National Initiative for Cybersecurity Education (NICE)

(formerly known as "CNCI Initiative 8")

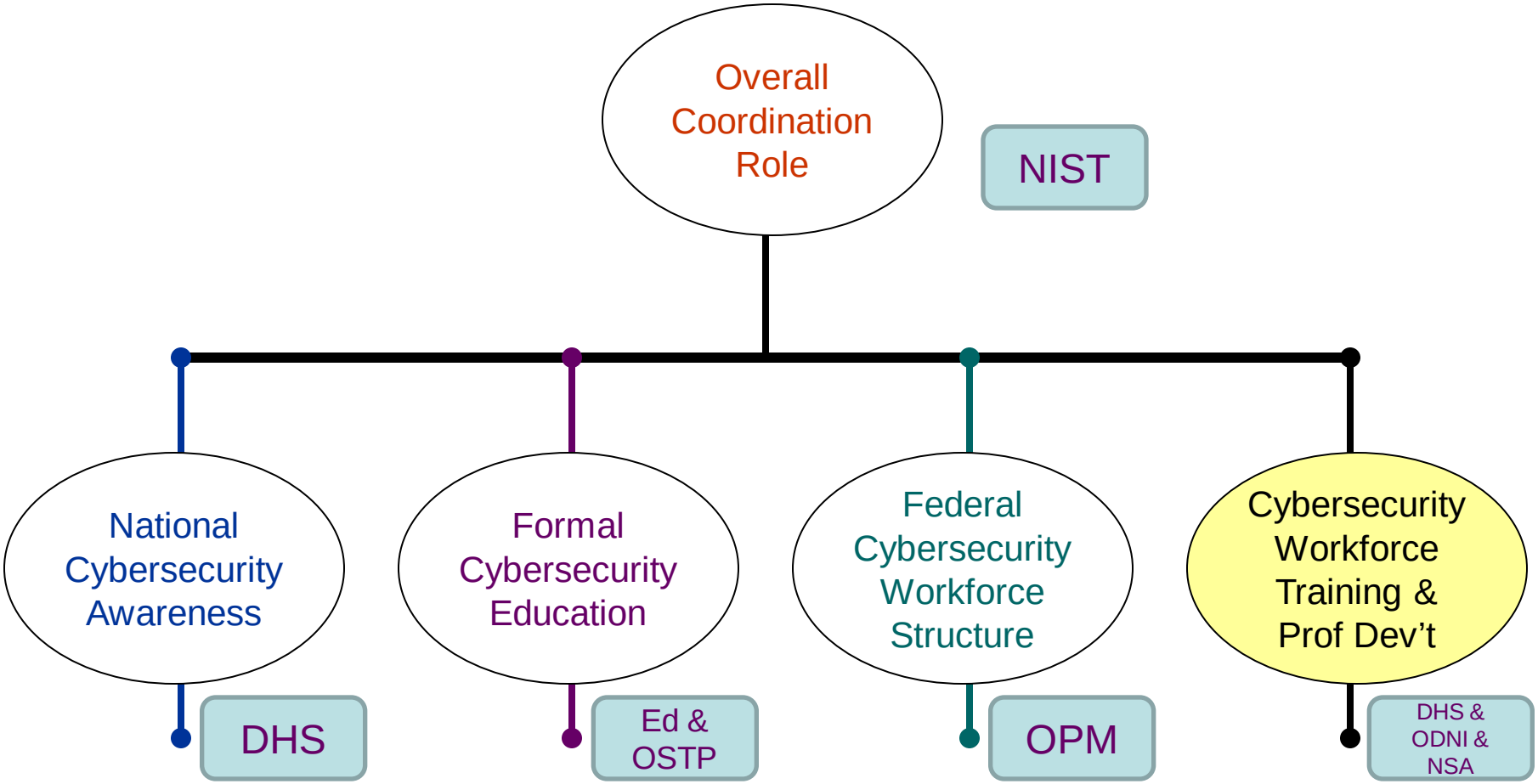
Track 4 – Cybersecurity Workforce Training and Professional Development

