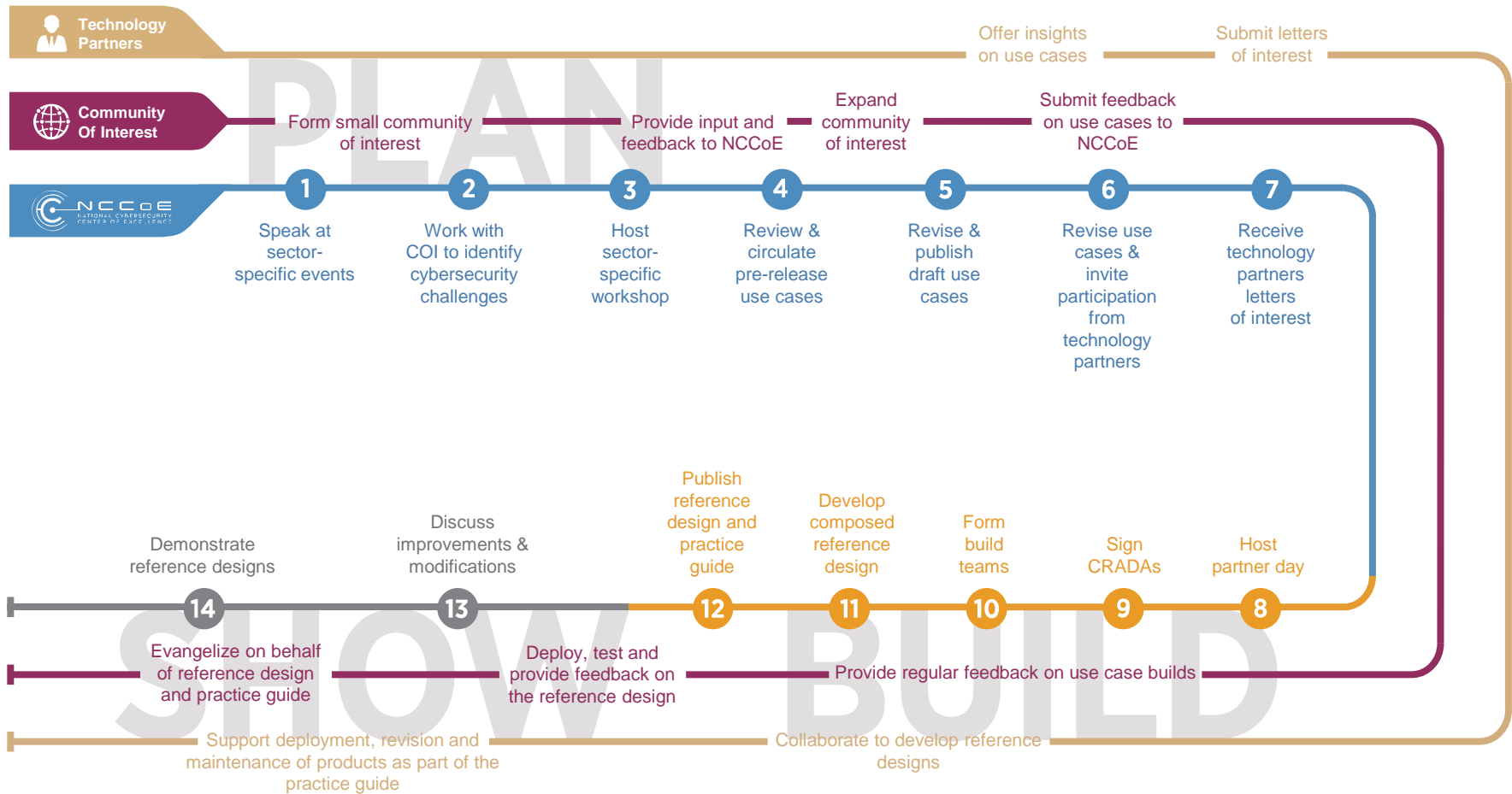
Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

The NCCoE seeks problems that are

- ▶ Broadly applicable across much of a sector, or across sectors
- ▶ Addressable through one or more reference designs built in our labs
- ▶ Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

Two kinds of reference designs

- ▶ Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- ▶ Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)





Focus on technology-driven security challenges

Building blocks address a technology-adoption gap common across multiple sectors by creating reference designs that follow the center's primary tenets (standards-based, modular, repeatable, commercially available, usable, and open and transparent).




Identify building block

Security challenges come from technology companies, systems integrators, industry, academia, NCCoE staff members, other parts of NIST and other government agencies, and the public.




Seek public comment

Building block descriptions include a problem statement and goal, security characteristics, approach, architecture, technology component list, and relevant standards and best practices. The NCCoE seeks public comment on the applicability of the challenge and the validity of the proposed approach, then publishes a revised building block description with the public comments and their disposition.

