DoD Cybersecurity Test & Evaluation: Where We Were, Where We Are & Where We Are Going!

Prepared for 2014 NDIA T&E Conference
Mr. Pete Christensen
pchris@mitre.org
703-983-2516

With support from
Ms. Jean Petty
jpetty@mitre.org
703-983-9269
Special Thanks to
DASD DT&E and OSD DOT&E

22 July 2014

1300-1400

Some portions previously Approved for Public Release; Distribution Unlimited. 14-1912

MITRE

What, Why and How?

- **What do we want to accomplish?**
  - Provide an overview of DOD Cybersecurity T&E Activities
- **Why is this important?**
  - Existing processes have been ineffective!
  - Cybersecurity T&E, Systems Security Engineering (SSE), and RMF processes must be aligned and mutually supportive
  - DT&E should provide feedback as early as possible!
  - OT&E outcomes will be better!
- **How will we do it?**
  - Overview DOD Cybersecurity T&E Phases
  - Overview TRMC and National Cyber Range
  - Discuss Cyber Evaluation Framework
  - Walk through a simple example and have fun!

Cybersecurity WORDLE

Cyber Threats WORDLE

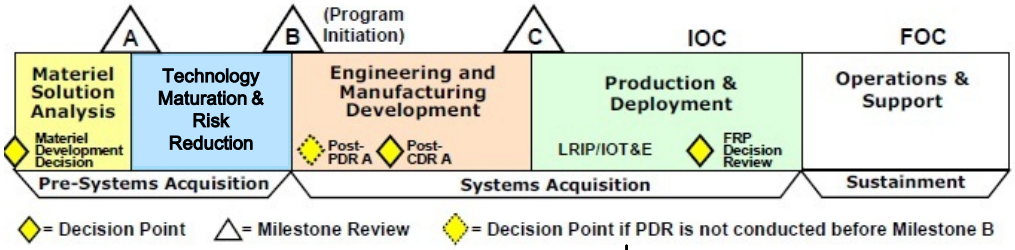
Defense Acquisition WORDLE

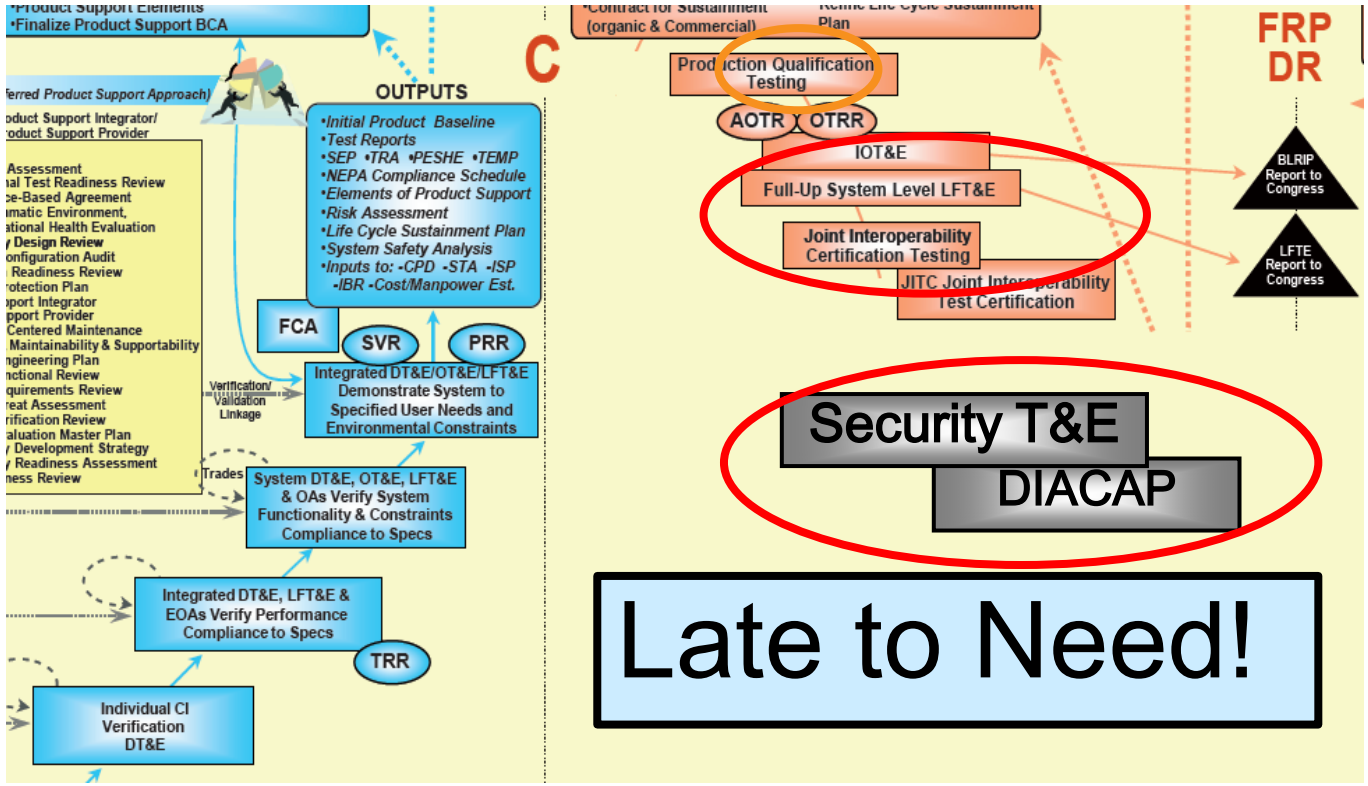

Cyber Goths

Graphic Source: WIKIMEDIA Commons

MITRE