Working Group Summary

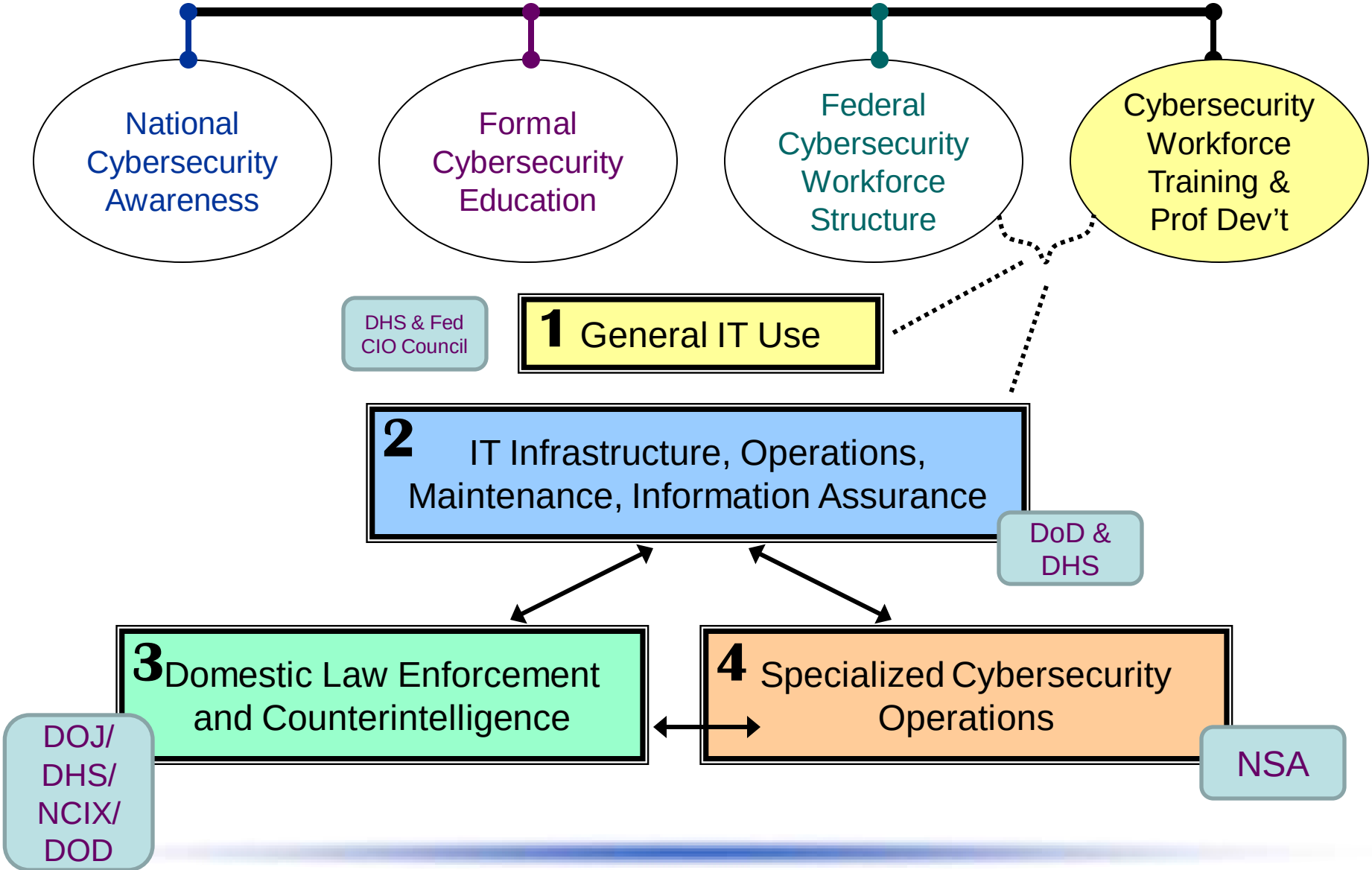
12 August, 2010

"Building Capacity for a Digital Nation" --
The President's Cyberspace Policy Review

Organizational Structure



Track 4: Four Functional Work Areas



Morning Sessions
(Cybersecurity Workforce and Education/Training Issues)

Industry Panel

- IT standards strictly enforced; leadership included in process
- Need and want everyone in the cyber fight; all and interested and empowered; no different in government and industry
- Youth are frequent users, but not more security savvy
- Needs to be deep, it needs to be national; IT departments should not be assumed to do all the training and security (shared responsibility)
- Collaboration with academic institutions and training providers
- Leverage "blended" learning options
- Regular "spear-phising" exercises (ROI)
- Full-time practitioners as trainers; curriculum is irrelevant with the wrong instructor; knowledge matters more than taking classes; measure practical experience
- New required skill sets -- Cyber hunters, risk analysts/managers, incident analysts, malware forensics, etc… eye to the future
- Three challenges:
  - Out of the "1000," how many more have we created?
  - Need to make pathways to those who are uncomfortable with technical work
  - Transform the areas of architecture and engineering of IT

Morning Sessions

(Cybersecurity Workforce and Education/Training Issues)

Government Panel

- Three buckets: acquire, grow, and sustain
- What are the basic skills for the cybersecurity professionals?
  - Need that piece of essential knowledge for all federal employees
  - Expanded for others
- Learn from the private sector; agreements exist – open up to partners from private sector; have to change mindsets
- Hiring, hiring, hiring

Morning Sessions
(Cybersecurity Workforce and Education/Training Issues)

Joint Panel

- Very important to collaborate and work together
- Follow-up is critical
- Developing a common framework (lexicon, skills, etc.)
- In competition for same workforce… need to build shared workforce for the nation

Afternoon Sessions
(Professional Development Model)

Presentation of Cyber Workforce “Professional Development Model” and discussions

- Briefing: Generate ideas and understand national perspectives on the competency assurance needed for typical work roles.
- Exercise to generate ideas regarding the necessity or suitability of different types of professional development components for a specific work role or community of interest.

Afternoon Sessions

Track Four Functional Areas 1, 2, 3 presentations and best practices

Track 4 – Cybersecurity
Workforce Training and Professional Development

Summary/Key Points

- Given time limit outlined Functional Areas 1 and 2
- Will be constructing Working Groups in the future
- DCITA/DC3 is “model” organization for creating an enterprise training resource…
- Communications of broad and future efforts is critical

Track Four
3 X 5 Card Topics (1)

- National SysAdmin Standard does not exist. What performance matrices/score should be passing?

- Using the continuum of cyber training (instruction, exercise, competition, and certification), how do you use this life cycle and what tools are required?

- How is the federal government going to put programs/ policies together that will help the hiring process within the federal government?

- Is the federal government willing to change its hiring process? Will it be streamlined to make it quicker and smoother?

Track Four
3 X 5 Card Topics (2)

- What are the specific job-related skills sets required for the national cyber-related workforce, broken down into John Mills' four key areas?

- On the topic of professionalization, will the discussions lead to a career path such that a new hire will understand the knowledge and learning needed to advance (this may help retention in Track 3, but may not mesh with current practices where advancement is achieved by changing jobs/companies)?

- Is discussion limited to cyber training, or will training include other "softer" skills, which will create a well-rounded professional (i.e., driving toward all the needs of a CISO other roles leading to a CISO)?

Questions?