Defensive Cyber Operations Testing

Dr. Georgianna "George" Shea

MITRE support to D-DT&E

MITRE

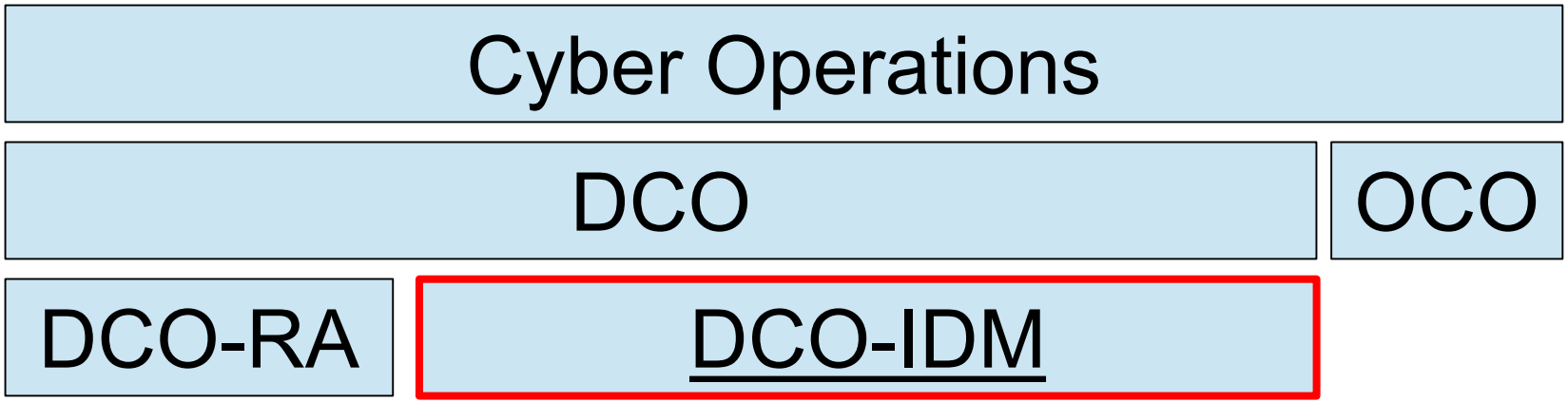
Who do I support? D- DT&E

Roles and Responsibilities

- Policy, Guidance, and Congressional Reporting.
- Major Program Engagement.
- T&E Workforce

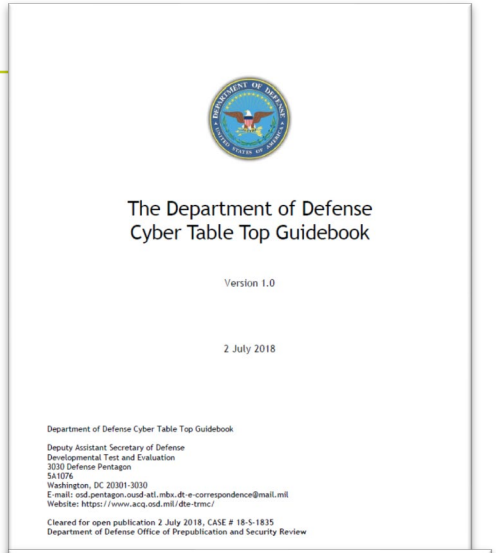
DCO Defined

- **DCO – Defensive Cyber Operations**
- **OCO – Offensive Cyber Operations**
- **DCO- RA – DCO Response Action**
- **DCO-IDM – DCO Internal Defensive Measures**



Cybersecurity T&E Guidance 6 Phases

- **Developmental Testing**
  - Phase 1 Understanding Requirements
  - Phase 2 Characterize the Cyber-Attack Surface
  - Phase 3 Cooperative Vulnerability Identification (CVI)
  - Phase 4 Adversarial Cybersecurity DT&E (ACD)
- **Operational Test**
  - Phase 5 Cooperative Vulnerability and Penetration Assessment (CVPA)
  - Phase 6 Adversarial Assessment (AA)


