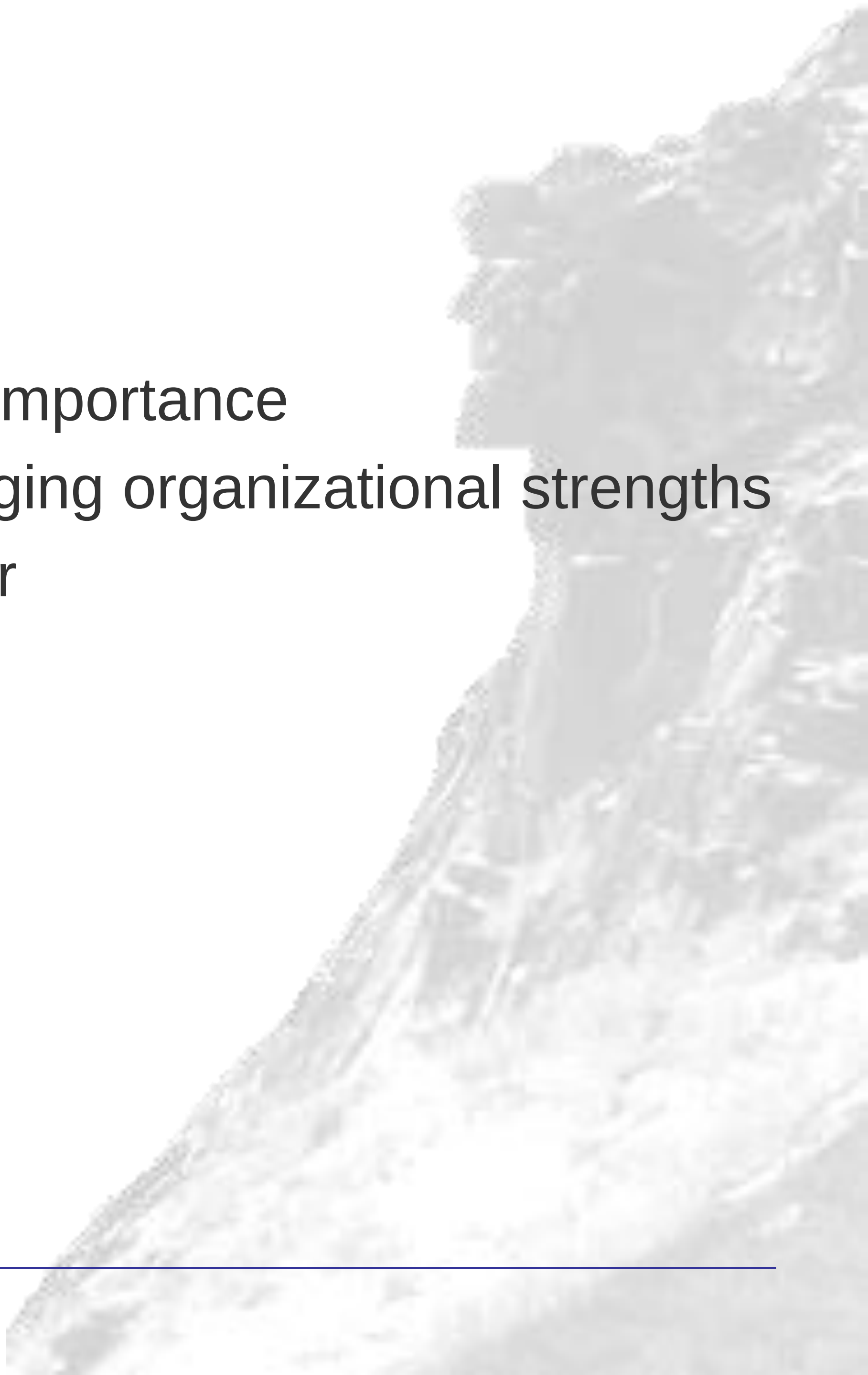
State of New Hampshire Cybersecurity Update

Perry Plummer, Director HSEM
Denis Goulet, Commissioner & CIO

10/28/2016

AGENDA

- Background, highlighting the importance
- All Hazards Approach, leveraging organizational strengths
- Explaining the executive order
- Next steps



Cyber Attacks – Do we have a problem?

Who’s being Attacked?

