Lessons Learned from Cyber S&T Roadmap Development

14 April 2014

Dr. Steven E. King

Deputy Director for Cyber Technology

Information Systems & Cyber Security Directorate (IS&CS)

Assistant Secretary of Defense for Research and Engineering

(U) S&T Influencing the DOD Cyber Landscape

- **The Cyber S&T community plays a key role to support DoD strategic objectives:**
  - DoD Strategic Priorities
  - Cyberspace Policy
  - Trustworthy Cyberspace
  - COCOM capability requirements
  - Strategy for Operating in Cyberspace
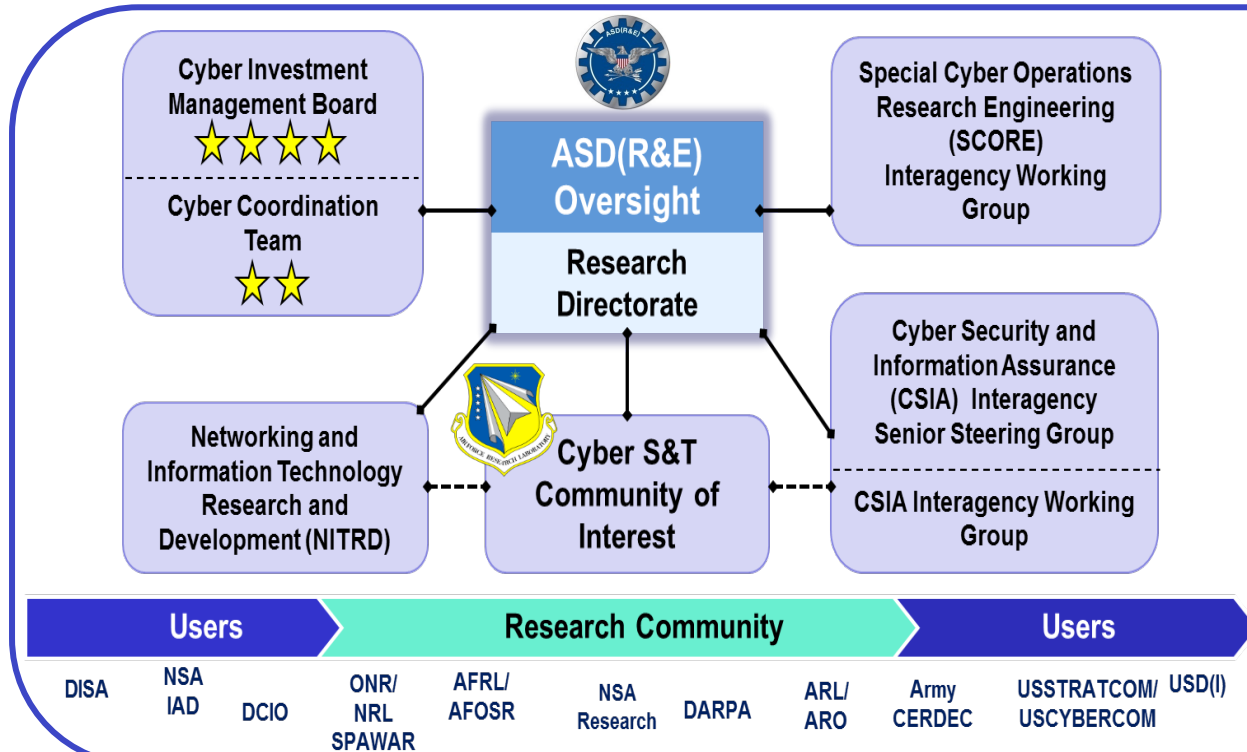 - Priorities for 21st Century Defense

Cyber Integration Group (CIG)

Cyber Investment Management Board (CIMB)

COCOMs

S&T Community

Enhance United States National Security & Economic Prosperity

(U) DoD Cyber S&T Coordination

Management

ASD(R&E)
- OSD led the development of the original Cyber S&T Roadmap
- Now provides oversight to the Community of Interest (COI)

Execution

AF Research Lab (AFRL)
- Leads the COI, and update of the Cyber S&T Roadmap

Service Labs and NSA
- Collaboratively develop the Roadmap, providing input from their Service organization perspectives

Engagement

USCYBERCOM
- Provided operational and capabilities requirements
- Defining mission team functions and capability requirements

Joint Chiefs of Staff
- Provided Cyberspace Operational Activity requirements

Diagram elements:

- Cyber Investment Management Board ★★★★
- Cyber Coordination Team ★★
- ASD(R&E) Oversight — Research Directorate
- Special Cyber Operations Research Engineering (SCORE) Interagency Working Group
- Cyber Security and Information Assurance (CSIA) Interagency Senior Steering Group
- CSIA Interagency Working Group
- Networking and Information Technology Research and Development (NITRD)
- Cyber S&T Community of Interest