The Department of Defense
Cyber Table Top Guidebook

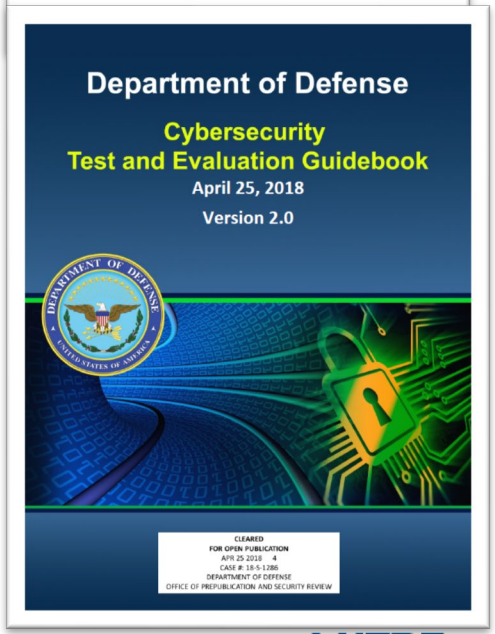
Version 1.0

2 July 2018

Department of Defense Cyber Table Top Guidebook

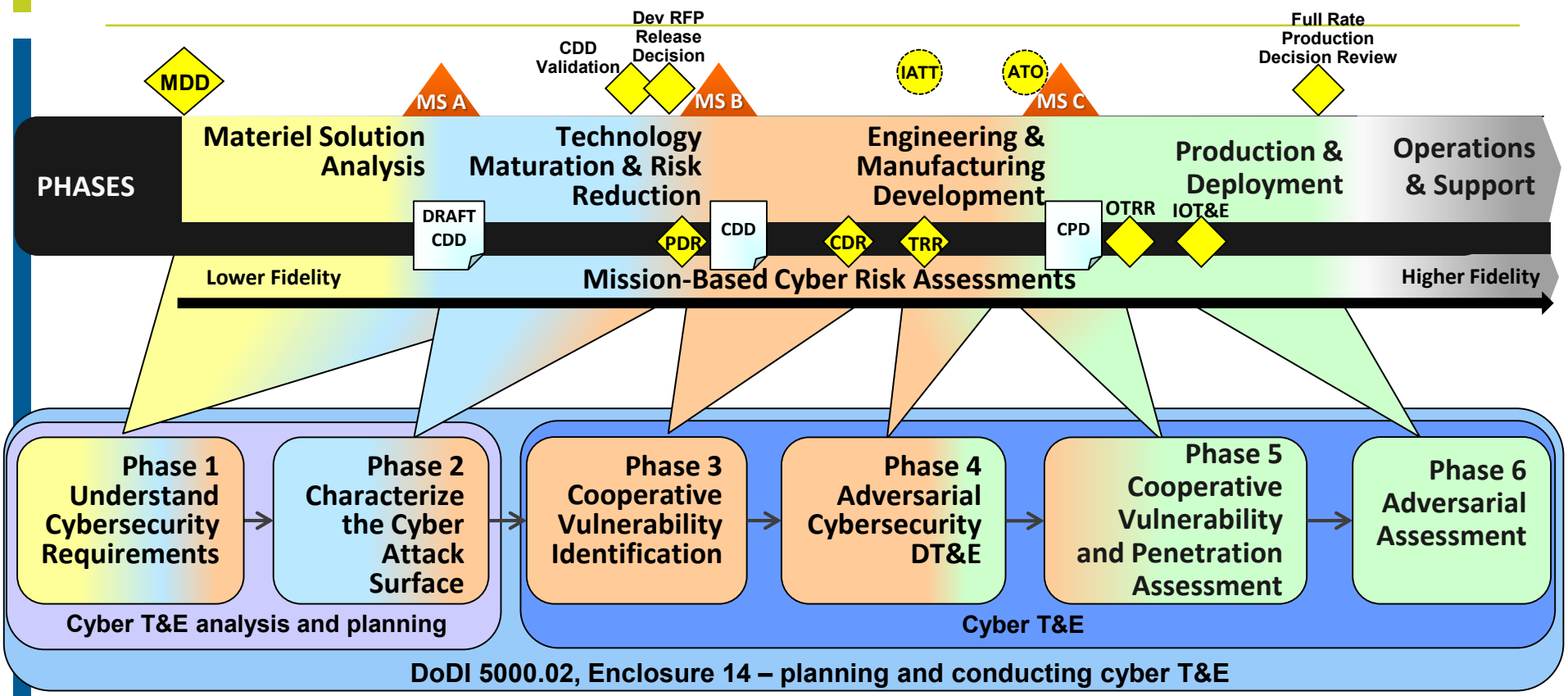
Deputy Assistant Secretary of Defense
Developmental Test and Evaluation
3030 Defense Pentagon
5A1076
Washington, DC 20301-3030
E-mail: osd.pentagon.ousd-atl.mbx.dt-e-correspondence@mail.mil
Website: https://www.acq.osd.mil/dte-trmc/

Cleared for open publication 2 July 2018, CASE # 18-S-1835
Department of Defense Office of Prepublication and Security Review



MITRE

Cybersecurity T&E Process



- **Cybersecurity T&E is necessary and required by policy**
  - Evaluates a system's mission performance in the presence of cyber threats
  - Informs acquisition decision makers regarding cybersecurity, resilience and survivability

