National Initiative for Cybersecurity Education (NICE)

(formerly known as "CNCI Initiative 8")

Track 4 – Cybersecurity Workforce Training and Professional Development

11 August, 2010

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

Groundwork for NICE

- **Cybersecurity** identified as one of the most serious economic and national security challenges we face.
- **NICE** was established to help face this challenge head on
  - –with a strategy to build a cyber savvy nation through training, awareness, K through post-graduate educational programs,
  - –and professional development for federal security professionals.
- Builds on the Comprehensive National Cyber Initiative's Initiative 8 -- "Expand cyber education."
- NICE will establish operational, sustainable, and continually improving cybersecurity education.

Track 4 Charter (Goal)

- *"In collaboration with private industry as appropriate, as well as State, local and tribal partners, establish, provide or otherwise set standards and strategies for National cybersecurity training and professional development, including those required for Federal government civilian, military, and contractor personnel.*
- *In accordance with the objectives of the White House Cybersecurity Policy Review and Initiative 8 of the Comprehensive National Cybersecurity Initiative (CNCI); disseminate those standards and strategies to, and facilitate their adoption by, US educators, state and local governments, and private industry"*

Track 4 Tasks

- **Establish Requirements:** Using an agreed-upon taxonomy of competencies and occupational specialties
- **Determine Current Capabilities:** Catalog, by specialty and competencies, training and professional development programs offered
- **Identify and Close Training/Development Gaps:** Identify gaps that exist between training/professional development requirements, and existing programs, and strategies to close gaps
- **Project and Propose Resource Requirements.** Review current and projected resource requirements and develop appropriate out-year estimates
- **Develop Objectives, Metrics and Measures:** Identify measurable objectives and input, process, output, and outcome metrics/measures