Process arrow: Users → Research Community → Users

Users	Research Community	Users
DISA	ONR/ NRL SPAWAR	ARL/ ARO
NSA IAD	AFRL/ AFOSR	Army CERDEC
DCIO	NSA Research	USSTRATCOM/ USCYBERCOM
	DARPA	USD(I)

(U) Roadmap Lessons Learned

- **Cyber S&T Roadmap is organized by technology areas**
- **Extremely difficult to define metrics by technology areas**
- **Candidate metrics will be identified in terms of operational capabilities**
- **Cyber domain/threats are constantly evolving, requiring frequent updates to Roadmap**
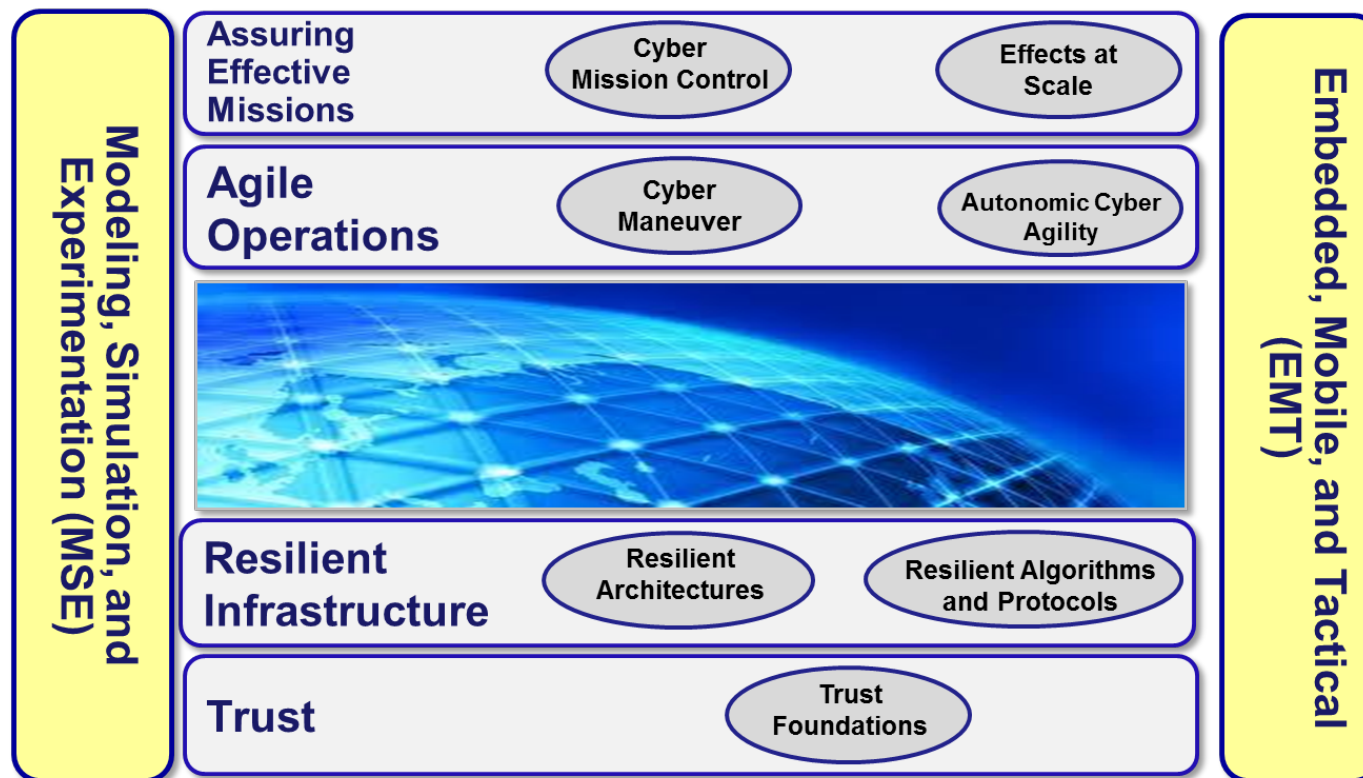
BACKUP

Cyber S&T Capability Framework

Defensive Capabilities

Discover, understand, and block the adversary	Make embedded/ weapons systems resilient	Reduce DoD Network attack surface

Situational Awareness and Courses of Action Capabilities

Map networks and systems	Understand cyber dependencies of missions	Integrate course of action analysis across cyber, other non-kinetic and kinetic

Figure is UNCLASSIFIED