



Certification Training



Knowledge Sharing



Continuous Learning



Mission Assistance

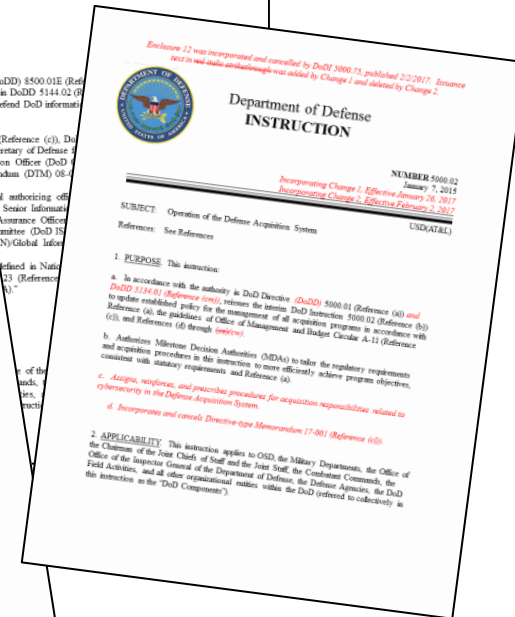
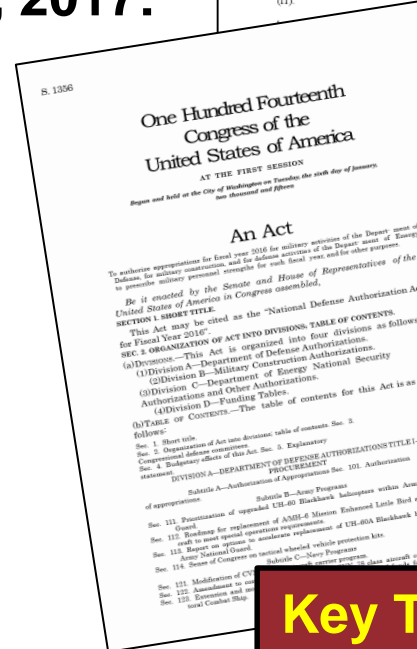
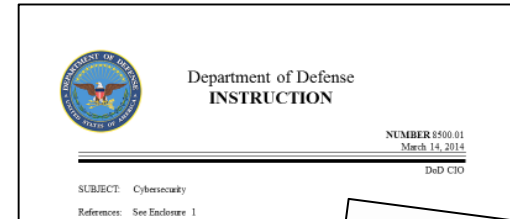
Professor Edward A. Adkins
Defense Acquisition University (DAU)
Engineering, Test and Cybersecurity
Edward.Adkins@dau.mil

Cybersecurity & Resiliency: Key Actions for T&E Personnel



Overview

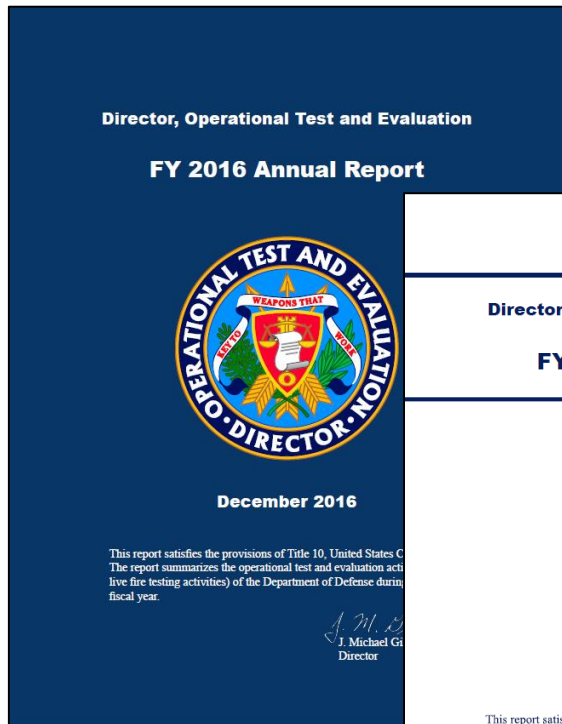
- Why the Big Deal?
- DODI 8500.01 & 8510.01, Mar 2014
- DODI 5000.02 dated Feb 2, 2017:
 - Program Managers
 - T&E Community
 - Service AOs
- Resiliency & NDAA 1647
- Summary



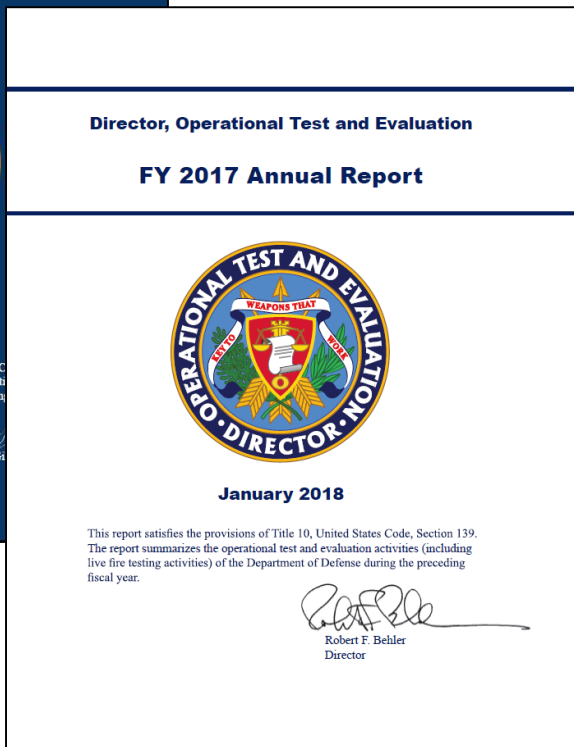
Key T&E Take-Aways here



Why the Big Deal?



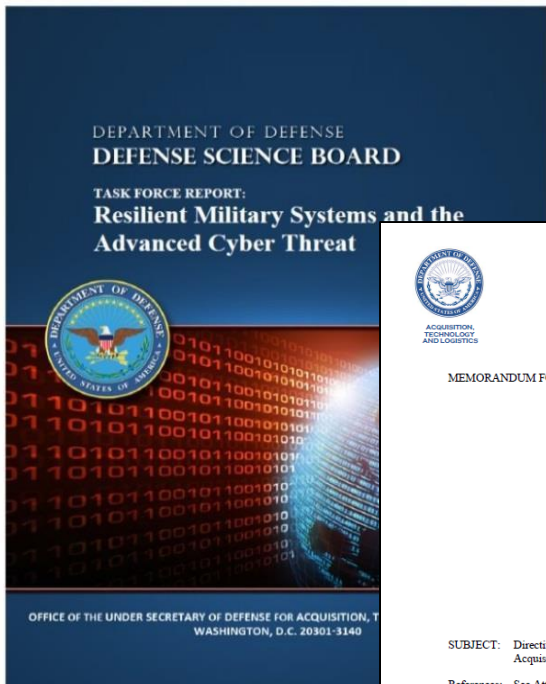
DOT&E 2016 Annual Report: “Most operational tests have found significant vulnerabilities and limitations in the system’s ability to sustain missions or rapidly restore capabilities when compromised.” (p 441)



DOT&E 2017 Report reported on a Joint Missile Program: “The contractor identified a Category I vulnerability during test preparation: a trained and knowledgeable cyber analyst could gain access to the missile guidance software.” (p. 107)



Why the Big Deal?