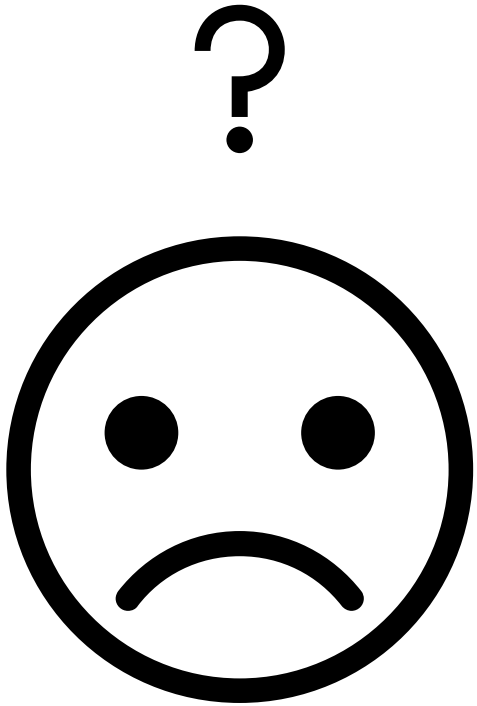
DODI 8500.01 Cybersecurity

DODI 8530.01 Cybersecurity Activities Support to DoD Information Network Operations

Phase 1
Understanding Requirements

Example of program cybersecurity requirements:

- Make it cyber secure
- Meet RMF

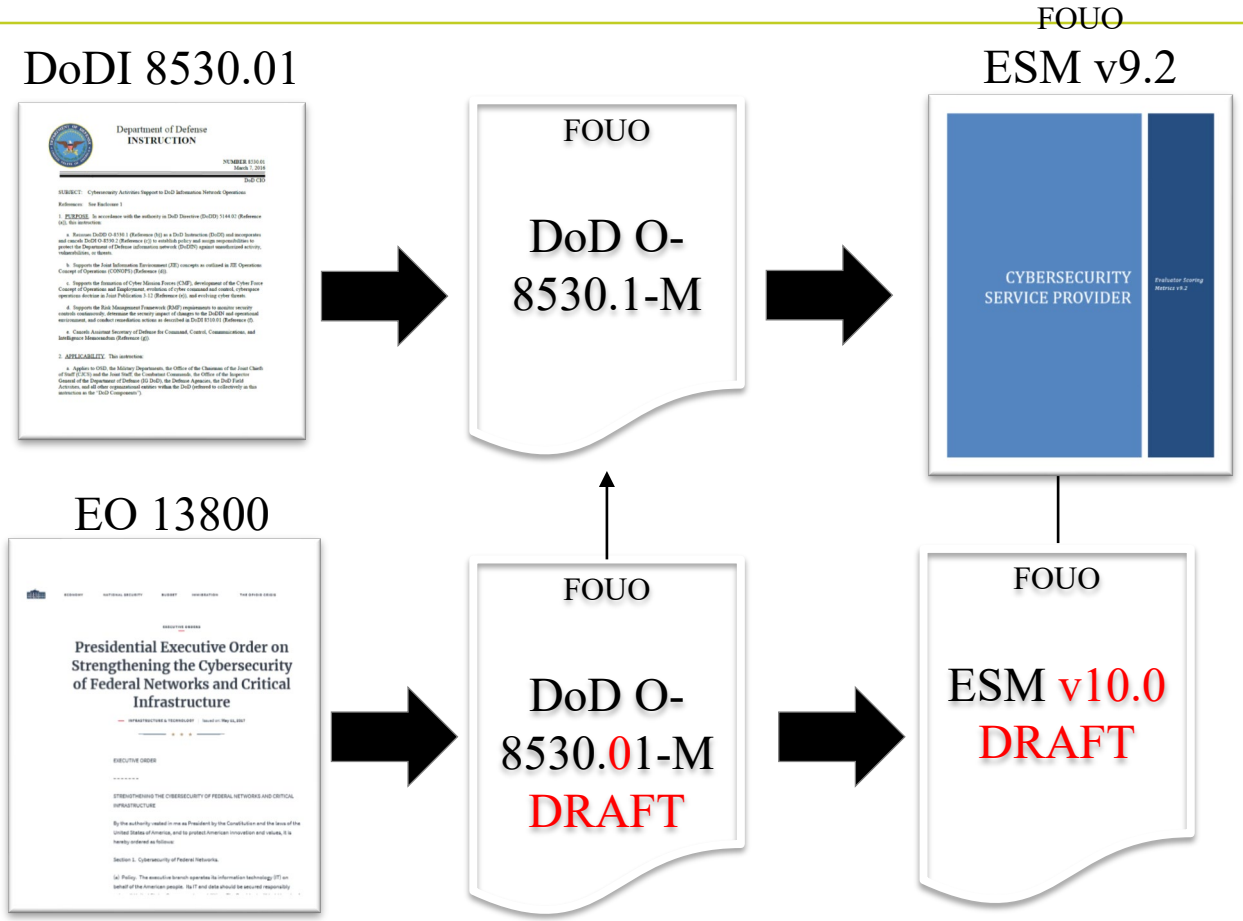


Actual Requirements

- **DODI 8500.01 Cybersecurity, March 2014**
  - 3(d) "Cyberspace Defense. Cyberspace defense will be employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on DoD information networks.