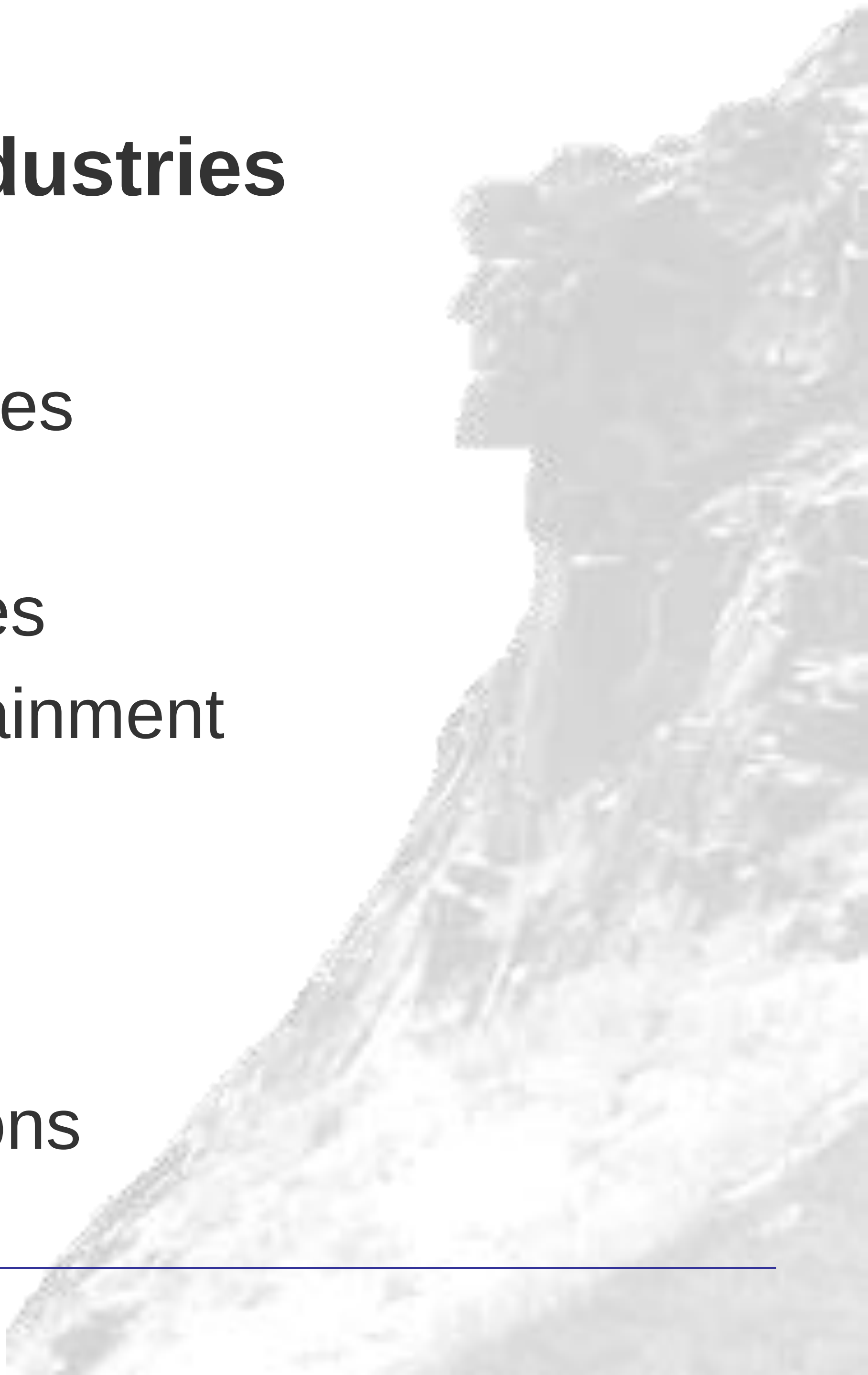
- Sony
- Target
- Anthem
- Fiat Chrysler
- IRS
- TJ Max
- US Office of Personnel Management

Just to name a few!

Most Hacked Industries?

Most Hacked Industries

- 28% Computer Services
- ***<u>15 % Government</u>***
- 12% Financial Services
- 9% Media and Entertainment
- 7% Education
- 5% Healthcare
- 5% Retail
- 5% Telecommunications



Strapped for resources. State and local governments are a prime target for the pervasive and sophisticated threats launched by stealthy cyber criminals. These attacks are not just an epidemic, they are a pandemic.