DSB Report: “The DoD should **expect cyber attacks to be part of all conflicts in the future**, and should not expect competitors to play by our version of the rules” (p.5)



THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

January 11, 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF
DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE
AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC
AFFAIRS
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-type Memorandum (DTM) 17-001 – Cybersecurity in the Defense Acquisition System

References: See Attachment 1.

Purpose. In accordance with the authority in DoD Directive (DoDD) 5134.01, this DTM:

- Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.
- This DTM is effective January 11, 2017; it must be incorporated into DoD Instruction (DoDI) 5000.02. This DTM will expire January 11, 2018.

Applicability. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this DTM as the “DoD Components”).

Policy. It is DoD policy that:

Decision Type Memorandum
17-001, dated 1-11-17:

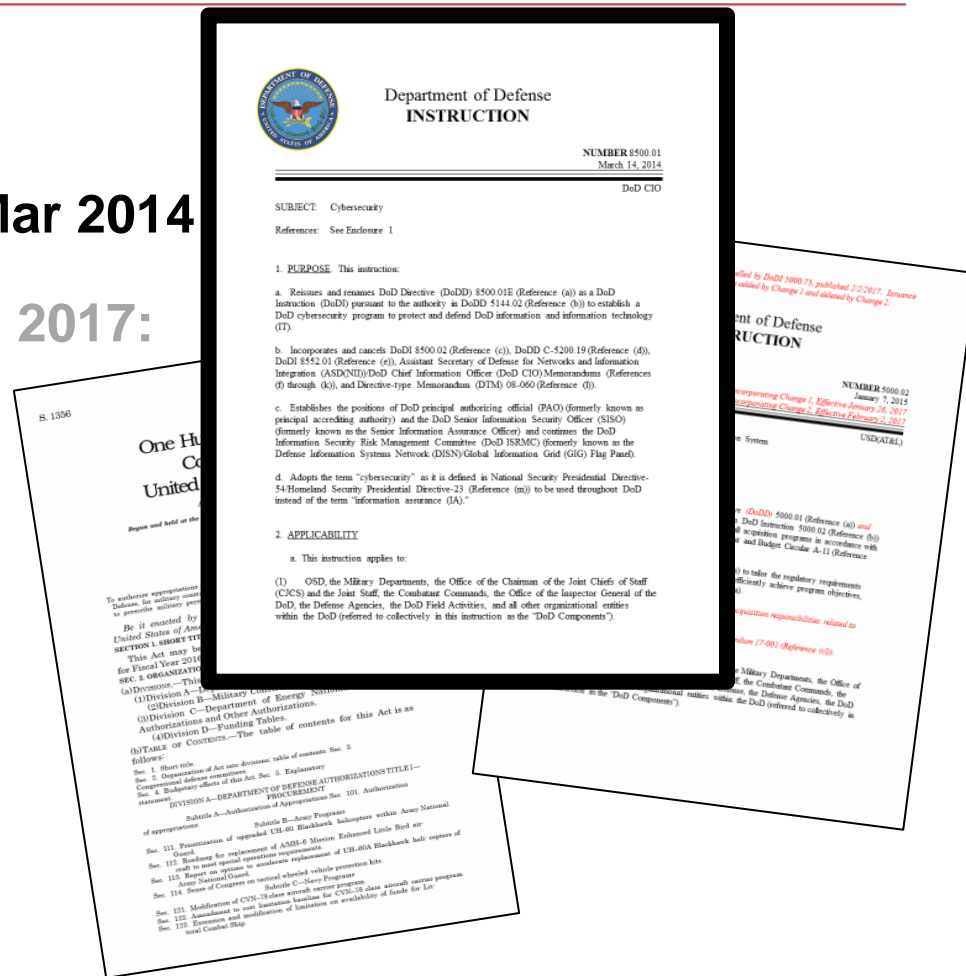
“Responsibility for
cybersecurity extends to
**all members of the
acquisition workforce.”**

A BIG DEAL for Testers!



Overview

- Why the Big Deal?
- DODI 8500.01 & 8510.01, Mar 2014
- DODI 5000.02 dated Feb 2, 2017:
 - Program Managers
 - T&E Community
 - Service AOs
- Resiliency & NDAA 1647
- Summary



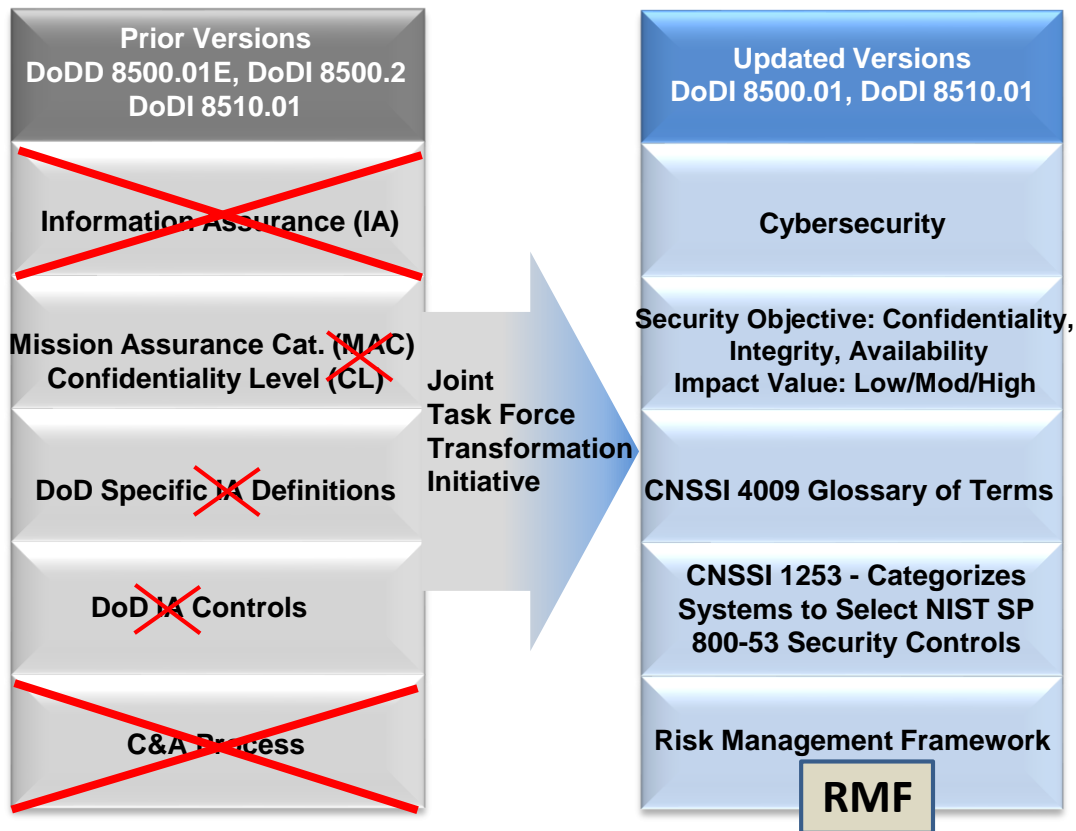


DODI 8500.01: Cybersecurity

The DoD CIO updated several 8500-series publications to transition from ~~information assurance (IA)~~ to Cybersecurity.
~~Not Cyber Security!~~

These policies employ a more holistic, adaptive, resilient and dynamic approach to implement cybersecurity across the full spectrum of IT and cyber operations.