- **DODI 8530.01 Cybersecurity Activities Support to DoD Information Network Operations (DODIN) March 2016:**
  - DCO Internal Defensive Measures

DoD DCO Requirements:

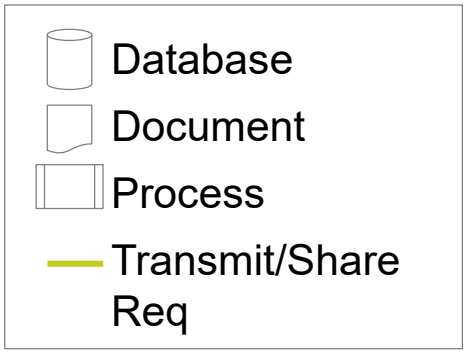


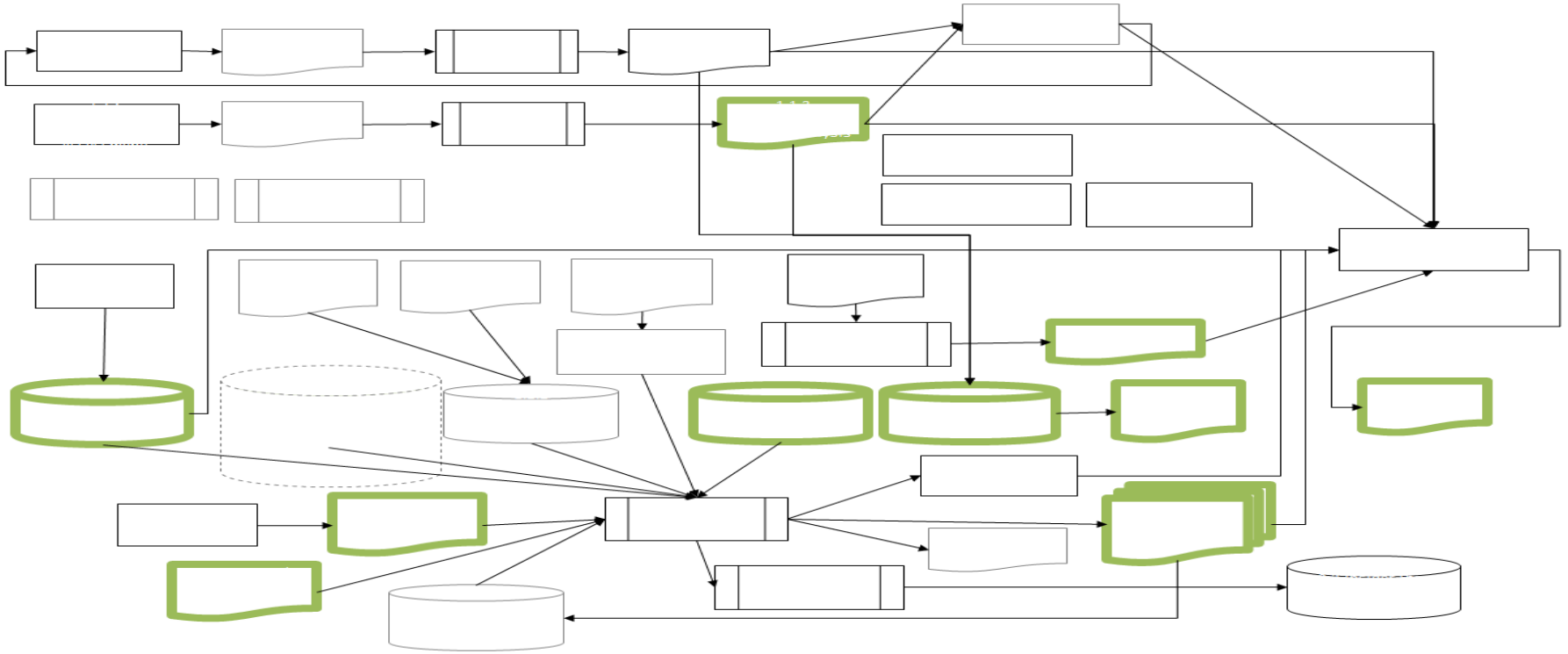
Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Follow the CSF)

MITRE

ESM Required Services

- **Implied system requirements**
  - Data repositories
  - Data/Information sharing capabilities
  - Data/Information correlation capabilities





RMF Relationship

Allocating Responsibilities- Provisioning Cybersecurity Services

Model	Description
Organic	All services self-provisioned
Single External Provider	Services leveraged from an existing, certified provider
Multiple External Providers	Services leveraged from multiple existing, certified providers
Hybrid Mix (Organic & External Provider)	Some services self-provisioned and other services leveraged from an existing, certified provider.