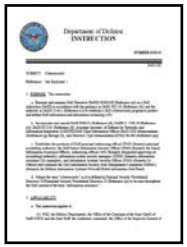
(Former) DASD (DT&E) Principal Deputy
Dr. Steve Hutchison: Interoperability, Security T&E

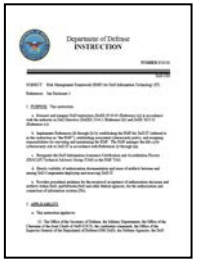




Where We Are Now: Ongoing Policy and Guidance Activities

- **Interim DoDI 5000.02: Issued 26 Nov 2013**
  - New/better guidance for both developmental and operational testing of IT
- **DoD 8500.01, Cybersecurity: Issued 14 Mar 2014**
  - "Cybersecurity" adopted for DoD: replaced "information assurance"
  - Policy: Risk Management, Resilience, Integration and Interoperability…
  - Applied early, integrated across lifecycle
- **DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: Issued 14 Mar 2014**
  - Implements RMF (replaced DIACAP)
  - Policy, Responsibilities, Visibility, Reciprocity
- **Cybersecurity T&E Process**
  - DASD DT&E internal guidelines developed until DAG promulgated
  - DASD DT&E and OSD DOT&E are collaborating
- **Defense Acquisition Guidebook Chapter 9**
  - DASD SE, DT&E and OSD DOT&E are collaborating
- **Cybersecurity Implementation Guidebook for PMs**
  - Will address Cybersecurity T&E
- **Cybersecurity T&E Guidebook**
  - Work in progress to provide more detailed Cybersecurity T&E guidance