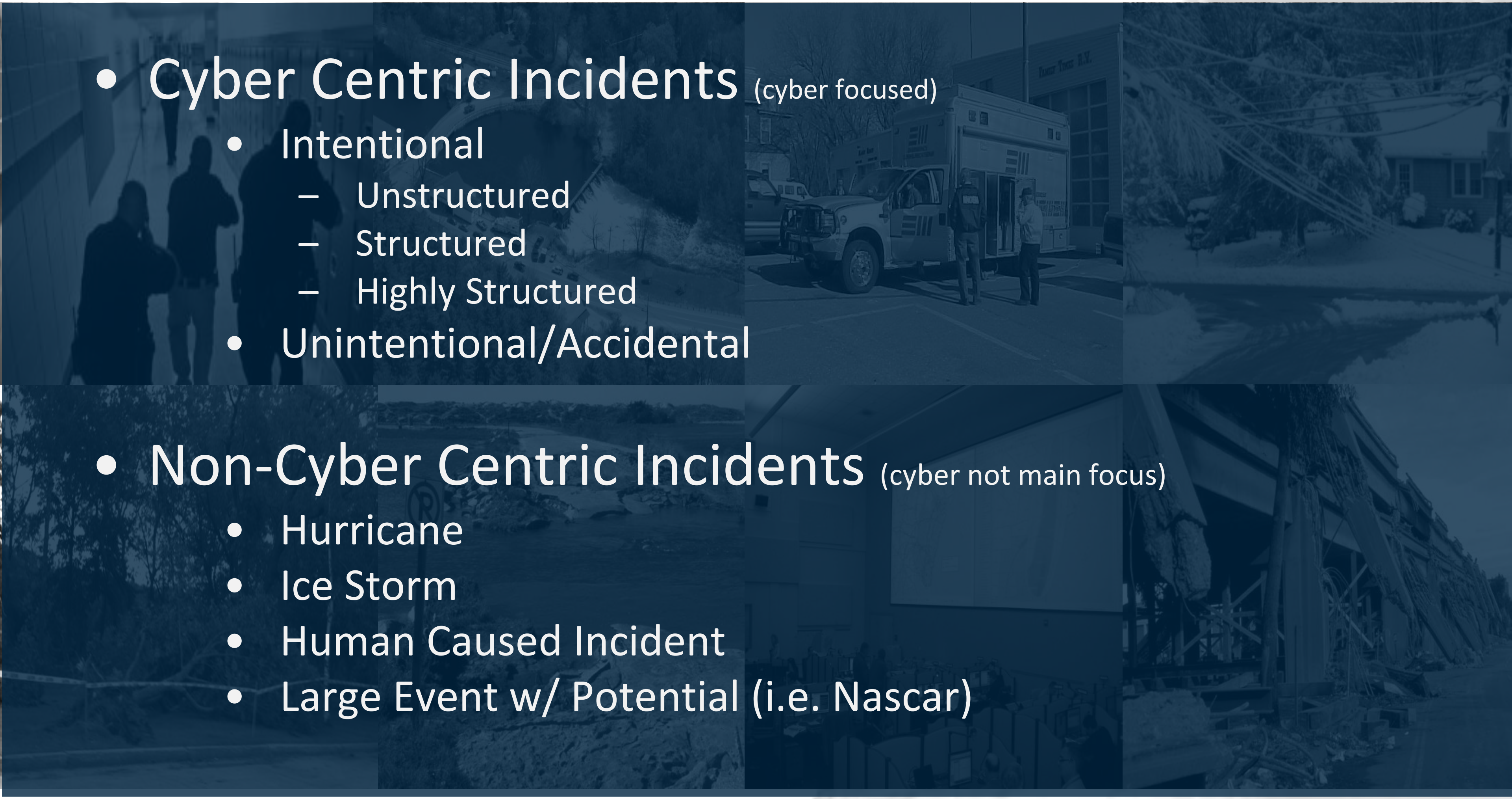
Unfortunately, no one is safe and diligent proactive mechanisms are the only cure!

FireEye – Research Study

How are we going to respond?