Identify areas of responsibility to include inherited controls to SCA

DODI 8510.01 RMF

Step 1: Categorize	
Step 2: Select Controls	**DODI 8510.01 -** "…address security controls that may be satisfied through inheritance"
Step 3: Implement Controls	
Step 4: Assess Controls	DODI 8510.01 inherited security controls, maintained by the providing system
Step 5: Authorize System	**DODI 8510.01 "…**identify all common controls inherited"
Step 6: Monitor	**DODI 8530.01** Supports the Step 6 of RMF

Sample of Inherited Controls from CSSP

ID	Confidentiality			Integrity			Availability			DCO Common Controls
	L	M	H	L	M	H	L	M	H	
AC-21		x	x							x
AT-2	x	x	x	x	x	x	x	x	x	x
AU-6	x	x	x	x	x	x				x
CA-1	x	x	x	x	x	x	x	x	x	x
CA-2	x	x	x	x	x	x	x	x	x	x
CA-7	x	x	x	x	x	x	x	x	x	x
CA-8						x				x

Determine responsibility of controls (organic or external)

NIST 800-137 Approach Information Systems Continuous Monitoring

DCO Monitoring capability in support of RMF step 6: Continuous Monitoring

Phase 1: Understand DCO Requirements

- Will the system provide a DCO capability or will a provider?
- Is the system designed to enable continuous monitoring (NIST SP 800-137)?
- Do the system requirements account for DCO tools and architectural requirements?

Phase 2
Characterize the Cyber-Attack Surface

Assess Planned Execution

- **People**
  - Experience
  - Offensive cyber mindset
  - Mission understanding
  - Analytical capability
- **Process**
  - Situational Awareness
  - Data Consolidation
  - Effective organizational relationships
  - Repeatable
- **Technology**
  - Tools
  - Automation

Have you established workforce requirements?

Evaluate manning plans and the ability to PMR, across the system.

Have you established process enabling requirements?

Evaluate processes to PMT across the system.

Have you implemented enabling technologies?

Test the technologies ability to PMR across the system.

PPT = People Processes, Technologies

PMR = Prevent, Mitigate, Recover

Assess DCO Capabilities

- **Prevent:**
  - The ability to protect critical mission functions from cyber threats.

Have you established prevention capabilities?

Evaluate how PPT enable prevention across the system

- **Mitigate:**
  - The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.

Have you established mitigation capabilities?

Evaluate how PPT enable mitigation across the system

- **Recover:**
  - The resilience to recover from cyber-attacks and prepare mission systems for the next fight.

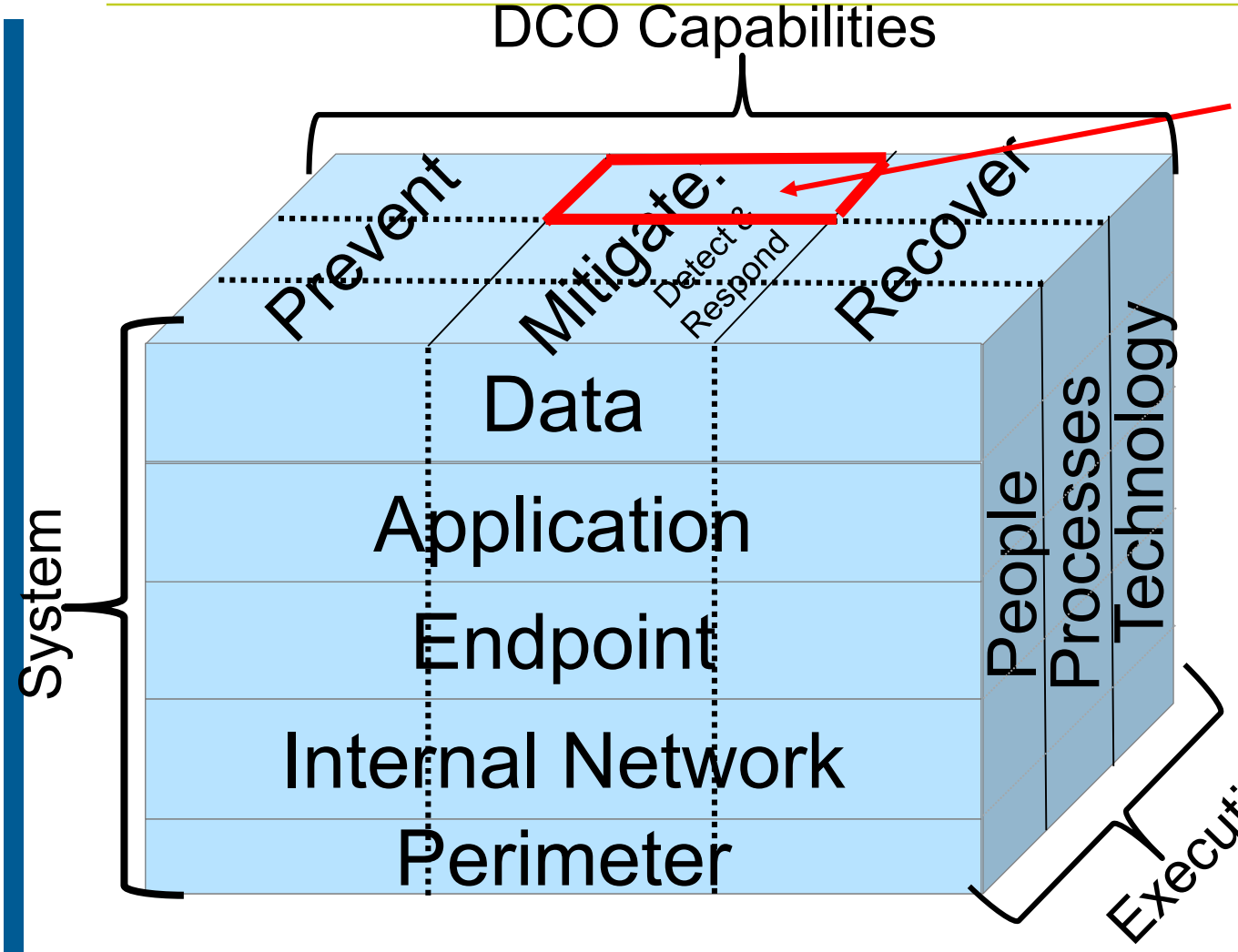
Have you established recover capabilities?

