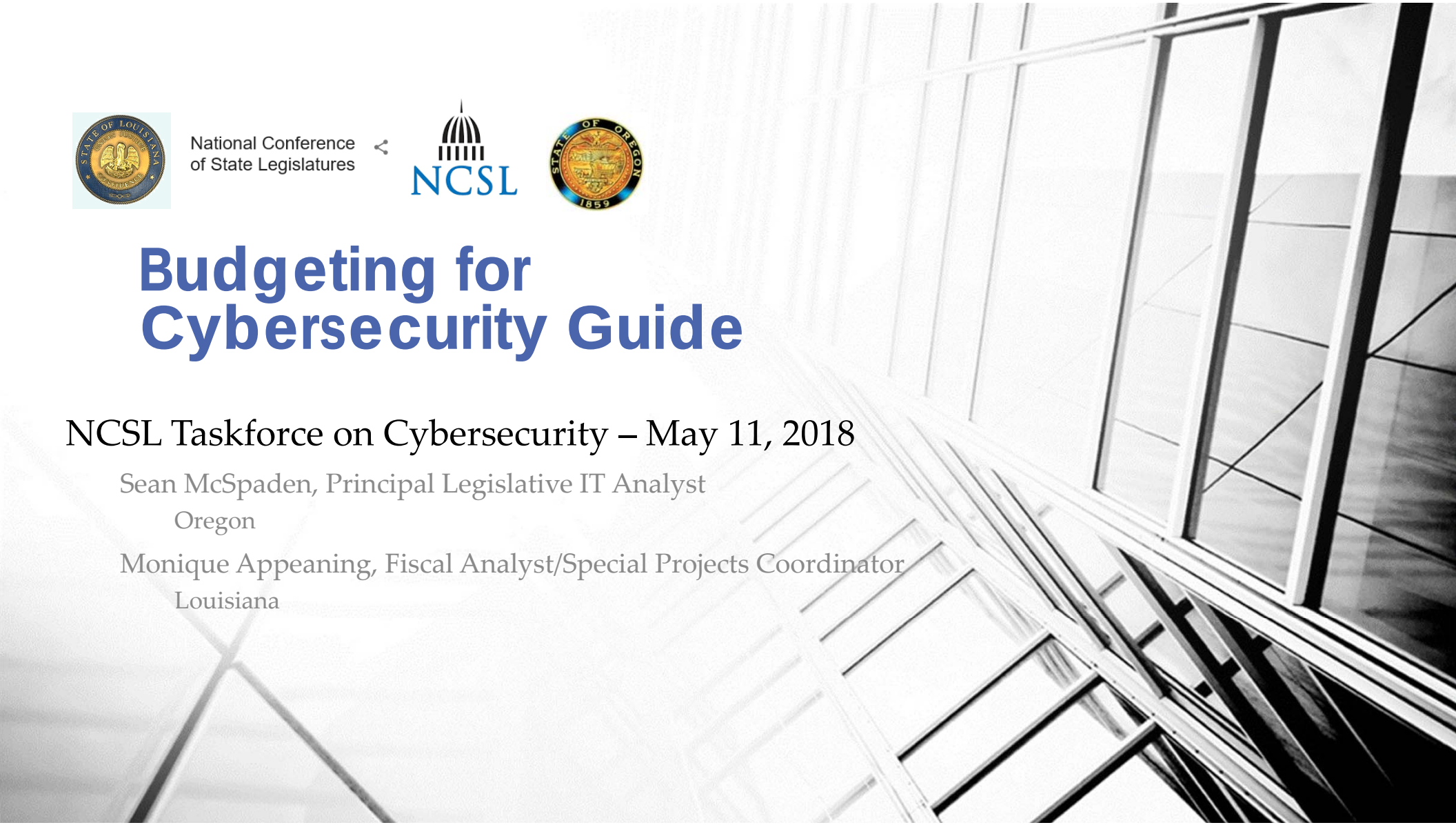

National Conference of State Legislatures

NCSL

Budgeting for Cybersecurity Guide

NCSL Taskforce on Cybersecurity – May 11, 2018

Sean McSpaden, Principal Legislative IT Analyst
Oregon

Monique Appeaning, Fiscal Analyst/Special Projects Coordinator
Louisiana

Contributors

- NCSL Cybersecurity Staff: Susan Parnas Frederick, Danielle Dean
- NASCIO – National Association of State Chief Information Officers
- 18F Office of the U.S. General Services Administration
- Oregon, Louisiana, Texas, Oklahoma, Mississippi, Connecticut, Michigan, and Illinois

THANK YOU

Purpose of the Guide

- Starting point for discussion on cybersecurity-related budget requests
- Help Legislators and Legislative Staff better understand
  - Cybersecurity terminology
  - Cybersecurity Risks that exist
  - Typical activities and resources required – Planning, Preparation, Mitigation, Response and Recovery
  - Cyber preparedness – an ongoing process that requires "maintenance of effort" and flexibility in budgeting
  - Resource prioritization, governance and organizational models
- Help Legislators and Legislative Staff feel comfortable with cybersecurity-related budget numbers and what they are based on.

Underlying Premise of the Guide

- State government systems, networks and infrastructure are vital…. And are under near constant cyber attack
- Organizational Structure and Placement of Responsibility & Accountability for Cybersecurity - Matters
  - Must know who is supposed to lead; who is responsible & accountable
  - Directly affects – type, scale, and complexity of governance, organizational and funding models
  - Drives budgeting and cost allocation decisions - individual agency, program area/multi-agency, branch-wide, or statewide

Cybersecurity Governance, Responsibility and Accountability

- Who must be involved? Who makes which decisions?
- How will risk be assessed and by what criteria?
- Acceptable risk (risk tolerance) – who decides?
- How will risks be addressed? Coordinated vs. Independent approach
- Who implements proposed solutions?
- Who is responsible?
- Who is ultimately accountable?