- All Hazards Approach
  - Anticipate
  - Prepare
  - Respond
  - Recover

Cyber Incidents



- Cyber Centric Incidents (cyber focused)
  - Intentional
    - Unstructured
    - Structured
    - Highly Structured
  - Unintentional/Accidental

- Non-Cyber Centric Incidents (cyber not main focus)
  - Hurricane
  - Ice Storm
  - Human Caused Incident
  - Large Event w/ Potential (i.e. Nascar)

A Cyber incident is like an iceberg!

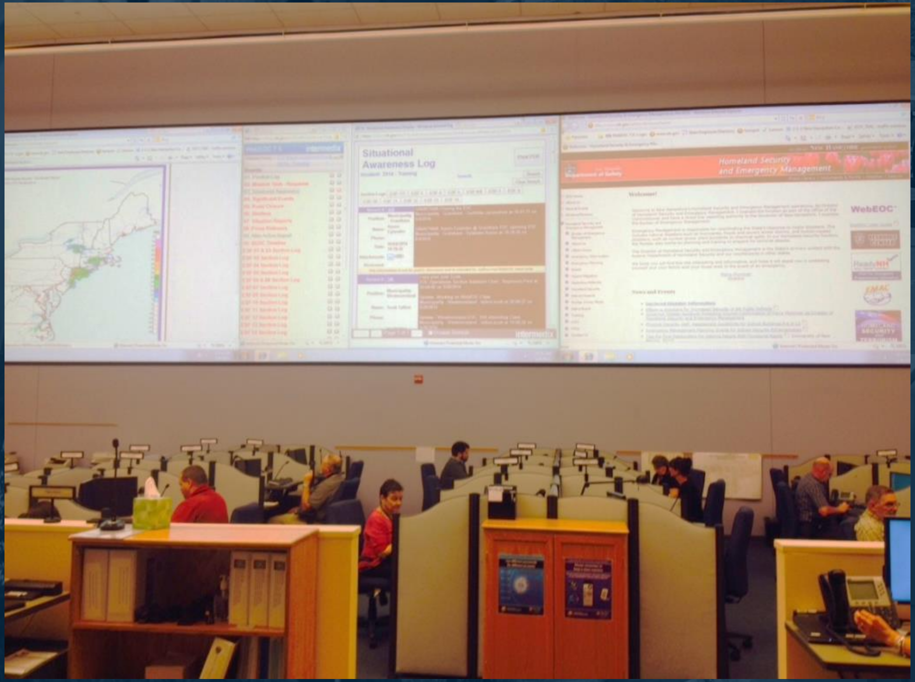
Cyber Response Team Role (State Network ?)

EOC Role also includes:

- All State Operations
  - All branches
- Local Communities
- Critical Infrastructure
  - All Sectors
- Public Safety
- Business Community / Private Sector

"Whole Community" Approach

State Emergency Operations Center (EOC)


Situational Awareness Log
Homeland Security and Emergency Management
WebEOC

155 EOC activations in past 8 years
20 times in FY2014

- **Central Command**
  - Coordinate State Response
  - Facilitate Federal Response
- **Maintain a *big picture* view**
- **Resource for Local EOC's & State Agencies**