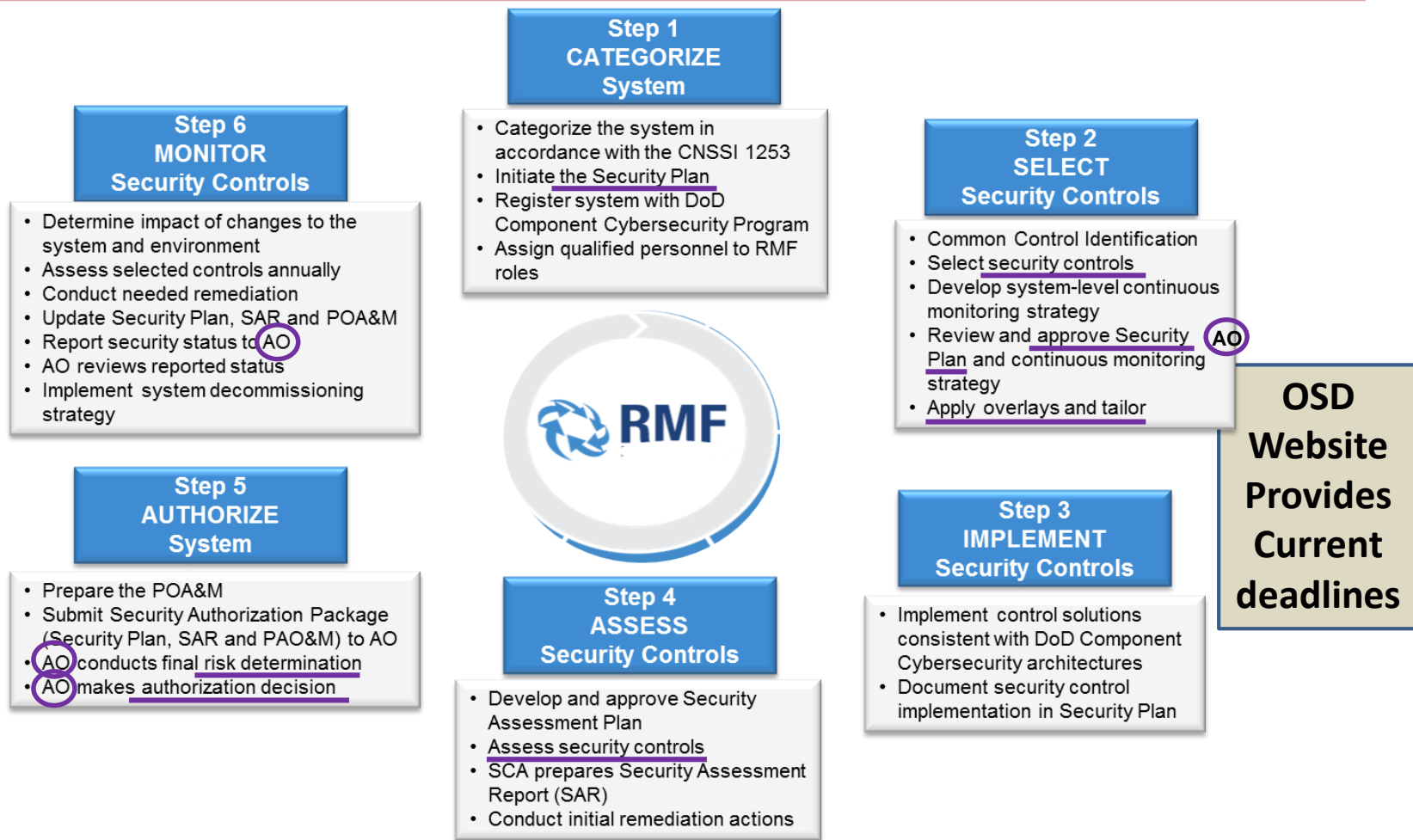
Both revised March 2014



Use current / correct terms



DODI 8510.01: RMF





OSD Website... the RMF Timeline

Completed DIACAP Package Submitted to AO for Signature	ATO Date	Maximum Duration of ATO under DIACAP
Present through May 31, 2015	Determined by AO Signature Date	2.5 years from AO signature date (Nov 30, 2017)
June 1, 2015 through February 1, 2016		2 years from AO signature date (Feb 1, 2018)
February 2, 2016 through October 1, 2016		1.5 years from AO signature date (Apr 1, 2018)

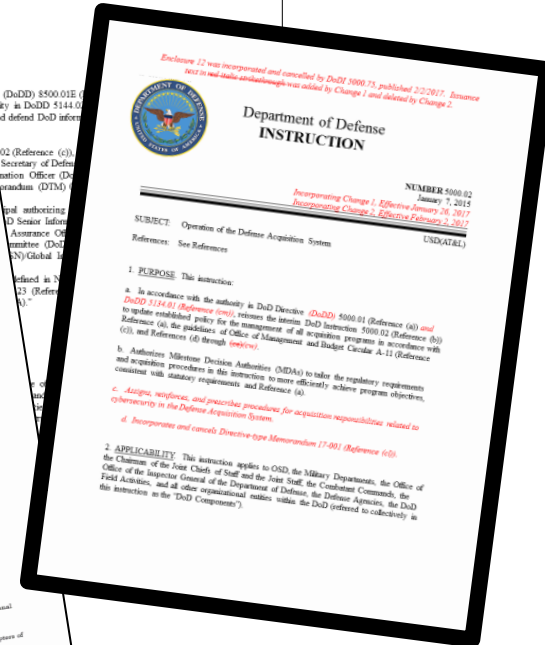
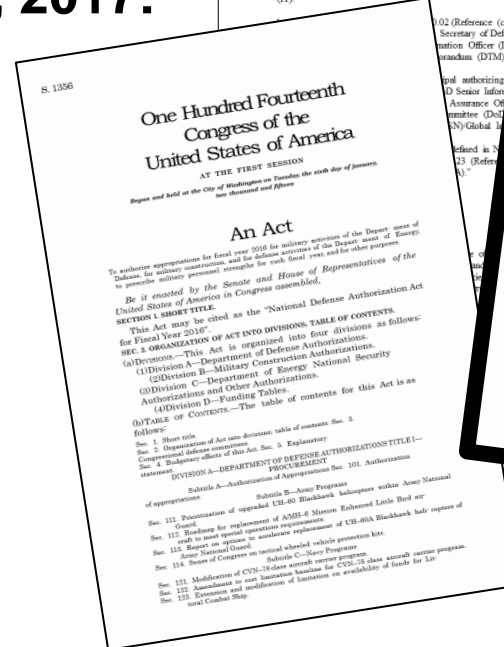
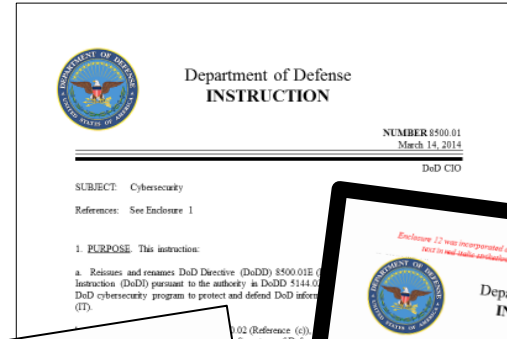
**Authorizing Officials (AOs)
are responsible for their
portfolio(s) timeline**

Your RMF transition plan?



