State of New Hampshire Cybersecurity Strategy and Actions

Commissioner Goulet

Director Plummer

Commissioner Toumpas

Assumptions

- The term “statewide” is meant to convey that scope is not limited to the executive branch.
- The items we’re proposing are in process or future state. There are many things that are already being done.
- We will take a tiered approach where a baseline will be applied to agencies in a consistent manner (no opt out), with provisions to add additional capabilities at an agency level as desired or externally mandated.

The Vision

A robust statewide cybersecurity function that provides practical and effective protection and response mechanisms, which adapt over time as threats evolve.


Cyber Security is Everyone's
Responsibility

Strategy

- Implement and operate a set of collaborative and standard processes that fully leverage existing capabilities, adding new capabilities as appropriate, and incorporating public-private partnership in a holistic manner.
- In the following areas:
  - Protection
  - Operations
  - Mitigation & Response
  - Human Factors
  - Continuous Improvement

Cybersecurity Governance

- Strategy Development, Evangelism, Implementation, Operations – **DoIT, HSEM, TAG, CAC members**
- Consult and Advise – **Agency Heads, IT Council**
- Driving Public-Private Partnership – **ACEPS ***
- Approval and Oversight – **Governor's Office**

** Refers to the ACEPS Cyber Sub-committee*

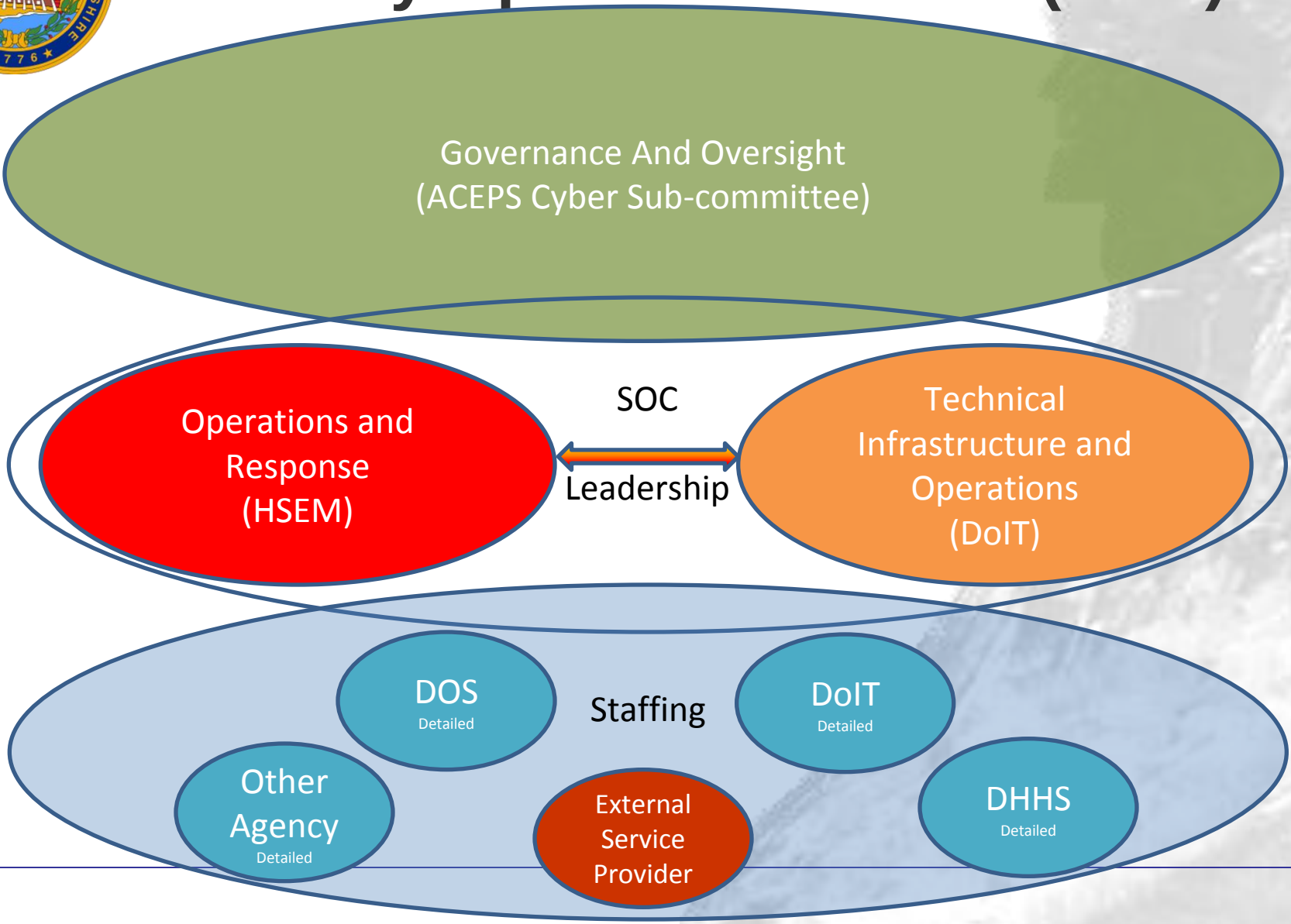
Protection

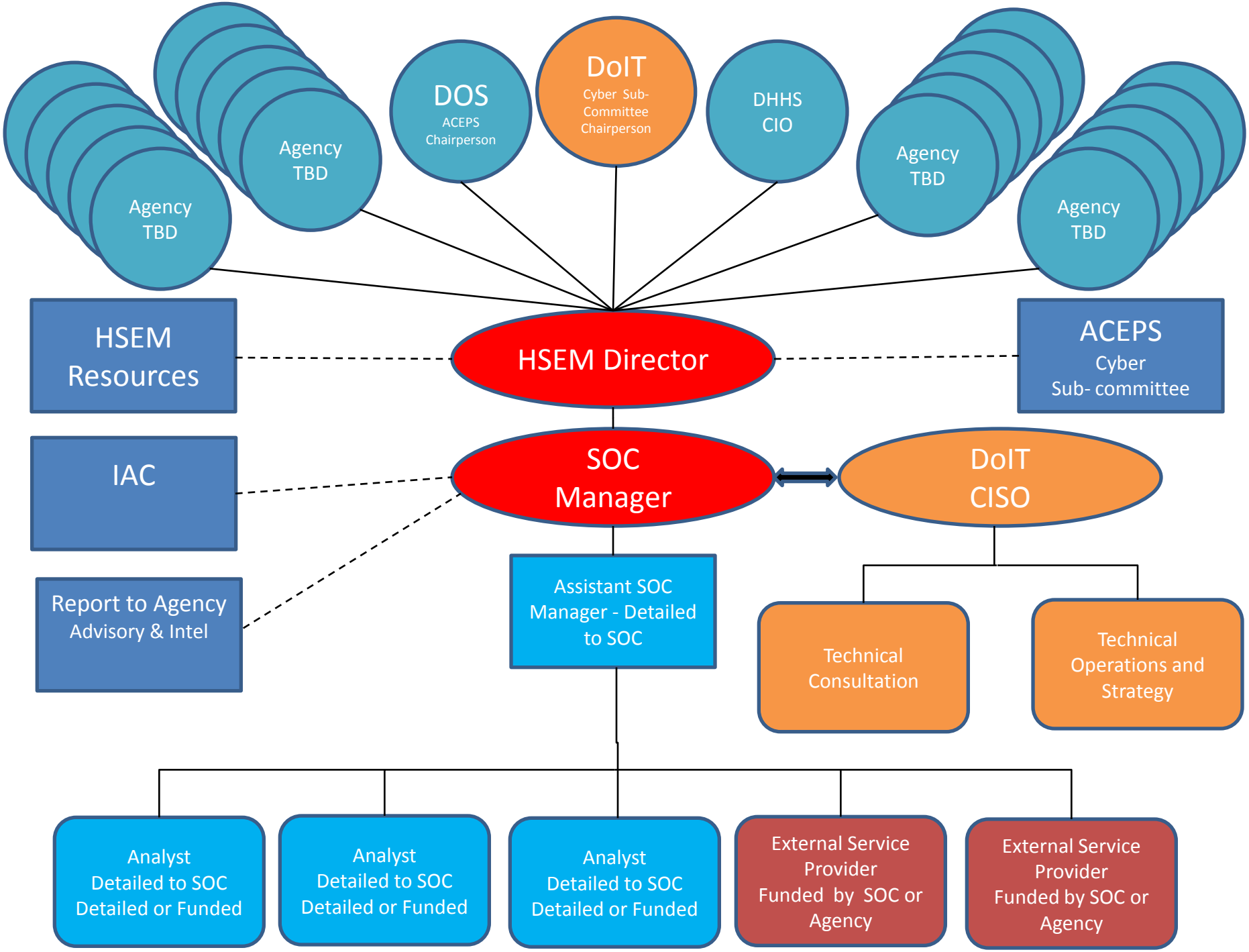
- Strengthen local administration controls
- Application white listing
- Advanced threat detection (zero day)
- Distributed denial of service (DDOS) mitigation services
- Network access controls (NAC) *(in process)*
- Administrative (Active Directory) delegation tools
- Consistent baseline policies for:
  - Computer use
  - Device protection
  - Internet access & use

