

www.DAU.mil



Foundational Learning



Workflow Learning



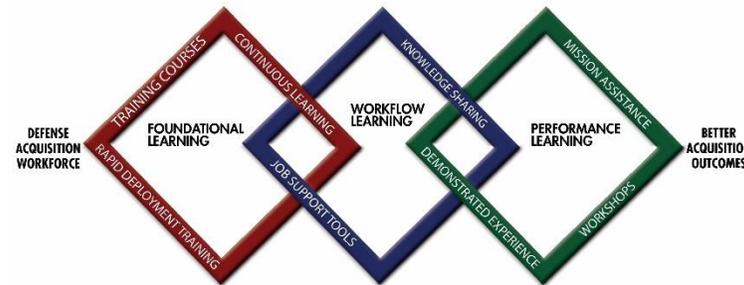
Performance Learning

David Pearson
Director, Engineering and Technology Center
May 25, 2016



DAU CYBERSECURITY CURRICULUM

- Cybersecurity Drivers in DoD and DAU
- Foundational Learning Developments
- Performance Learning Efforts
- Workflow Learning Initiatives
- Future Plans



Acquisition Learning Model

DAU is well positioned to provide cybersecurity training to the acquisition workforce



Cybersecurity (CS) Definition

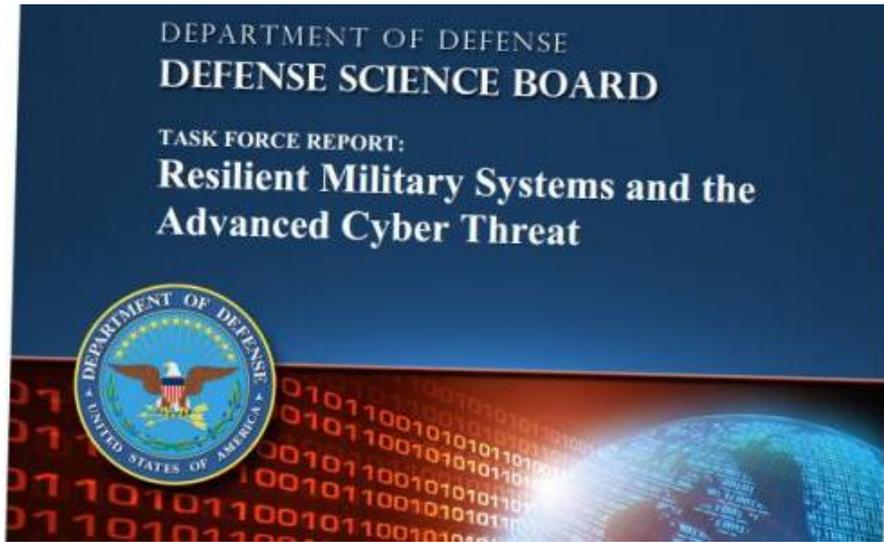
“Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”

National Security Presidential Directive-54 / Homeland Security Presidential Directive-23, “Cybersecurity Policy,” January 8, 2008



Cybersecurity Concerns

- **Enormous investments in our national security (programs) may be compromised**