Overview

- Why the Big Deal?
- DODI 8500.01 & 8510.01, Mar 2014
- **DODI 5000.02 dated Feb 2, 2017:**
 - Program Managers
 - T&E Community
 - Service AOs
- Resiliency & NDAA 1647
- Summary





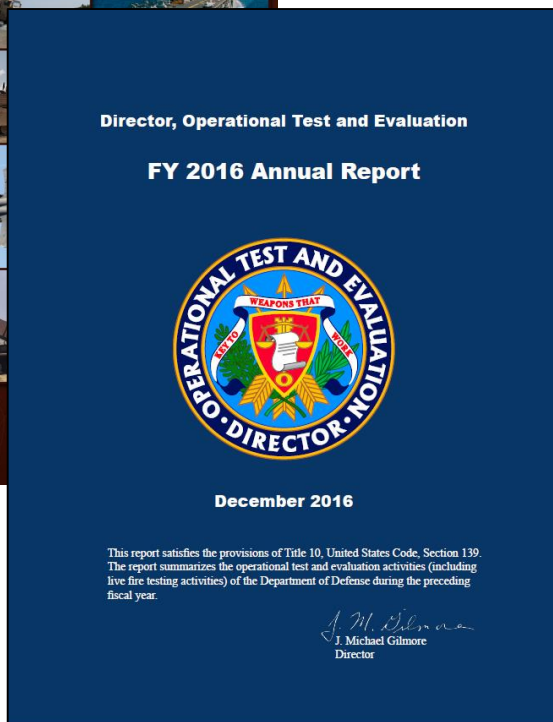
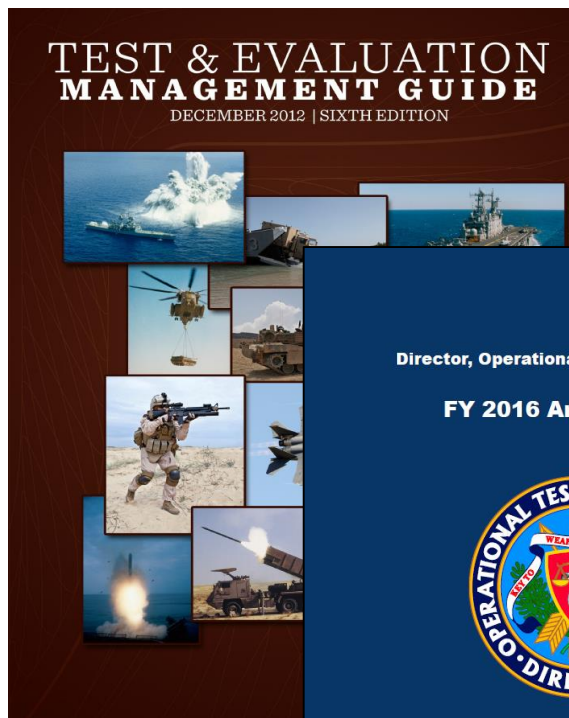
DODI 5000.02: The PM

- **DODI 5000.02**, dated Feb 2, 2017 – contains new **Enclosure 14: Cybersecurity in the Defense Acquisition System**
 - 2. Cybersecurity Risks. “**Program Managers (PM)** pay attention to:
 - a. **Government** Program Organization.
 - b. **Contractor** Organizations. “Poor cybersecurity practices, untrained personnel, undetected malicious insiders,... incorrect classification of information... dissemination... control, and... network security can be used by threat actors...”
 - c. **Software** and **Hardware**.
 - d. System **Interfaces**.
 - e. Enabling and **Support Equipment, Systems, and Facilities**. **Test equipment,... training systems** can be used by threat actors”



Review the Architectures!

Architectures



T&E Management Guide: “In preparation for DT and OT, the test agencies should... **verify the test and security architecture is representative of the operational and system views...** Identify discrepancies between the test architecture and documented [architecture] views.” (p. 254 – 255)

DOT&E FY16 Annual Report:
 “Program offices and operational test agencies **need to place greater emphasis on** the following areas:

- Development and documentation of **complete system architectures**



DODI 5000.02: The PM

- **DODI 5000.02**, dated Feb 2, 2017 – contains a new **Enclosure 14: Cybersecurity in the Defense Acquisition System**
 - 3.b. Design for Cyber Threat Environments. “In order to design, develop, and acquire systems that can operate in applicable cyber threat environments, PMs will...”
 - 1.b. Program Manager (PM) Responsibilities. “PMs... are responsible for the cybersecurity of their programs, systems, and information. This responsibility starts from the earliest exploratory phases of a program ...**through all phases** of the acquisition. Acquisition activities include system **concept trades, design, development, Test & Evaluation (T&E), production, fielding, sustainment and disposal.**”

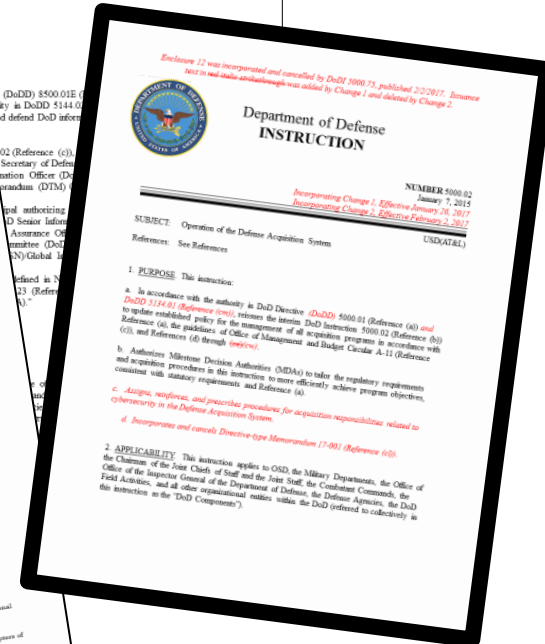
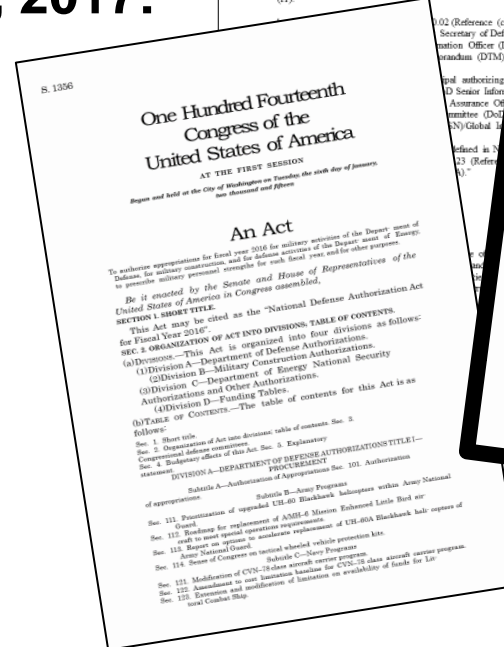
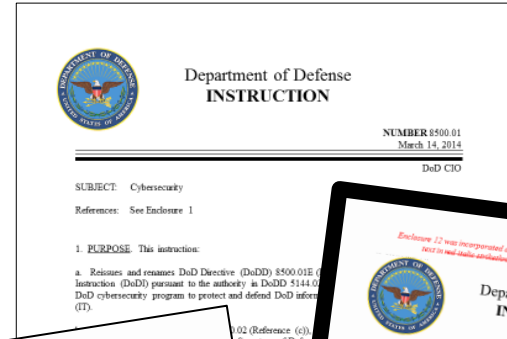


PMs can't do this alone!