Evaluate how PPT enable recovery across the system.

PPT = People Processes, Technologies

PMR = Prevent, Mitigate, Recover

Do you have a blind spot?



Testable capabilities during development.

Test:

- Measures of effectiveness
- Measures of performance

Will the (people, process and technologies) effectively (Prevent, Mitigate, and Recover) cyber attacks throughout the system?

Example of Data/Detect/Technologies capabilities across the system to test:

	Perimeter	Internal Network	Endpoint	Application	Data
Cyber Kill Chain: Recon	NIDS, SEIM, firewall, Honeynet…	NIDS, SEIM, firewall, Honeynet…	HIDS, SEIM, host agents, Honeypot, …	HIDS, SEIM, Application log auditing, Honey file….	HIDS, SEIM, log auditing, Honey token/Honeyfile….
Delivery					
Exploitation					
Installation					
C2					
Actions on Objectives					

Measures of Effectiveness:

How many intrusions were detected?

Measures of Performance:

What sensors are in place?

Phase 2: Attack Surface

- Will activity be detected?
- Does the monitoring capability make the system more vulnerable?
- Has the Incident Response Plan been analyzed/tested? (CTT)

Is there a Defense-In-Depth Strategy being implemented?

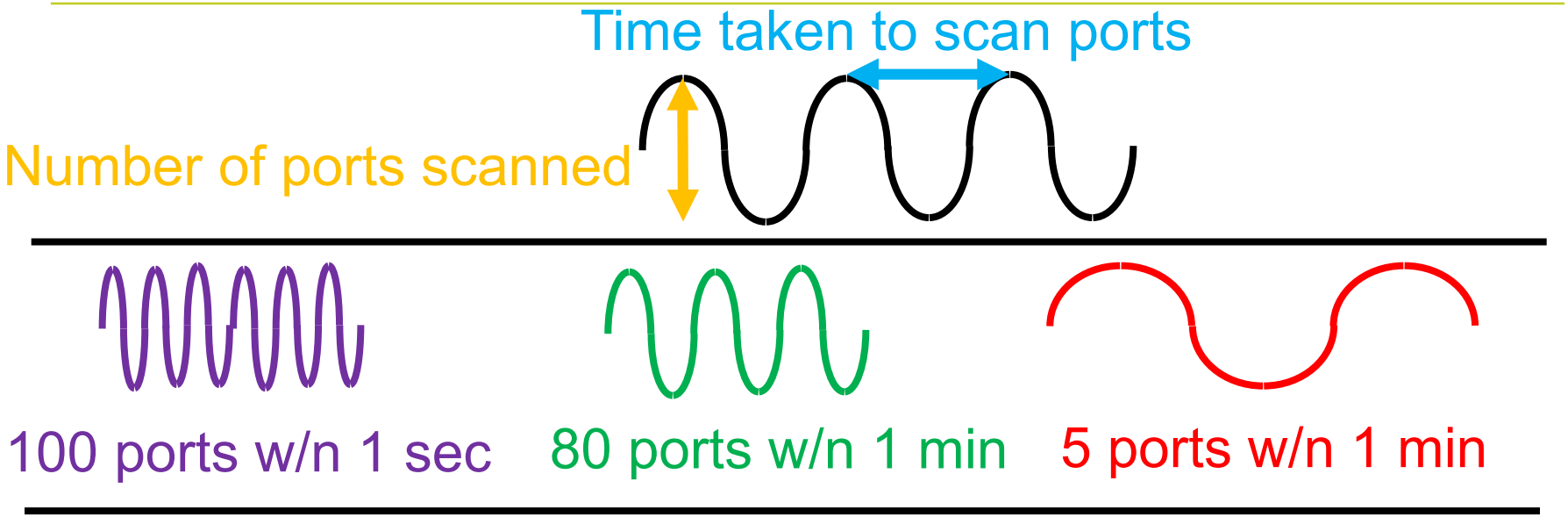
Phase 3
Cooperative Vulnerability Identification (CVI)