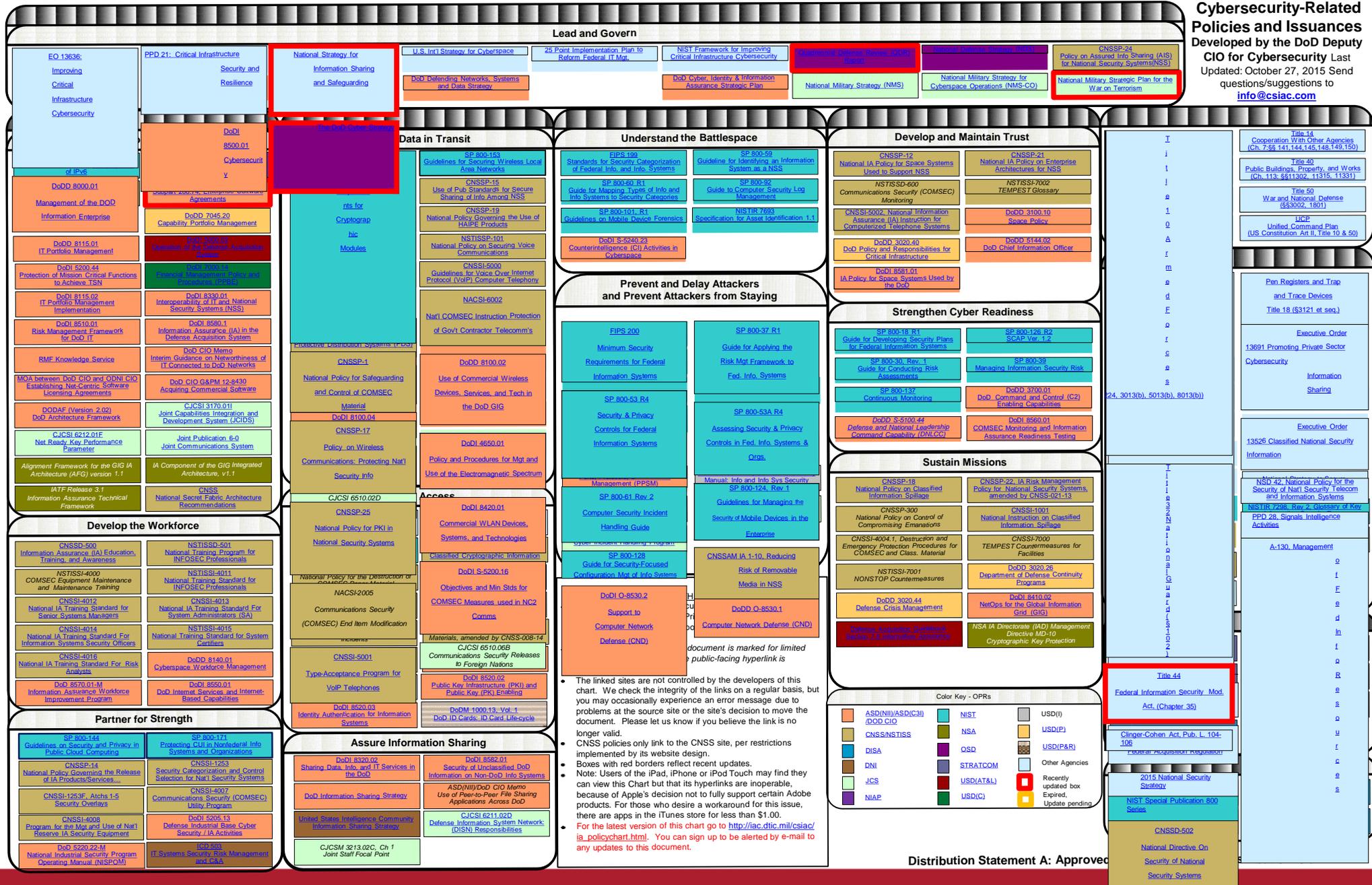


JAN 2013

- **Commanders unable to control our forces and our systems**
 - Weapons systems may not fire or operate (effectively)
 - C2 and Business systems failures
 - Weapons may be aimed back at US
- **Commanders lose trust in information in our systems**
 - Will our critical systems work under cyber attack?
 - Denial of Services: Networks, Infrastructure, Resupply
 - Data and Supply Chain Corruption

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances Developed by the DoD Deputy CIO for Cybersecurity
 Last Updated: October 27, 2015
 Send questions/suggestions to info@csiac.com



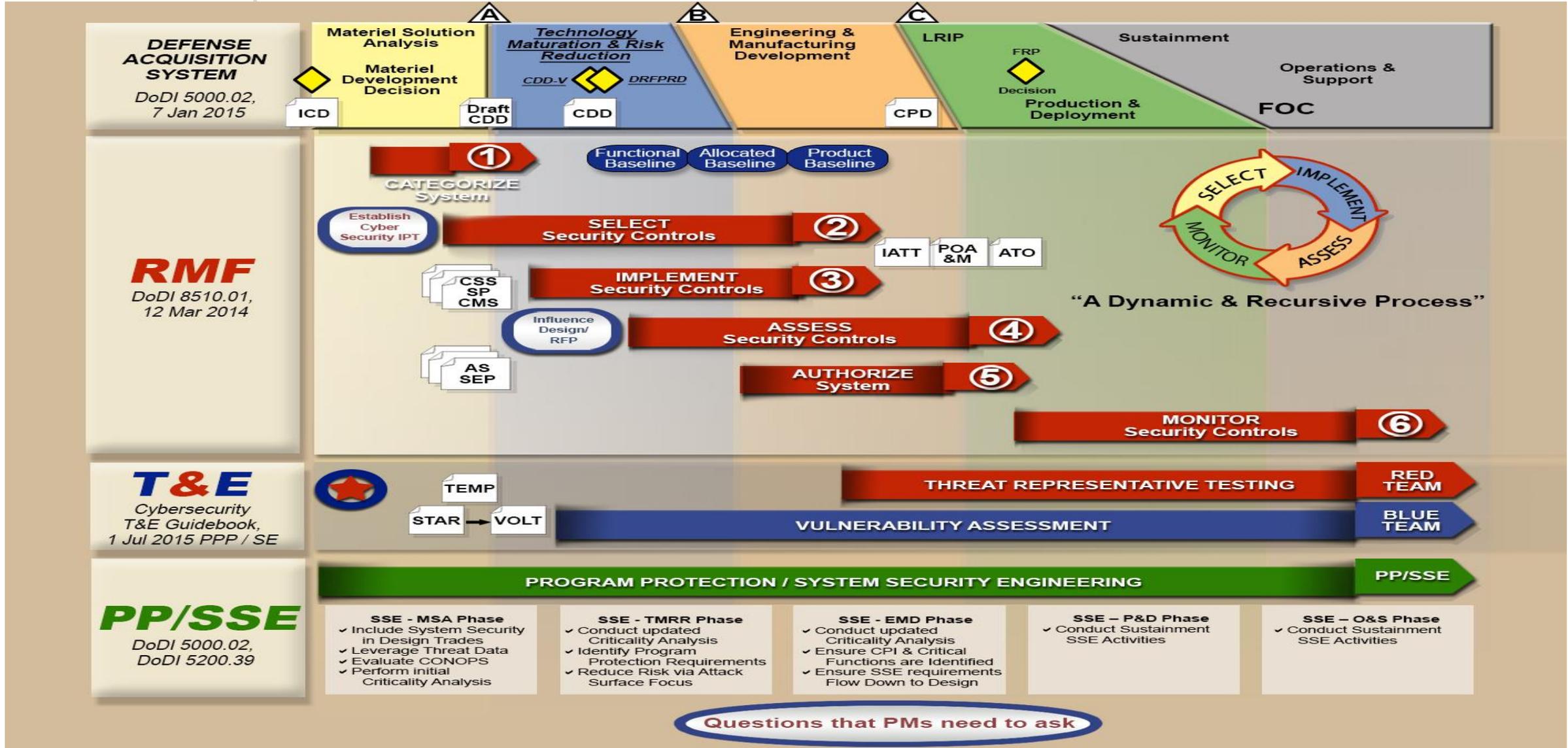
The linked sites are not controlled by the developers of this chart. We check the integrity of the links on a regular basis, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.