Overview

- Why the Big Deal?
- DODI 8500.01 & 8510.01, Mar 2014
- **DODI 5000.02 dated Feb 2, 2017:**
 - Program Manager
 - T&E Community
 - Service AOs
- Resiliency & NDAA 1647
- Summary





DODI 5000.02: T&E Personnel

- DODI 5000.02, dated Feb 2, 2017 – contains Enclosure 14: Cybersecurity in the Defense Acquisition System
 - (2)(b) Identify digitized T&E data that will contribute to assessing progress toward achieving...requirements. The T&E strategy should include explicit cybersecurity requirements, but also all key interfaces. Determine avenues and means by which the system may be exploited for cyber-attack and use this information to design T&E activities and scenarios.”
 - 3.b(2)(c) Collaborate with Authorizing Officials (AOs)... from program inception and throughout the life cycle.”
 - Cyber Table Top (CTT) help available



Use DASD/ DT&E's CTT



DODI 5000.02: T&E Personnel

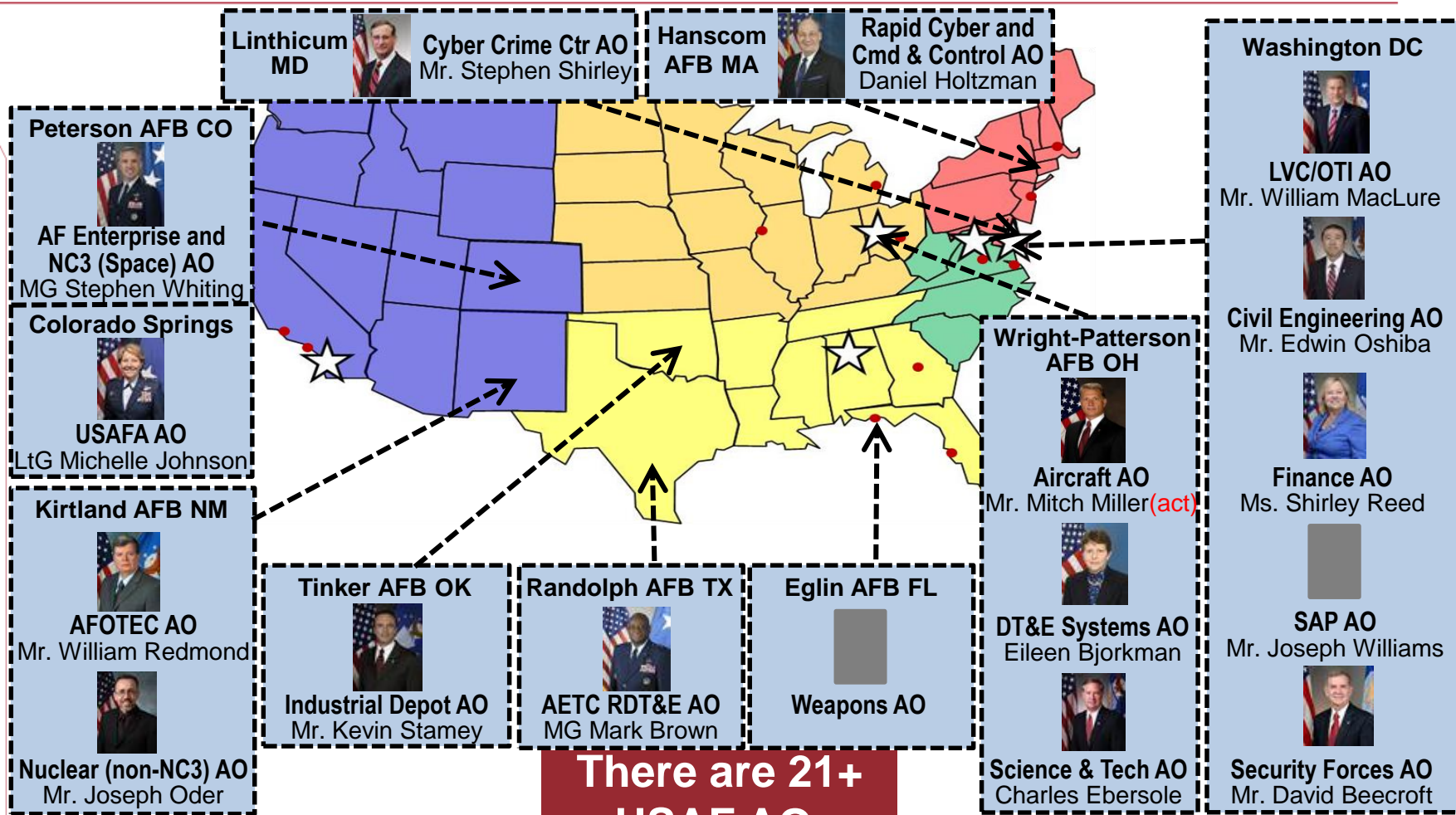
- DODI 5000.02, dated Feb 2, 2017 – contains Enclosure 14: Cybersecurity in the Defense Acquisition System
 - 3.b(13) Plan for cybersecurity T&E in order to identify and eliminate as many cybersecurity shortfalls as early as possible... Beginning early, before Milestone A, work closely with the Chief Developmental Tester as well as the T&E WIPT to plan...and conduct cybersecurity T&E. Cybersecurity T&E spans the entire material life cycle of the program... T&E activities should be planned for and documented in the Test & Evaluation Master Plan
- DODI 8510.01: “The Interim Authorization to Test (IATT)... granted only when operational environment or live data is required [for DT&E] test objectives,...and should expire at the completion of testing.”