Cybersecurity Strategy, Program and Assessments

- Reasonable expectations
  - Formal Cybersecurity Strategy – agency, branch-wide, or statewide
  - Regular Risk Assessments – at least once per biennium (if not more often)
    - Those responsible must share – when, who, what (at an appropriate level of detail), and consequences (i.e. what risks will/won't be addressed if budget is/isn't approved)
  - Regular Vulnerability Assessments of key facilities, data centers, networks, systems based on mission criticality – at least monthly or quarterly
  - Penetration Tests for at risk facilities and systems (as warranted)
  - Rules of engagement for information sharing
    - Must provide Legislative branch with the information it needs for appropriations and oversight WHILE protecting access to and disclosure of sensitive information

Cybersecurity Education and Training

- Cybersecurity is a team sport! Involves PEOPLE, processes and technology
- Employee training is essential (consistent and uniform)
  - User Awareness (at least annually)
  - Technical (one-time and on-going)
    - Cybersecurity landscape is constantly shifting
    - Cyber attacks are becoming increasingly sophisticated
    - Knowledge, skills and abilities must be validated and periodically (if not continually) updated over time.
- State legislators and legislative staff should be open to reasonable and justified training-related budget requests.
  - If training isn't occurring and budget requests aren't made – something is wrong

Cybersecurity – Hardware, Software, Services

- Budget requests should include monies (one-time and ongoing) for hardware, software and professional services related (but not limited) to:
  - IT Asset Inventory
  - Vulnerability Scanning
  - Firewalls
  - Intrusion Detection & Intrusion Prevention Systems
  - Anti-virus, anti-spam/spam-filtering, and anti-malware software
  - Log management and monitoring software
- Some hardware & software is best deployed centrally; some can be deployed locally
- Responsible approach – leverage existing hardware/software investments to the greatest extent possible
- Redundant/duplicative investments should be proactively avoided

Cybersecurity – Third Party-managed Services

- Insourcing cybersecurity as a core state government function is preferred <u>but not always possible</u>
- Third-party cybersecurity consulting and managed services may be required
- Budget requests may include (but not limited to):
  - Security operations center (SOC) services
  - Firewall services
  - Intrusion detection system (IDS) and intrusion prevention system (IPS) services
  - Incident and breach response services
  - Monitoring, detection, and alerting services
  - Forensic investigation and analysis services; and more recently
  - Cyber Analytics

Cybersecurity – related Audits

- Internal
  - Step 1: Ensure regular auditing of cyber-related activities
  - Step 2: Require actionable improvements
  - Step 3: Understand each agency's multi-year strategy
- Executive/Legislative Audits
  - Key Questions
    - Does your state have a legislative auditing office or an IT committee with statutory authority to evaluate, validate, and report on the security practices of state government?
    - Is the statutory authority placed with another entity within state government (perhaps the secretary of state)?
    - Can the auditing entity perform comparable evaluations for all three branches of government and for other public bodies (for example, local governments, schools or special districts)?
    - Are the costs for cyber-related audits budgeted for in advance or are they unexpected/unbudgeted expenses?

Cybersecurity – related Audits (Continued)

- Federal Government Audits
  - List of federal regulations and laws with which states must comply is numerous and diverse, and affect most state government program areas
    - e.g. Internal Revenue Service (IRS), Health Insurance Portability Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Criminal Justice Information Services (CJIS)
  - Achieving and maintaining compliance, participating in and responding to audits can be costly and time consuming
- Audits of Third Party Hosting Facilities
  - State governments are increasingly considering use of "cloud" service providers
    - Shift from capital to operational expenditures may/may not reduce costs and may/may not make securing state data and systems more complicated and costly.
  - State legislators and legislative staff
    - Need to know how extensive the use of "cloud services" is across the enterprise
      - Should reasonably expect those responsible for cybersecurity to communicate about steps being taken to ensure state data, systems, and infrastructure remain secure in these "cloud" service provider computing environments.

Cybersecurity Insurance

Some initial questions:

- Does your state have cyber insurance? How is the yearly cost calculated?
  - If your state has cyber insurance, ask to see the underwriting document to see which agencies are insured and the cost.
- What is covered under your state's cyber insurance policy? Is that coverage adequate and uniform?
- Where is your state on the NIST scale? Mature and uniform cybersecurity practices can lower cyber insurance costs.

Conclusion

- "An ounce of prevention is worth a pound of cure." *Benjamin Franklin*
- Effectively addressing Cybersecurity in government is about exercising due diligence and due care
  - It's about governance, planning, risk assessment and management, appropriate resource allocation and deployment, and performance auditing
  - It's about leadership, stewardship, responsibility, and accountability for results
- We hope this Budgeting for Cybersecurity Guide will help you
  - Better understand and evaluate cyber-related budget requests
  - Properly assess and address your state's unique cyber risks/vulnerabilities and their associated costs

Questions / Discussion

National Conference of State Legislatures

NCSL

Contact Information

- Sean McSpaden, Principal Legislative IT Analyst
  - Oregon Legislative Fiscal Office
  - 503-986-1835 | Sean.L.McSpaden@state.or.us
- Monique Appeaning, Fiscal Analyst/Special Projects Coordinator
  - Louisiana Legislative Fiscal Office
  - 225-342-7236 | appeaningm@legis.la.gov
- NCSL Staff
  - Susan Parnas Frederick | 202-624-3566 | susan.frederick@ncsl.org
  - Danielle Dean | 202-624-8698 | danielle.dean@ncsl.org

National Conference of State Legislatures

NCSL