 **Establish a build team(s)**
The NCCoE works with the technology community to identify security components that address a particular challenge. NCEP companies and other product vendors join build teams and work with the NCCoE to create reference designs. Depending on interest and the diversity of relevant technologies, we may build multiple reference designs for a single building block.

 **Create the reference design**
Working with the identified technology components, the build team develops a reference design that addresses the building block challenge.

 **Document the reference design**
The reference design is captured in a NIST practice guide along with relevant instructions, tutorials, techniques, test sets and outputs, and standards and best practices.



- ▶ Share ideas for use cases, building blocks or workshops.
- ▶ Comment on technical architectures, or suggest applicable components.
- ▶ Provide feedback on our reference designs.

Visit <http://nccoe.nist.gov>

Email nccoe@nist.gov

Call 240-314-6800

Questions?

Please identify yourself and your organization
as you ask your question.

THE CALL, THE COUNCIL, AND THE FRAMEWORK

The Emerging Policy and Mission Space
of the Nation's Cybersecurity

Thomas MacLellan

Director

Homeland Security and Public Safety Division

NGA Center for Best Practices

March 27, 2014

The logo for the National Governors' Association features a stylized, multi-pointed star or compass rose in shades of gold and blue. A thin, golden line extends from the top point of the star across the page, passing behind the date.

NATIONAL
GOVERNORS
ASSOCIATION

National Governors Association (NGA)

Bipartisan, collective voice of the Nation's governors

- ❖ **Office of Federal Relations:** Represents states on Capitol Hill and before the Administration on key federal issues
- ❖ **Center for Best Practices:** Develops and assists states in implementing innovative solutions to public policy challenges

Resource Center for State Cybersecurity

The mission of the NGA Resource Center for State Cybersecurity is to help governors improve their state's cybersecurity posture and response capabilities by providing strategic and actionable policy recommendations that governors can adopt to craft and implement effective state cybersecurity policies and practices.

Co-chairs:

Maryland Governor Martin O'Malley

Michigan Governor Rick Snyder

Guiding Principles

- Support Governors.
- Be Actionable.
- Reduce Complexity.
- Protect Privacy.
- Employ Technologically Neutral Solutions.
- Focus on the State as Enterprise
- Promote Flexible Federalism.
- Rely on Evidence-Based Practices.
- Use and Generate Metrics.
- Promote the Use of Incentives.

The Call

Act and Adjust: A Call to Action for Governors for Cybersecurity:

Provides governors with strategic recommendations they can immediately adopt to improve their state's cybersecurity posture.

Recommendations:

- ❖ Establish a governance and authority structure for cybersecurity.
- ❖ Conduct risk assessments and allocate resources accordingly.
- ❖ Implement continuous vulnerability threat monitoring practices.
- ❖ Ensure compliance with current security methodologies and business disciplines.
- ❖ Create a culture of risk awareness.

The Council

Formally established by Presidential Executive Order, the Council of Governors (Council) serves as a mechanism for governors and key federal officials to address matters pertaining to the National Guard, homeland defense, and defense support to civil authorities. Consists of 10 governors appointed by the President (five from each party)

Cyber Mission: Framework for State-Federal Unity of Effort on Cybersecurity.

Establishes basic principles and a list of key areas for collective effort, such as establishing roles and responsibilities, improving information sharing and enhancing operational coordination.

- Not intended to be an exhaustive list of specific requirements, but rather a tool to facilitate and measure progress.

The Framework

The Call directly supports the NIST Framework for Improving Critical Infrastructure Cybersecurity in two ways:

- ❖ Implement continuous vulnerability threat monitoring practices.
- ❖ Ensure compliance with current security methodologies and business disciplines.

Moving Forward:

Other Areas, Other Thoughts

- Improving state and federal coordination
- Enhancing the role of fusion centers in supporting a cybersecurity mission
- Ensuring a skilled cybersecurity workforce
- Securing critical energy systems and infrastructure
- Determining effective cybersecurity governance structures
- Modeling state cybersecurity legislation
- Developing effective public-private partnerships
- Identifying state cybersecurity requirements

Thomas MacLellan
NGA Center for Best Practices
Homeland Security and Public Safety Division
tmaclellan@nga.org
202-624-5427

Questions?

Please identify yourself and your organization as you ask your question.