AO signs/ approves IATTs



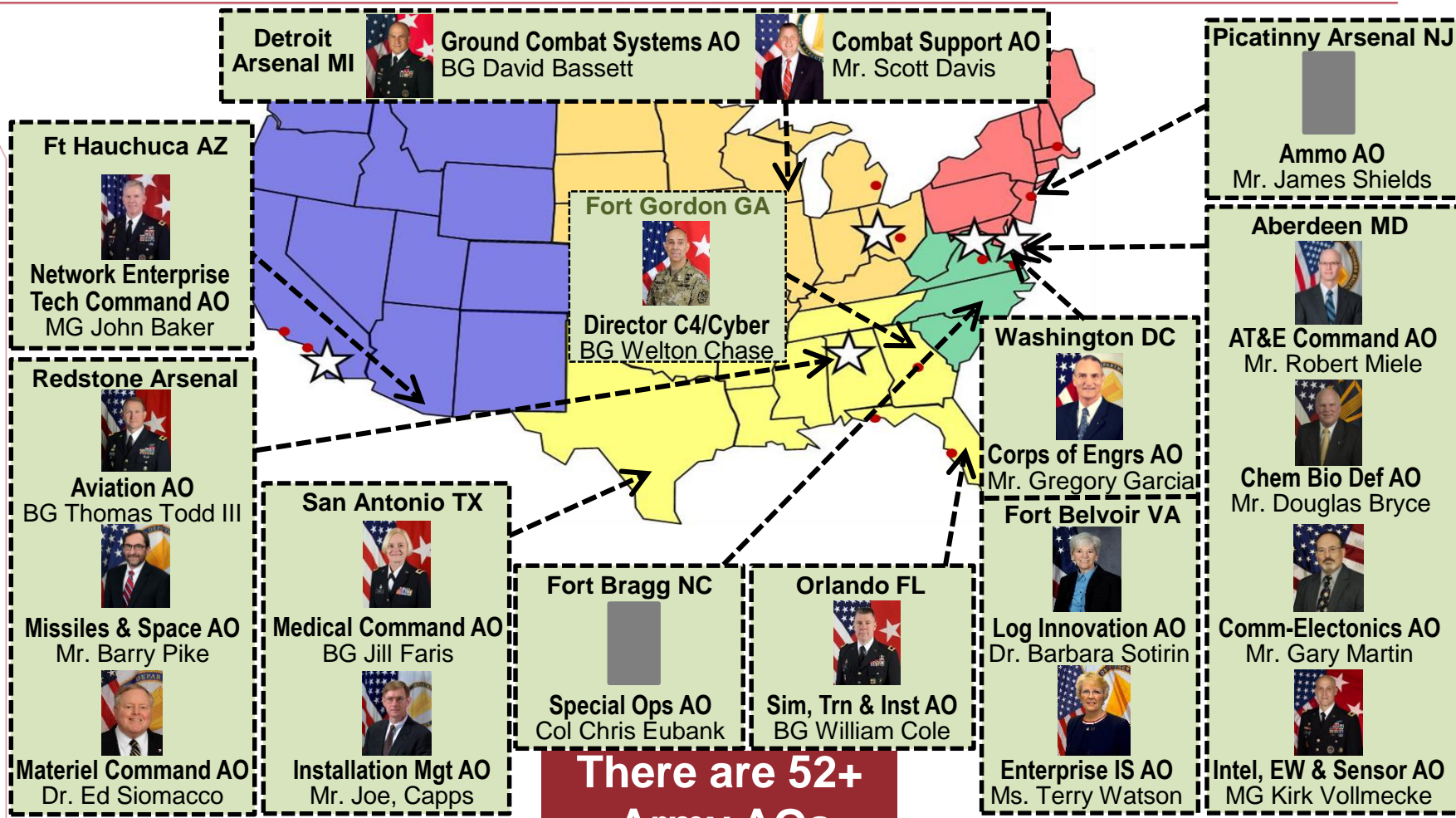
Key Service AOs (USAF)



**There are 21+
USAF AOs**



Key Service AOs (Army)

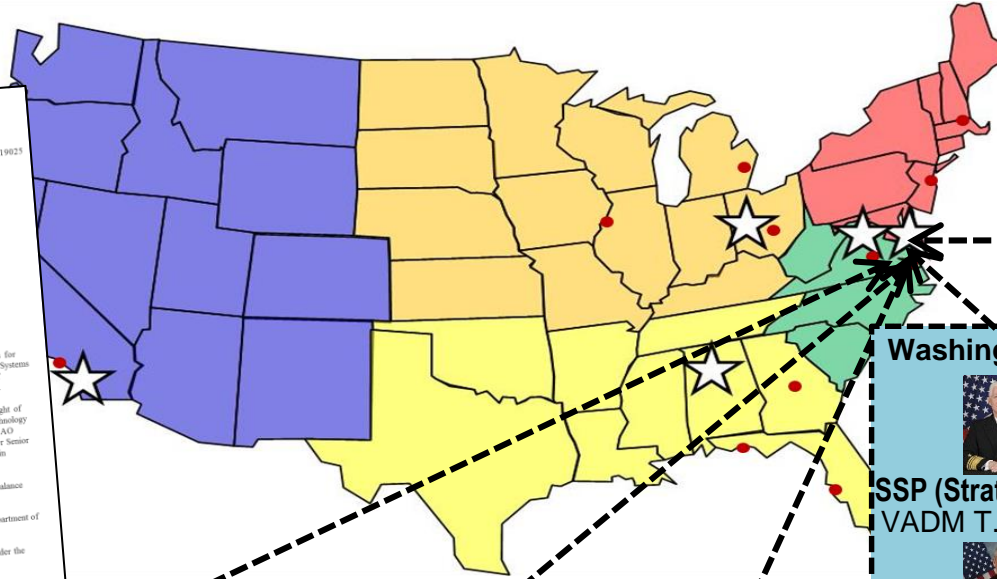
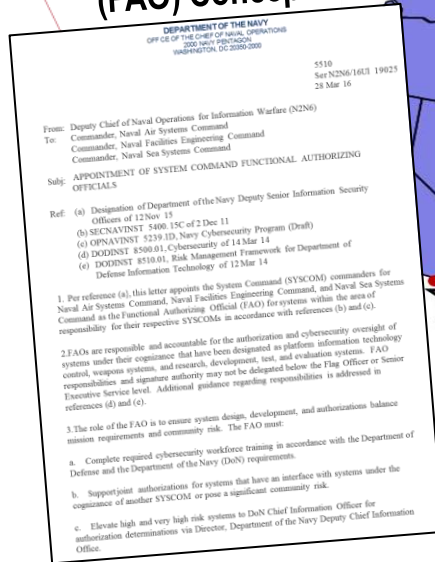


**There are 52+
Army AOs**



Key Service AOs (Navy & USMC)

Navy uses Functional (FAO) Concept



Quantico VA

USMC Systems AO
Dr. Ray Letteer

Norfolk VA

Navy AO (GIG)
Mr. Neal Miller

Patuxent River MD

NAVAIR FAO
VADM P. Grosklags

Washington DC

SSP (Strat Sys) FAO
VADM T. Benedict

NAVSEA FAO
VADM Tom Moore

NAVFAC FAO
RADM Muilenburg

Washington DC

Special Comp Info AO
VADM Jan Tighe

**There is 1 USMC
AO & 6+ Navy**

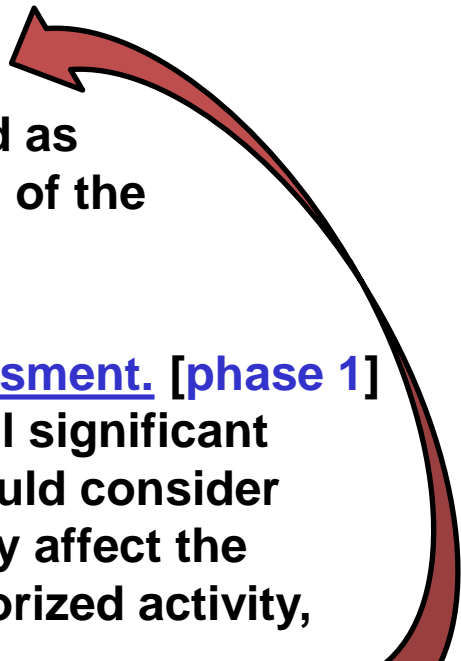


DoDI 5000.02: T&E Personnel

- **DODI 5000.02, dated Feb 2, 2017 – contains Enclosure 14: Cybersecurity in the Defense Acquisition System**
 - 3.b.(13).(a) Developmental Testing (DT&E) [two parts]
 - 3.b.(13).(a).1. “Cooperative Vulnerability Identification. Conduct T&E activities to collect data needed to identify vulnerabilities and plan the means to mitigate or resolve them, including system scans, analysis, and architectural reviews.
 - 3.b.(13).(a).2. Adversarial Cybersecurity DT&E. Conduct using realistic threat exploitation techniques in representative environments and scenarios to exercise critical missions within a cyber-contested environment to identify any vulnerabilities.”