EOC Coordination

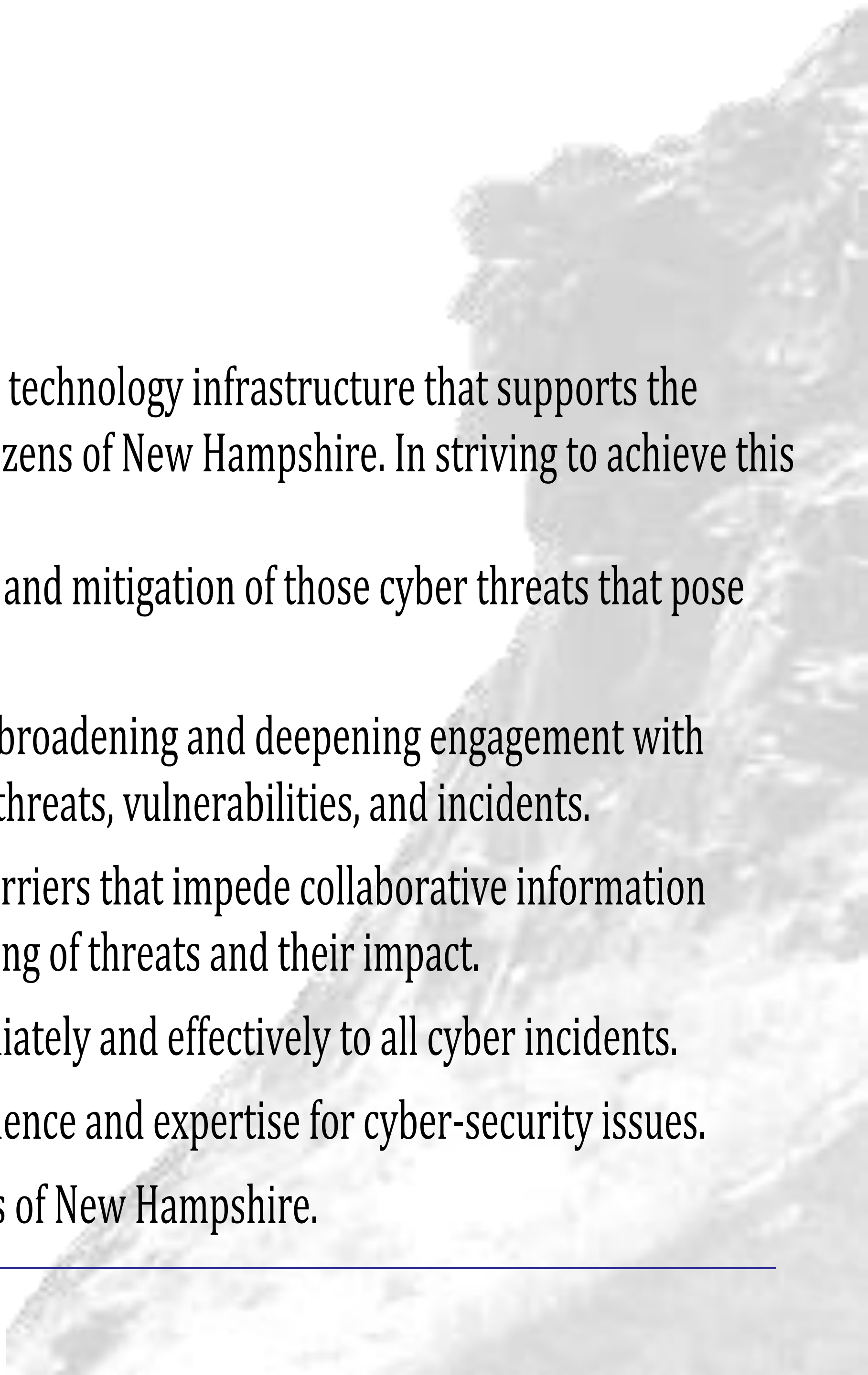
Emergency Support Functions (ESF)

1. Transportation
2. Communications & Alerting
3. Public Works & Engineering
4. Firefighting
5. Emergency Management
6. Mass Care, Housing and Human Services
7. Resource Support
8. Health & Medical
9. Search & Rescue
10. Hazardous Materials
11. Agriculture, Natural and Cultural Resources
12. Energy
13. Public Safety & Law Enforcement
14. Long-Term Community Recovery & Mitigation
15. Public Information

The Executive Order

- Establishes the New Hampshire Cyber Integration Center (NHCIC), within the Incident Planning and Operations Center (IPOC)
- Sets the expectation for timely and complete information sharing with NHCIC
- Defines an oversight and governance vehicle, NHCIC Executive Oversight Committee
- Reaffirms the important role of the Cybersecurity Advisory Committee (CAC)