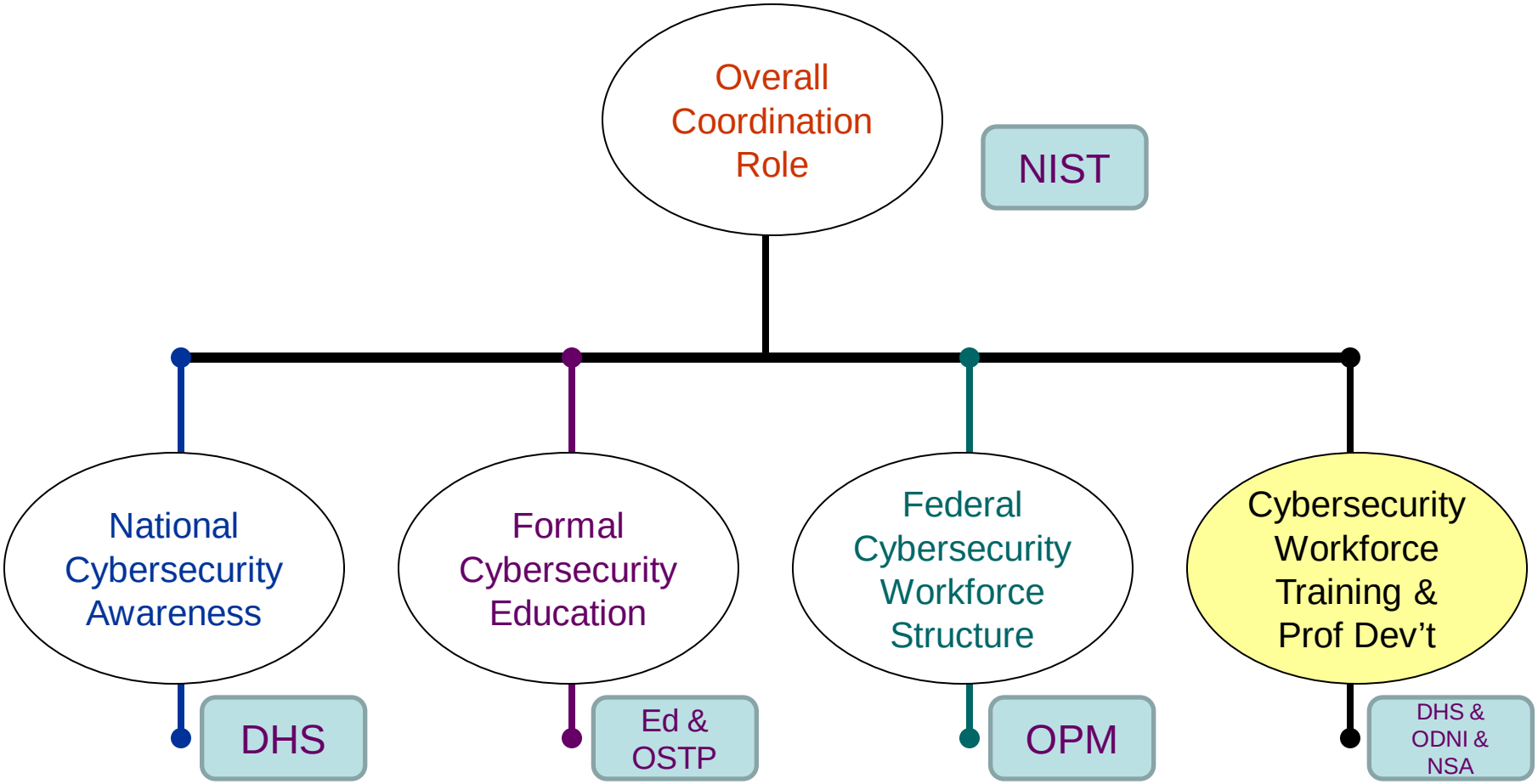
Track 4 Interdependencies

- **Interdependent Requirements.** Tracks 3 and 4 will both require appropriate competency models and update or establish new Federal occupational series to reflect that analysis.
- **Interdependent Standards.** Jointly-developed competencies serve as the foundation for various professional qualification, training, promotion, and performance standards, as well as career paths and professional development plans and programs.
- **Interdependent Results.** Seamless integration between requirements, recruiting and accessions, training and career/professional development, and workforce sustainment/retention.
- **Relationships:** Build upon relationships established with academic institutions, State, local and tribal governments, associations' certification vendors, and private training organizations.