DoDI 5000.02: T&E Personnel

- DODI 5000.02, dated Feb 2, 2017 – contains Enclosure 14: Cybersecurity in the Defense Acquisition System
 - 3.b.(13).(b) “Operational Testing (OT&E). **Two phases** of cybersecurity testing are required as part of OT&E for all systems under the oversight of the Director of Operational Test and Evaluation.
 - Cooperative Vulnerability and Penetration Assessment. [phase 1] An overt examination of the system to identify all significant vulnerabilities and the risk of exploitation... should consider operational implications of vulnerabilities as they affect the capability to protect system data, detect unauthorized activity, react to system compromise, and restore system capabilities.”
- 

AO signs OT&E IATT/ ATO



DoDI 5000.02: T&E Personnel

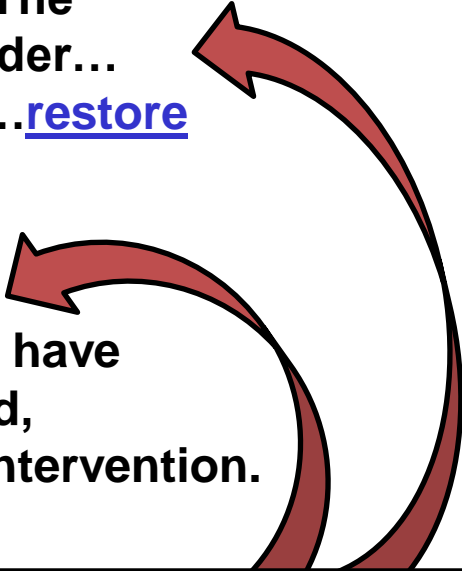
- DODI 5000.02, dated Feb 2, 2017 – contains Enclosure 14: Cybersecurity in the Defense Acquisition System
 - Adversarial Assessment. [OT&E phase 2] Assesses the ability of a unit equipped with a system to support its mission while withstanding cyber threat activity representative of an actual adversary...
The test must evaluate the ability to protect the system and data, detect and threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity.
Test... should [use a] National Security Agency [NSA]-certified adversarial [Red] team to act as a cyber aggressor presenting multiple intrusion vectors consistent with the threat.”



Is Restore part of Cybersecurity?



DoD Policy: “Restore”

- DODI 5000.02, Enclosure 5, Operational T&E: “Beginning at MS B,... measures will be used to evaluate operational capability to protect, detect, react, and restore to sustain continuity of operation.”
 - DODI 5000.02 Enclosure 14, Cybersecurity: “The [OT&E Penetration] assessment should consider... vulnerabilities as they affect the capability to...restore system capabilities.”
 - DODI 8500.01, Policy. Operational Resilience. “Whenever possible, technology components have the ability to reconfigure, optimize, self-defend, and recover [restore] with little or no human intervention.”
- 

Regarding POLICY...

Restore is part of Cybersecurity

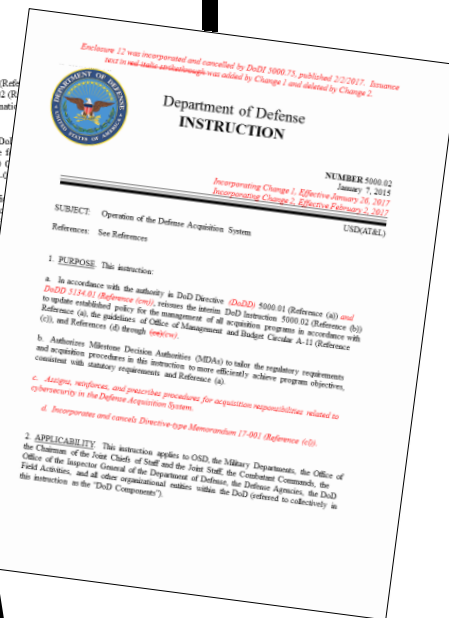
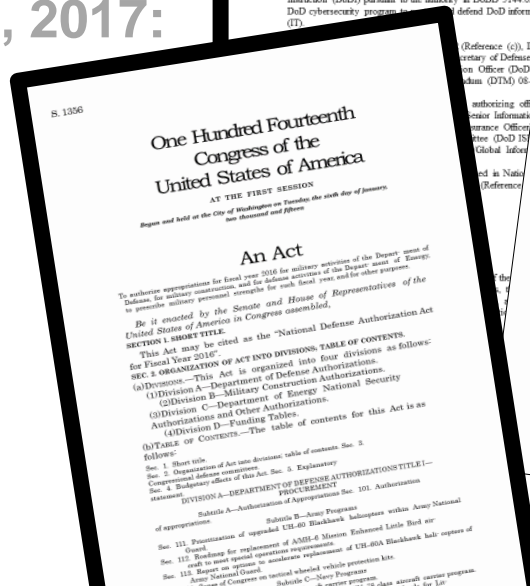
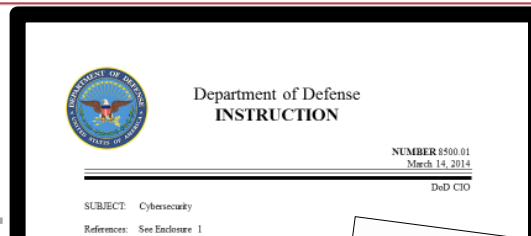


Overview

- Why the Big Deal?
- DODI 8500.01 & 8510.01, Mar 2014
- DODI 5000.02 dated Feb 2, 2017:
 - Program Manager
 - T&E Community
 - Service AOs
- Resiliency & NDAA 1647
- Summary

Regarding TECHNOLOGY...

Restore is not Cybersecurity yet





Operational Resilience



Department of Defense INSTRUCTION

NUMBER 8500.01
March 14, 2014

DoD CIO

SUBJECT: Cybersecurity

References: See Enclosure 1

1. PURPOSE. This instruction:

- a. Reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).
- b. Incorporates and cancels DoDI 8500.02 (Reference (c)), DoDD C-5200.19 (Reference (d)), DoDI 8552.01 (Reference (e)), Assistant Secretary of Defense for Networks and Information Integration (ASD/NII)/DoD Chief Information Officer (DoD CIO) Memorandums (References (f) through (k)), and Directive-type Memorandum (DTM) 08-060 (Reference (l)).
- c. Establishes the positions of DoD principal authorizing official (PAO) (formerly known as principal accrediting authority) and the DoD Senior Information Security Officer (SISO) (formerly known as the Senior Information Assurance Officer) and continues the DoD Information Security Risk Management Committee (DoD ISRMC) (formerly known as the Defense Information Systems Network (DISN) Global Information Grid (GIG) Flag Panel).
- d. Adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (m)) to be used throughout DoD instead of the term "information assurance (IA)".

2. APPLICABILITY

- a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

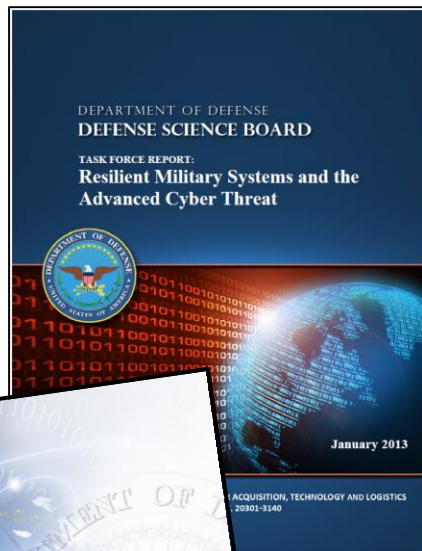
“Operational Resilience?”

- From DODI 8500.01 Glossary: “The ability of systems to resist, absorb, and recover from an adverse [attack] during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.”