Department of Defense
INSTRUCTION


Department of Defense
INSTRUCTION

Following DoDI 8500 series

MITRE

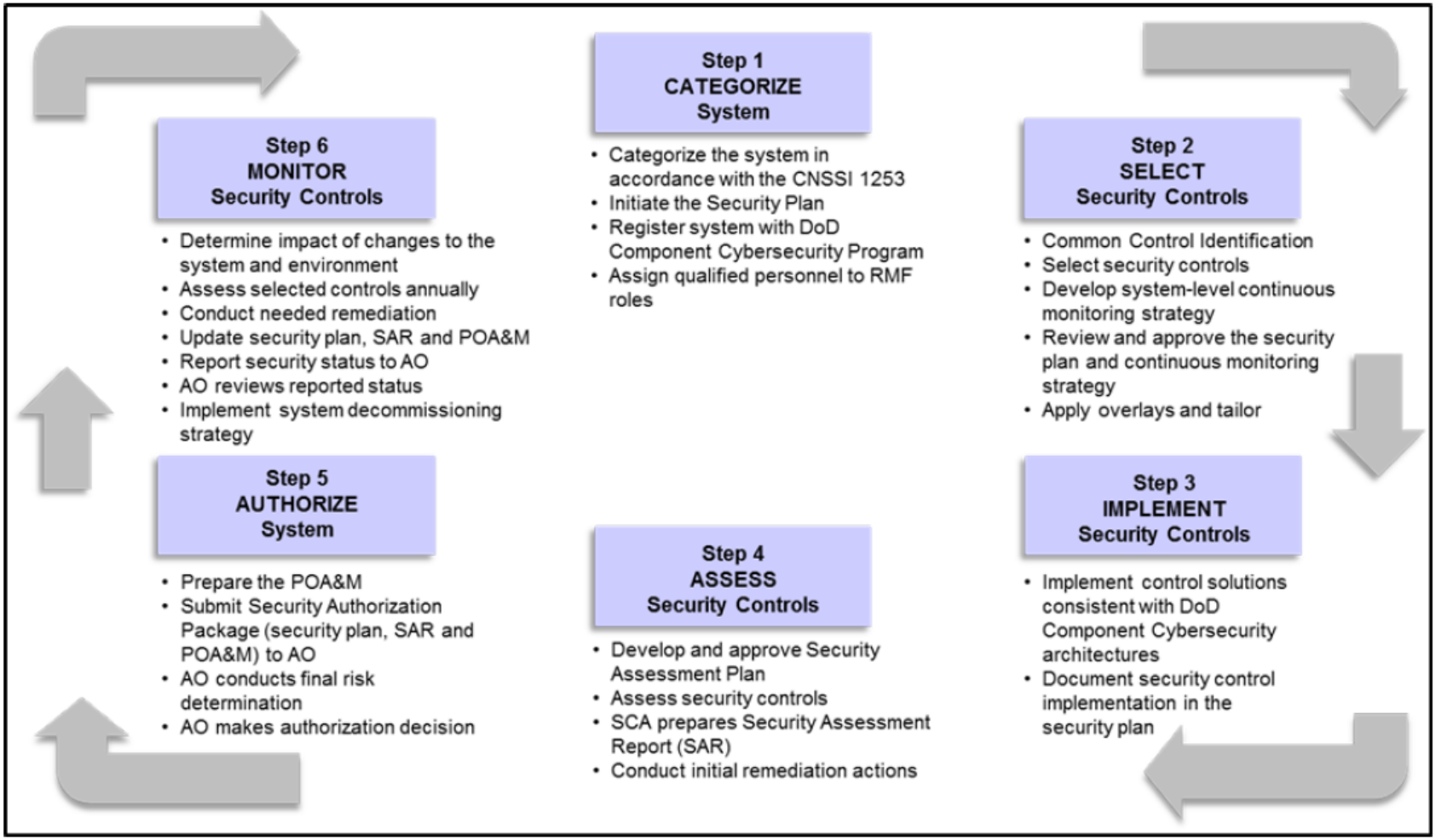
Cybersecurity
Important New Revisions to DoD 8500

- **Adopts the term: "Cybersecurity"**
- **Implements Risk Management Framework (RMF)**
  - New guidance from the National Institute of Standards and Technology (NIST) and Committee on National Security Systems Instruction (CNSSI) documents on cybersecurity
  - Mission Assurance Category/Confidentiality Level (MAC/CL) replaced with Cybersecurity Attributes (confidentiality, integrity, and availability) and impact levels (high, moderate, low)
- **Other terminology changes**
  - Certifying Authority => Security Control Assessor
  - Certification and Accreditation => Assessment and Authorization
  - Designated Approving Authority (DAA) => Authorizing Official (AO)

Coordinating Security Controls Assessments and T&E can make Cybersecurity A&A more efficient!