States at Risk: Cybersecurity in the States

State and Local Government Cybersecurity Framework Kickoff
National Cybersecurity Center of Excellence
March 27, 2014

Doug Robinson, Executive Director
National Association of State Chief Information Officers

Today's State IT Landscape



- ✓ **Cybersecurity threats!** New technologies, new risks, governance is hard, collaboration needed
- ✓ **Fiscal recovery:** CIOs still seeking IT operational **cost savings**, alternative IT sourcing strategies and **collaboration**
- ✓ **State CIO Balancing Act:** supporting legacy, business process transformation, innovation
- ✓ **State-Federal** symbiotic relationship: program execution
- ✓ **State CIO transitions**, continuing IT **workforce** retirements, skills gap, recruiting challenges

State CIO Priorities for 2014



1. Security



**2. Consolidation/
Optimization**



3. Cloud Services



**4. Project & Portfolio
Management**



5. Strategic IT Planning



**6. Budget and Cost
Control**



**7. Mobile Services/
Mobility**



8. Shared Services



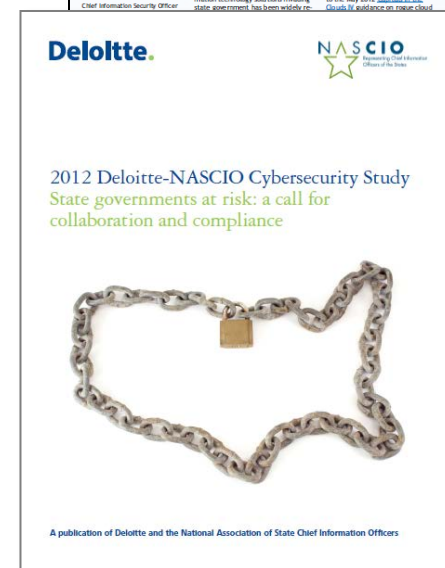
**9. Nationwide Public
Safety Broadband
Network**



10. Health Care

State Governments at Risk!

- States are attractive targets – data!
- More aggressive threats – organized crime, unorganized crime, hacktivism
- Critical infrastructure protection
- Emerging technology and services
- Data on the move
- Lack of broad executive support
- Enterprise authority unclear
- Need more training, awareness



CIOs seeking enterprise approaches
and solutions - governance

**Cybersecurity requires governance
and investment**

Outsourcing and the use of shared
services models increasing

Consolidation and cloud services
growing

Dissatisfied with IT procurement



Cybersecurity



Please characterize the current status of the cybersecurity program and environment in state government.

	Percent
Adopted a cybersecurity framework based on national standards and guidelines	78%
Acquired and implemented continuous vulnerability monitoring capabilities	78%
Developed security awareness training for workers and contractors	78%
Established trusted partnerships for information sharing and response	75%
Created a culture of information security in your state government	73%
Adopted a cybersecurity strategic plan	61%
Documented the effectiveness of your cybersecurity program with metrics and testing	47%
Developed a cybersecurity disruption response plan	45%
Other	6%

States are adopting a cybersecurity framework and implementing monitoring capabilities.

Cybersecurity



What major barriers does your state face in addressing cybersecurity?

	Percent
Increasing sophistication of threats	83%
Lack of adequate funding	77%
Inadequate availability of security professionals	55%
Emerging technologies	42%
Lack of visibility and influence within the enterprise	25%
Lack of support from business stakeholders	21%
Inadequate competence of security professionals	19%
Lack of clarity on mandate, roles and responsibilities	13%
Lack of legislative support	12%
Other	10%
Lack of executive support	6%



Desperately Seeking Security Frameworks – A Roadmap for State CIOs

Introduction: The Complex IT Security Environment in State Government

The IT security programs in state governments have evolved and are administered within a context of dynamically shifting configurations of hardware, software, and network capacities, which increasingly are interwoven into a fabric that delivers government programs to citizens — what NASCIO has called the digital infrastructure. These programs have in common the

In the current environment, in which state IT resources are severely constrained due to budgetary shortfalls, state governments are being impacted by the infusion of massive federal stimulus funds from the American Recovery and Reinvestment Act of 2009. Formula and grant funds are flowing into states already, putting significant new pressure on state IT staffs to quickly and transparently deliver on business demands and the requirements of expanded or entirely new programs. The speed of these allocations and the

MARCH 2009

“...the need for security professionals to continue monitoring and cross-walking a wide variety of security policy, standards, implementation guidelines and controls.”

“This creates a playing field within enterprise IT security in state governments that is uneven, sometimes confusing, and consistently challenging for security leadership.”



NASCIO's 2011 Cybersecurity Call to Action

Key Questions

- Does your state government support a “culture of information security” with a governance structure of state leadership and all key stakeholders?
- **Has your state implemented an enterprise cybersecurity framework that includes policies, control objectives, practices, standards, and compliance?**
- Has your state invested in information technologies that provide continuous vulnerability management and protect against critical cyber threats on an ongoing basis?
- Are security metrics available in your state that accurately measure and report intrusion attempts, penetrations, vulnerabilities and security breaches?
- Have state employees and contractors been trained for their roles and responsibilities in protecting the state's cyber assets?