Discussions occurred 2016-2017
with the NIST to update Special
Publication (SP) 800-53 (Rev 5),
or another NIST SP, with additional
Security Controls (SCs) for resilience.

More Resilience SCs Nearing

Other Resilience Terms...



Defense Science Board (DSB) Report on Resilient Military Systems and the Advanced Cyber Threat, Jan 13 2013

- “For cyber system resiliency there must be alternative system plans, back-up procedures, and reconfiguration / restart options. Effective resiliency requires that all systems critical to [the] mission be resilient.



Task Force on Cyber Deterrence, Feb 17 2017

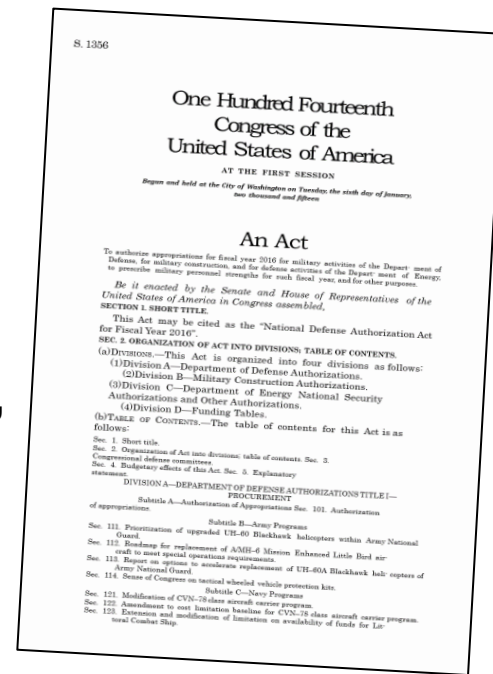
- “Offensive capabilities continue to grow, and [will] outpace cyber defense...and... resilience.”
- Recommendation: “spur and evaluate innovative technologies aimed at [improving] cyber resilience.”

Resilience Ability of a System



FY16 NDAA – Section 1647

- **Section 1647: Evaluation of Cyber Vulnerabilities of Major Weapon Systems**
 - (a) **Evaluation**. “The **SECDEF** shall... complete an evaluation of the cyber vulnerabilities of each **major** weapon system of the DoD NLT December 31, 2019.”
 - (b) **Plan for Evaluation**.
“The plan...shall [prioritize] evaluations based on criticality of major weapon systems, determined by Chairman of the Joint Chiefs of Staff based on threats. The plan... shall not duplicate: Task Force Cyber Awakening [TFCA] of the **Navy**... or Task Force Cyber Secure of the **Air Force**.”





NDAA for FY16 – Section 1647

- **Section 1647: Evaluation of Cyber Vulnerabilities of Major Weapon Systems of the Department of Defense.**
 - (c) Status on Progress. “**SECDEF** shall inform [Congress] of the activities undertaken in the evaluation of major weapon systems under this section as part of the quarterly cyber operations briefings under title 10, United States Code.”
 - (d) Risk Mitigation Strategies. “As part of the evaluation of cyber vulnerabilities of major weapon systems of the Department (DoD) under this section, Secretary of Defense... shall develop strategies for mitigating risks of vulnerabilities.”

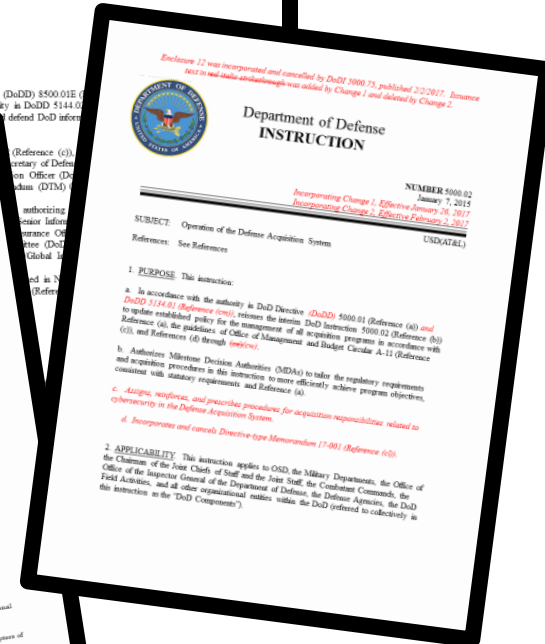
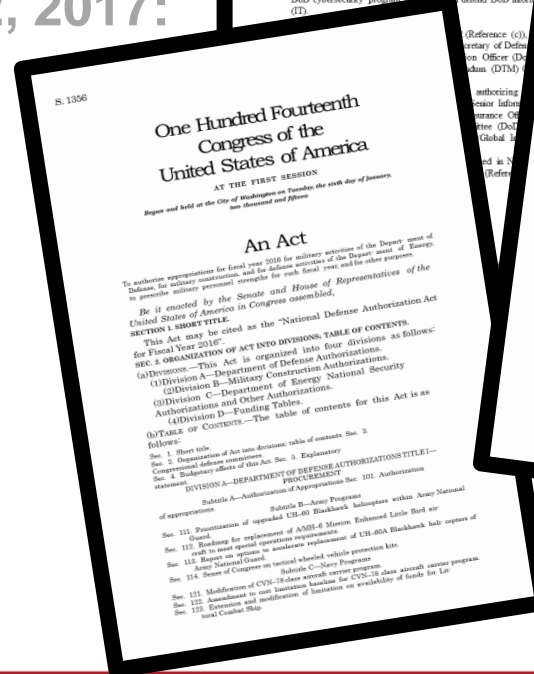
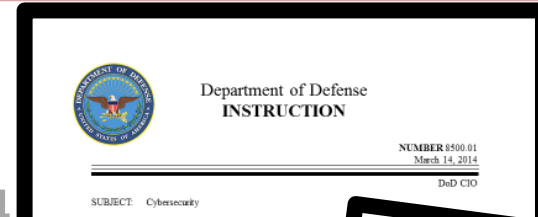


Increased Resilience Ownership



Overview

- Why the Big Deal?
- DODI 8500.01 & 8510.01, Mar 2014
- DODI 5000.02 dated Feb 2, 2017:
 - Program Managers
 - T&E Community
 - Service AOs
- Resiliency & NDAA 1647
- Summary





Summary: DAU Cybersecurity Team

DAU team:

Prior Army

Prior Navy

Prior Air Force

Prior DCMA

Prior Industry

DAU-W at San Diego CA



Derek
Duchain



Chris
Newborn



Paul
Shaw

DAU-S at Huntsville AL... and Eglin AFB FL *



Steve
Mills



Tim
Denman

Learning Dir



Heath
Ferry



Kim
Kendall



Edward
Adkins *

DAU-MW at Kettering OH



Dr. Ken
Beasley

DAU-MA at Pax River MD



Roy
Wilson



Vinny
Lamolinara

Cybersecurity training, workshops and consulting for the DoD



Summary

- Know Cybersecurity is a “big deal” for our National Security
- Use the right terms for discussing/ documenting Cybersecurity
- Be the T&E Cybersecurity expert; help your Program Offices
- Review documentation early for complete system architectures
- Collaborate with the (right) Service Authorizing Official (AO)
- Know Resiliency involves the system and has broad ownership
- DAU Cybersecurity team provides assistance and can help you



Professor Edward A. Adkins
Defense Acquisition University
Engineering, Test & Cybersecurity
Edward.Adkins@dau.mil