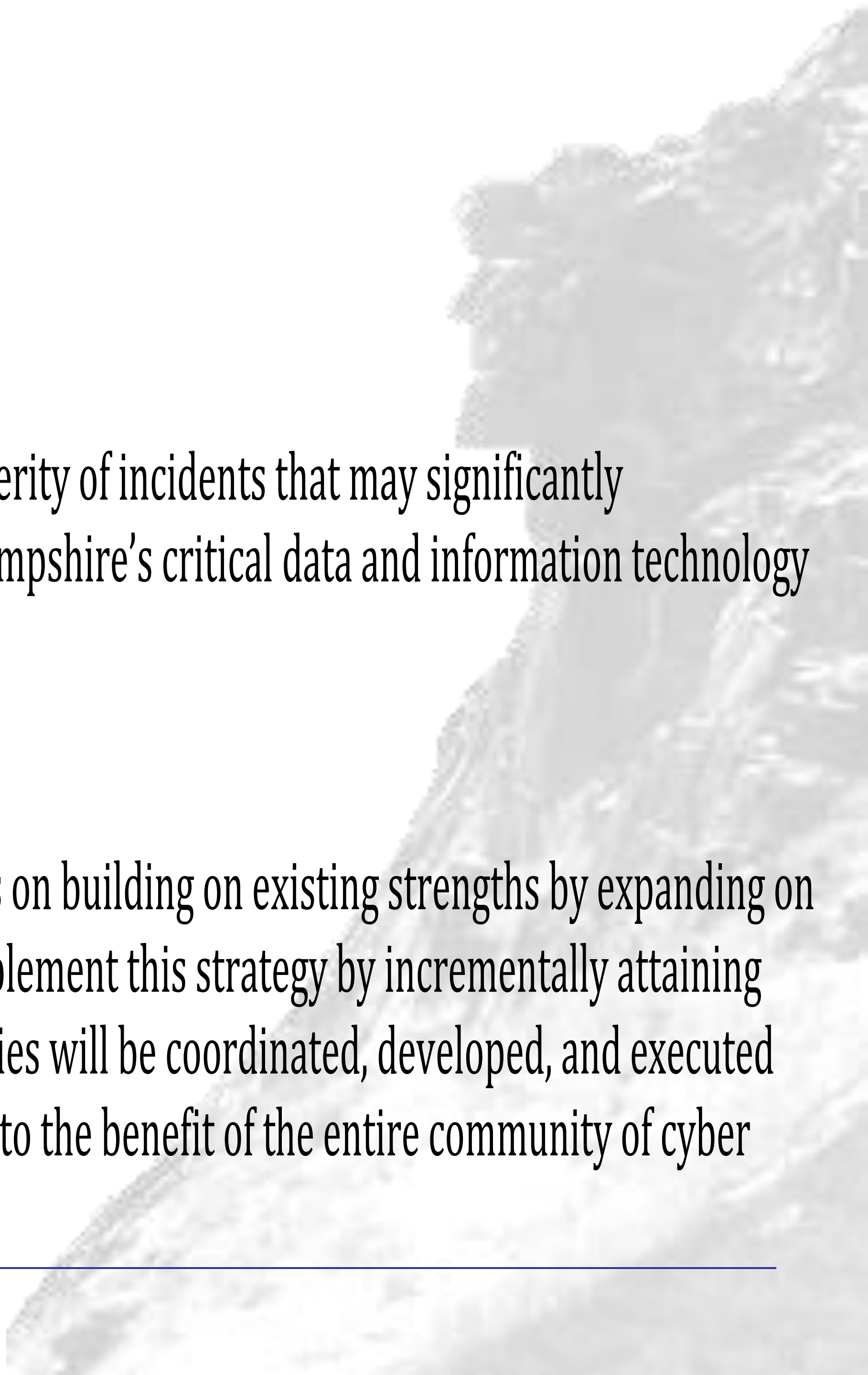
NHCIC, Vision



The NHCIC vision is a secure and resilient information technology infrastructure that supports the security, economy, and the health and safety of the citizens of New Hampshire. In striving to achieve this vision, the NHCIC will:

- Focus on proactively coordinating the prevention and mitigation of those cyber threats that pose the greatest risk to New Hampshire.
- Pursue whole-of-state operational integration by broadening and deepening engagement with partners through information sharing to manage threats, vulnerabilities, and incidents.
- Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.
- Maintain a sustained readiness to respond immediately and effectively to all cyber incidents.
- Serve stakeholders as a state wide center of excellence and expertise for cyber-security issues.
- Protect the privacy and critical data of the citizens of New Hampshire.

NHCIC… continued



Mission:

The NHCIC mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the New Hampshire's critical data and information technology infrastructure.

Approach:

To execute its mission effectively, the NHCIC will focus on building on existing strengths by expanding on their scope and breadth over time. The NHCIC will implement this strategy by incrementally attaining additional capabilities over time. Many of these activities will be coordinated, developed, and executed collaboratively with the NHCIC's operational partners to the benefit of the entire community of cyber stakeholders in New Hampshire.

Some Next Steps

- Adapt existing space in the IPOC
- Cross train the initial team members
- Consolidate monitoring and operations into the IPOC
- Setup DoIT helpdesk to accept cyber incident calls 7x24
- Setup 7x24 duty officer schedule
- Finalize Concept of Operations (CONOPS)