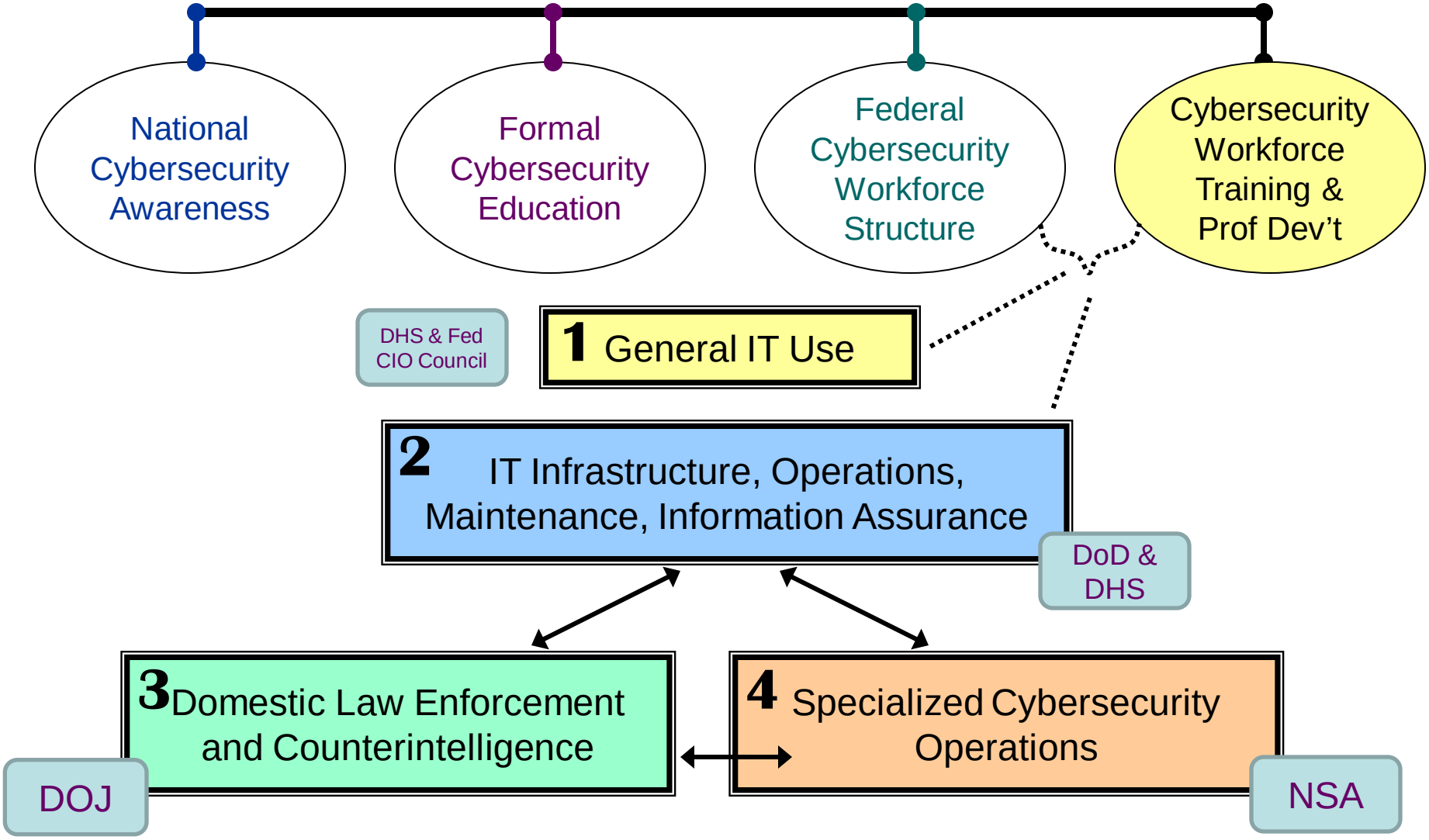
Approach to Track 4

- National in scope
  - focused effort towards the Federal workforce, including all federal civilian employees, members of the uniformed services, and contractor personnel who have direct or indirect access to a US Government (USG) computer network or information system,
  - with subsequent efforts extended to US public and private organizations external to the USG
- One of four complementary, synergistic tracks under NICE
- Tri-Leads: DoD, ODNI, DHS
- Four sub-tracks or “functional areas”

Organizational Structure



Track 4: Four Functional Work Areas



Track 4 Gameplan

Provide an opportunity for the four 'Functional Area' leads under the National Initiative for Cybersecurity Education (NICE), Track 4 (Cybersecurity Workforce Training and Professional Development) to:

- Gather, compare notes and progress, and to synergize and harmonize their efforts
- Focus on aligning approaches, overall planning, and charter development, and
- Discuss resourcing needs and programs.

Recognizes the interrelationships of all the workforce elements

Functional Area 1: General IT Use

- Scope: All Federal civilian employees, members of the uniformed services, and contractor personnel who have direct or indirect access to a USG computer network or information system, to ensure that they know and can carry out their general information/network security responsibilities.

Functional Area 2: IT Infrastructure, Operations, Maintenance, Information Assurance

- Scope: Those civilian employees, members of the uniformed services, and contractor IT professionals who have significant responsibilities for designing, developing, installing, operating, provisioning, protecting, or maintaining the security of IT networks.

Functional Area 3: Domestic Law Enforcement and Counterintelligence

- Scope: Domestic Law Enforcement Investigators (sworn officers and intelligence analysts) and members of the uniformed services involved in counterintelligence investigations of cyber events involving domestic IT systems, networks, and/or digital information/evidence.

Functional Area 4: Specialized Cybersecurity Operations

- Scope: Those Federal civilian employees, members of the uniformed services, and contractor personnel employed by departments and agencies who are engaged in **highly specialized and largely classified** cybersecurity operations focused on collection, exploitation and response.