Testing DCO Capabilities

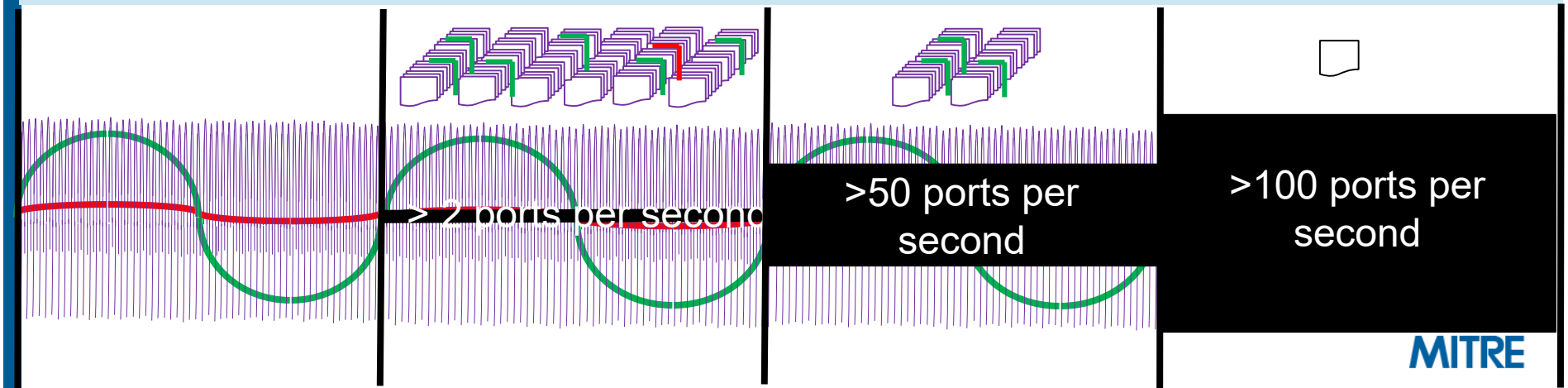
- Phase 3 CVI - verify cybersecurity and resilience requirements, identify vulnerabilities and needed mitigations
  - Cooperative aspects include:
    - Tuning Sensors
    - Baselining
    - Understanding adversary battle plan and mission effects (SOP development for response procedures)

ESM - Evaluator's Scoring Metrics
NIST - National Institute of Standards and Technology
ISO/IEC - International Organization for Standardization/International Electrotechnical Commission