- CNSS policies only link to the CNSS site, per restrictions implemented by its website design.
- Boxes with red borders reflect recent updates.
- Note: Users of the iPad, iPhone or iPod Touch may find they can view this chart but that its hyperlinks are inoperable, because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than \$1.00.
- For the latest version of this chart go to http://iac.dtic.mil/csia/ia_policychart.html. You can sign up to be alerted by e-mail to any updates to this document.

Distribution Statement A: Approved



Cybersecurity Across the Lifecycle





Stakeholders Driving Demand

- Acquisition Workforce Functional Leaders
- Mr. Kendall's Better Buying Power 3.0 initiatives
- Practitioners and field-level acquisition organizations

DAU Has Proactively Responded



Foundational Learning – IT

- CLE 074 Cybersecurity Throughout DoD Acquisition
 - Fielded in April 2015
- ISA 220 Risk Management Framework for Practitioners
 - Development in progress: student pilot scheduled for Jan. 2017
- FY16 New Starts
 - CLE 079 Supply Chain Risk Management
 - CLE 080 Software Assurance



Foundational Learning – ENG

- ACQ 160 Program Planning Protection Awareness
 - Provides an overview of program protection concepts, policy and processes
 - Intended for entire acquisition workforce with emphasis on ENG and PM
 - On track for June 2016 student pilot
- ENG 260 Intermediate Program Protection Planning
 - Focuses on application of PPP concepts and processes
 - Intended for systems engineers and system security engineers
 - Finalized course design document



Foundational Learning

- Test and Evaluation
 - New cybersecurity T&E process inserted into T&E curriculum
- Program Management
 - ACQ 202
 - PMT 252
 - PMT 352A
 - DSMC
- Contracting
 - CON 360
- Logistics
 - LOG 350



Performance Learning

- Extensive mission assistance efforts ongoing and planned
 - Air Force
 - Defense Contract Management Agency (DCMA)
 - Space and Naval Warfare Systems Command (SPAWAR)
 - Marine Corps Systems Command
 - Risk Management Framework Workshop
 - SPAWAR
 - NSWC Panama City



Workflow Learning

- Enhanced Web presence
- Risk Management Framework workshop for senior leaders
- Repurposing mission assistance products
- National Initiative for Cybersecurity Education (NICE) framework-based buildout of dozens of workflow learning assets is underway



NICE National Cybersecurity Workforce Framework

- The [National Cybersecurity Workforce Framework](#) provides a blueprint to categorize, organize and describe cybersecurity work into specialty areas, tasks, and knowledge, skills and abilities (KSAs).
- Consists of 32 specialty areas in 7 categories with associated KSAs grouped within each of the specialty areas.



Category	Responsible For:	Specialty Areas
Securely Provision	Conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development	IA Compliance, Enterprise Architecture, Sys Req Planning, Sys Development, SW Engineering, Tech Demonstration, Test & Evaluation

Knowledge, Skills and Abilities (KSAs) for each competency within the NICE framework will be a major driver for future DAU Workflow Learning Products



Looking ahead...

- Defense Acquisition Workforce as part of DoD's Cyberspace Workforce
 - DoD CIO to establish certification standards
 - AT&L to establish qualification requirements for work roles associated with R&D and acquisition of DoD IT, information systems, platform IT and cyberspace activities.
- Continued integration of cybersecurity training across the Acquisition Learning Model
- Cybersecurity Culture and Compliance Initiative (DC3I)



Summary

- Cybersecurity is a warfighting domain with deep implications for acquisition
- DAU is now well positioned to provide cybersecurity training to the acquisition workforce
- A coordinated strategy working across the ALM is being used to develop learning assets of varying formats
- Implementation of cyberspace workforce training requirements is maturing