Operations

- Patch management
  - Tighten up current methodologies
  - Resource appropriately
- Integrate security considerations into project planning methodology
- Commission outside assessment of posture and operational plans (risk assessment)
- Security Operations Center (SOC), collaborative & consistent statewide capabilities

Security Operations Center (SOC)




Agency TBD
Agency TBD
DOS
ACEPS Chairperson
DoIT
Cyber Sub-Committee Chairperson
DHHS CIO
Agency TBD
Agency TBD
HSEM Resources
HSEM Director
ACEPS
Cyber Sub- committee
IAC
SOC Manager
DoIT CISO
Report to Agency
Advisory & Intel
Assistant SOC Manager - Detailed to SOC
Technical Consultation
Technical Operations and Strategy
Analyst Detailed to SOC Detailed or Funded
Analyst Detailed to SOC Detailed or Funded
Analyst Detailed to SOC Detailed or Funded
External Service Provider Funded by SOC or Agency
External Service Provider Funded by SOC or Agency

Mitigation & Response

- Incident response workshops & exercises *
- Cyber insurance
- Broad collaboration to include:

DoIT	Federal Agencies
HSEM	Local Governments *
National Guard	Private Sector Entities *
State Agencies	Private Non-profit *

* *Refers to the ACEPS Cyber Sub-committee*

Cyber Insurance by Definition

Protection against losses related to information security breaches, such as data theft/loss, business interruption caused by a computer malfunction or virus, and fines or lost income because of system downtime and/or network intrusion.

Source: NASCIO 2015 Midyear Conference

Montana's Cyber Security Insurance

The state's commercial insurance policy provides coverage for:

- Data breach response costs including, but not limited to, forensic investigations, mail notification, and credit monitoring (one year)
- Fines/penalties assessed by regulatory authorities
- Revenue streams lost as a result of a breach
- Personal injuries and property damage for negligent acts or omissions of the state
- Website content and media
- Cyber ransoms and fines
- Public relations firm consultation

Source: NASCIO 2015 Midyear Conference

Human Factors

Cyber Hygiene Campaign

- Regular, accountable employee & supervisor training
- Standards for new hire screening & training
- Targeted social engineering testing:
  - Phishing and Spear Phishing
  - Flash drive exploits
  - Etc.
- Outreach to:

State Employees	Local Governments *
Agency Leadership	Private Sector Entities *
Legislative	Private Non-profit *

** Refers to the ACEPS Cyber Sub-committee*

Continuous Improvement

- Regular assessment – Agency Score Card
- Constant evaluation of new threats and methods
- Threat – risk analysis trending
- Prioritized partners (local governments and private sector entities) and address accordingly *****

** Refers to the ACEPS Cyber Sub-committee*

Challenges

- Acceptance of base standards is counter to existing culture in some cases *(employees, leadership, legislature)*
- Cross agency collaboration can be difficult
- Resources *(we will need to shift some priorities)*

Next Steps – Plan Details

- Kickoff bi-weekly SOC implementation planning sessions – August 2015
- Restart ACEPS Cyber Sub-committee – October 2015
- Ballpark pricing for DDOS mitigation services – complete
- Ballpark pricing for cyber insurance – September 2015
- Propose cyber investment level & plan to get there - TBD
- Plan to operationalize cybersecurity capital budget item – In Process

Next Steps – Plan Ratification

- Review cybersecurity plan with IT Council – 7/29/2015
- Review and solicit feedback from Commissioners – TBD
- Review and solicit feedback from CAC – 8/27/2015
- Update to Governor's Office – September 2015
- Review and final ratification by IT Council – October 2015