Example of "Tuning" a sensor



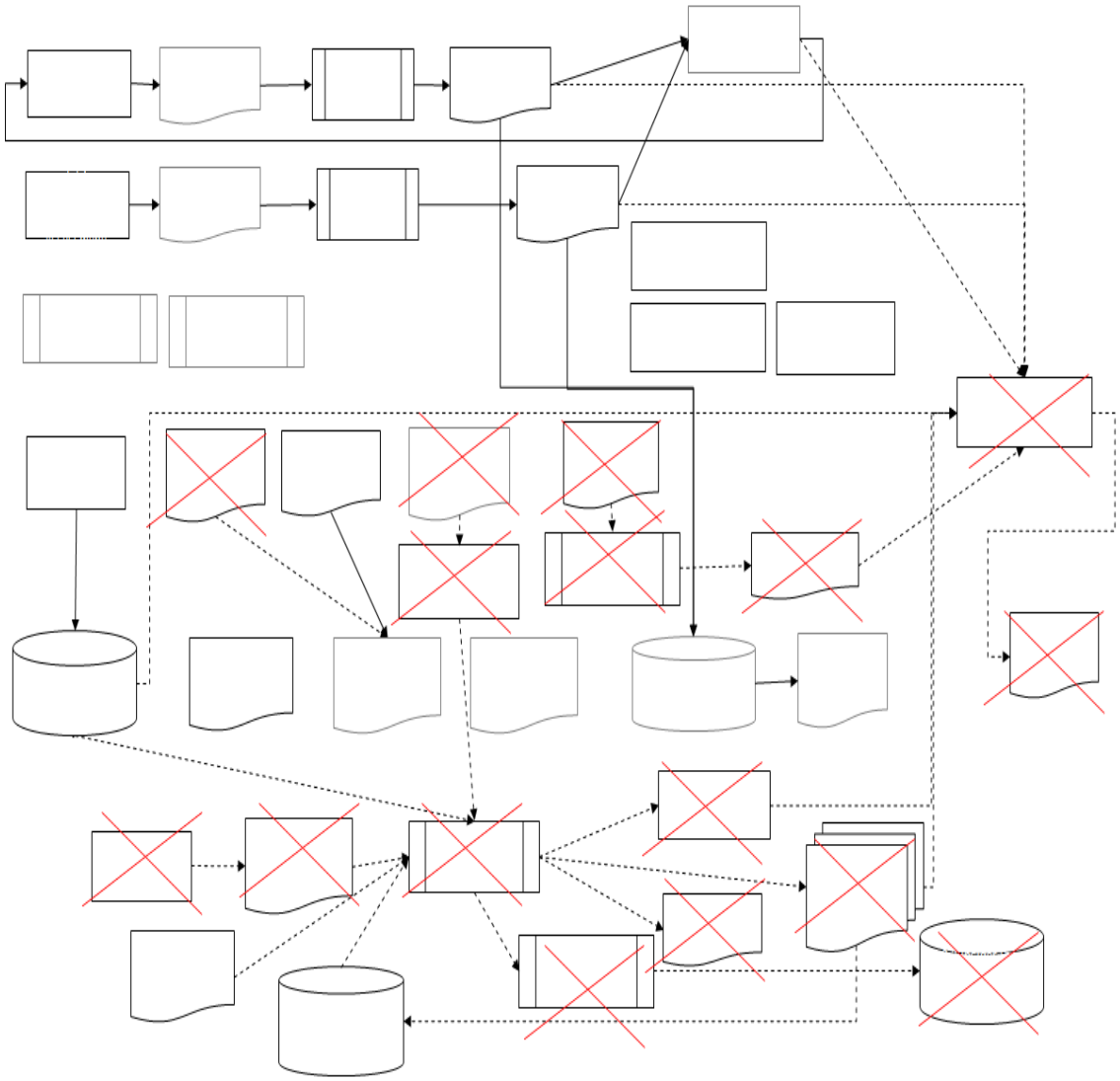
Thresholds determine the amount of traffic seen.



Example of Baselining

- Identify what is normal
  - Is it normal for employee to print at a rate of 10xs more than others?
  - What IPS are expected to be seen within your network?
  - Do system administrative duties line up with identified privilege escalation?
- How to baseline
  - Identify what is continually being flagged by sensors and find out why.
  - Tune sensors
  - Identify and record recognized operational events

ESM Assessment ML1 Example

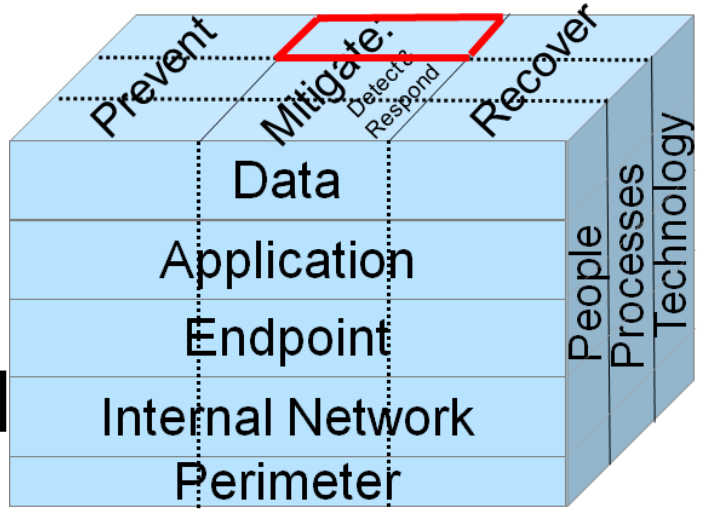


	2017	2018	2019
1.1.1			
1.1.2			
1.1.3			
1.2.1			
1.2.2			
1.2.3			
1.2.4			
1.2.5			
1.3.1			
1.3.2			
1.3.3			
1.4.1			
2.1.1			
2.1.2			
2.1.3			
2.1.4			
2.1.5			
2.2.1			
2.2.2			
2.3.1			
2.3.2			
2.3.3			
2.4.1			
2.4.2			
2.4.3			
3.1.1			
3.1.2			
3.1.3			
3.1.4			

Phase 4
Adversarial Cybersecurity DT&E (ACD)

DCO Test and Evaluation

- Phase 4 ACD - tests the system's cybersecurity and resilience using a mission context in a cyber-contested operating environment.



- Test:
  - Prevent, Mitigate, Recover capabilities
  - People, Processes, Technologies
  - Throughout the entire system

Questions?

Contact Information:

Dr. Georgianna Shea

gshea@mitre.org

MITRE