Promoting Cybersecurity in the States

Awareness and Education

Best Practices and Tools

Enterprise Approaches and Governance

NASCIO Resources: www.nascio.org/advocacy/cybersecurity



States at Risk: NASCIO on Cybersecurity

NASCIO will work with Federal Partners to:

Promote enterprise state adoption of the NIST Framework and monitor

Incentivize and support maturing public sector cybersecurity governance

Create a State overlay to complement the NIST Framework

Build Public Sector IT Workforce Programs

States at Risk: Cybersecurity in the States



Follow us...



drobinson@nascio.org

Questions?

Please identify yourself and your organization as you ask your question.



Follow us...



drobinson@nascio.org

Break

We'll resume in 15 minutes

C³ VOLUNTARY PROGRAM



PROGRAM OVERVIEW and SLTT Resources

Welcome to the community.

OUR ROLE

Ranging from emergency services and transportation systems to SLTT governments, the U.S. critical infrastructure provides the essential services that underpin American society.

Critical Infrastructure

EO 13636 highlights the need for improved cybersecurity among critical infrastructure. PPD-21 calls for efforts to strengthen the physical and cyber security and resilience of our Nation's critical infrastructure.



- Framework implementation guidance
- Focal point for resources and tools
- Relationship management
- Feedback collection

Administration Policies



Cybersecurity Framework

One of the major components of the EO is the development of the Framework by NIST to help SLTT governments reduce and manage their cyber risk as part of their approach to enterprise risk management.



Critical Infrastructure Cyber Community Voluntary Program

- The C³ Voluntary Program website offers an overview of the program, downloadable tools, and outreach materials

Visit us at www.dhs.gov/ccubedvp

- Links to the US-CERT C³ Voluntary Program gateway
 - Existing programs/resources have been aligned with the Framework Core Function Areas (Identify, Protect, Detect, Respond, Recover)
 - Broken out by stakeholder type
 - Demonstrates offerings to support the Framework's principles



Cyber Resilience Review

- DHS will support use of the Cybersecurity Framework primarily through the Cyber Resiliency Review (CRR).
 - No-cost, voluntary, non-technical assessment to evaluate an organization's information technology resilience.
 - The CRR may be conducted as a self-assessment or in-person.
 - To date, DHS has conducted more than 330 CRRs at the request of critical infrastructure entities nationwide.
 - The inherent principles and recommended practices within the CRR align closely with the central tenets of the Cybersecurity Framework.
- Analyzes current practices and how they compare to the principles of the Cybersecurity Framework.



State, Local, Tribal, and Territorial Cybersecurity Engagement Program

- The mission of the SLTT Cybersecurity Engagement Program is to build partnerships with non-Federal public stakeholders including governors, mayors, State HSAs, CIOs and CISOs to advance the Department's mission in protecting critical network systems. The Program also grant funds the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- MS-ISAC
 - Designated by DHS as a key resource for cyber threat prevention, protection, response, and recovery for the nation's SLTT governments
 - DHS is funding deployment and implementation for Managed Security Services via the MS-ISAC to States and Territories that adopt the NIST Cybersecurity Framework.
 - Adoption is measured by State and Territory participation in programs and initiatives outlined by the Framework's five key areas

For More Information Contact Us at SLTTCyber@hq.dhs.gov



2013 Nationwide Cyber Security Review

- Survey to determine SLTT governments' cyber security risk awareness
 - Completed via a partnership between DHS, CIS MS-ISAC, and NASCIO
 - A total of 304 government entities responded (87% increase from 2011)
 - All 50 States
 - 93 Local Governments
 - 151 State Agencies
 - 8 Academia
 - 2 Tribal Governments



Questions?

Please identify yourself and your organization as you ask your question.



Moderator: Elliot Schlanger, CISO, State of Maryland

Panelists

- Chris Boyer, Assistant Vice President for Public Policy, AT&T
 - Danielle Kriz, Director, Global Cybersecurity Policy, Information Technology Industry Council
 - John S. Miller, Director of Cybersecurity Policy and Strategy Senior Counsel, Security & Privacy, Intel
 - Angela McKay, Director for Cybersecurity Strategy and Policy, Global Security Strategy and Diplomacy, Microsoft
 - Ken Durbin, Continuous Monitoring and Cybersecurity Practice Manager, Symantec
-

Questions?

Please identify yourself and your organization
as you ask your question.

Group Discussion

- How current initiatives fit together
- Identification of gaps and future work needed

Please identify yourself and your organization when contributing to the discussion.

Way Forward

- Prioritization of next steps
- Identification of leads for follow-on work
- Discussion of future related meetings

Please identify yourself and your organization when contributing to the discussion.

National Security Council

- Concluding Comments
-