MITRE

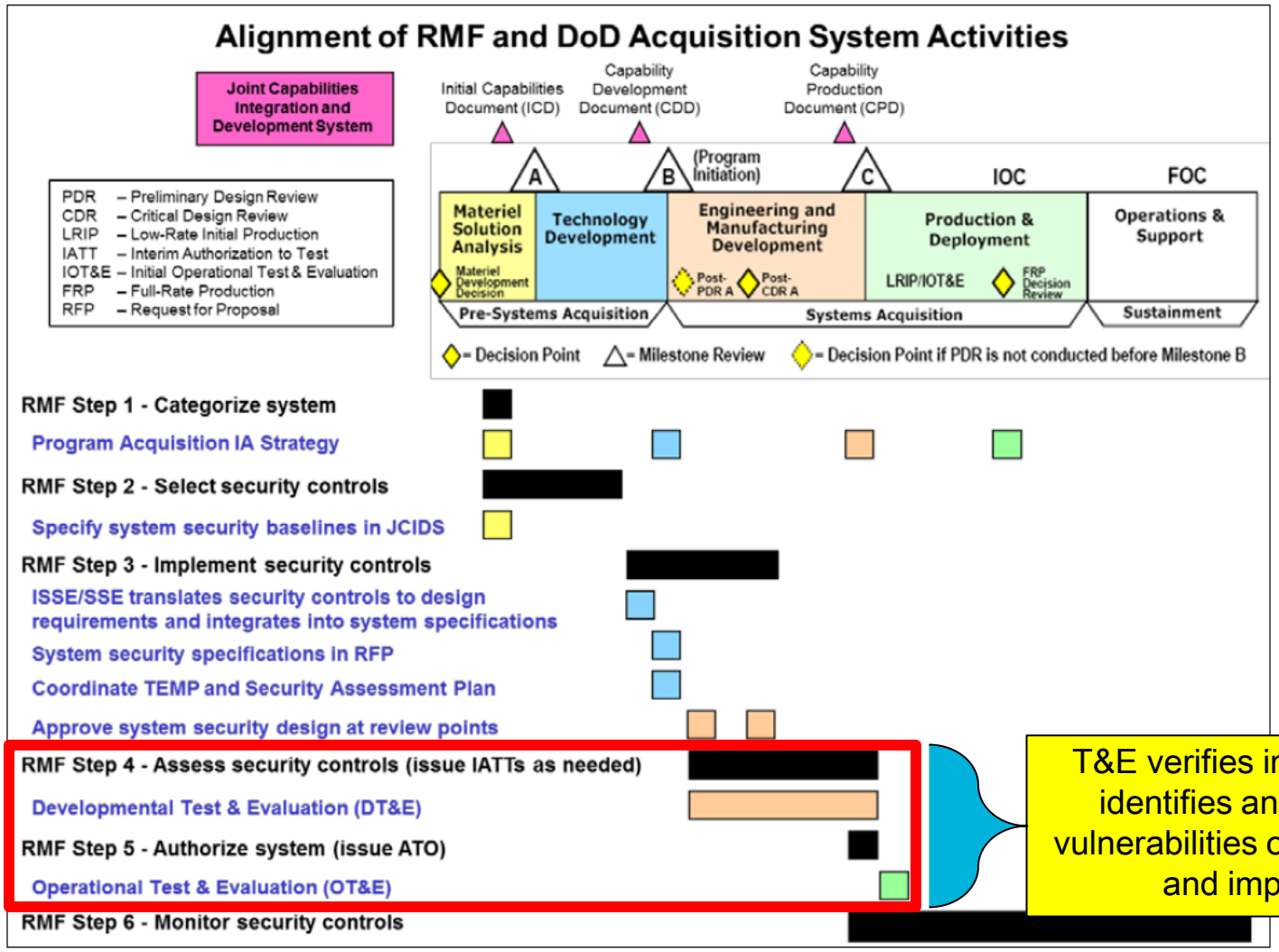
Risk Management Framework (RMF) for Information Systems and Platform Information Technology (PIT) Systems



Graphics Source: DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: Issued 14 Mar 2014

MITRE

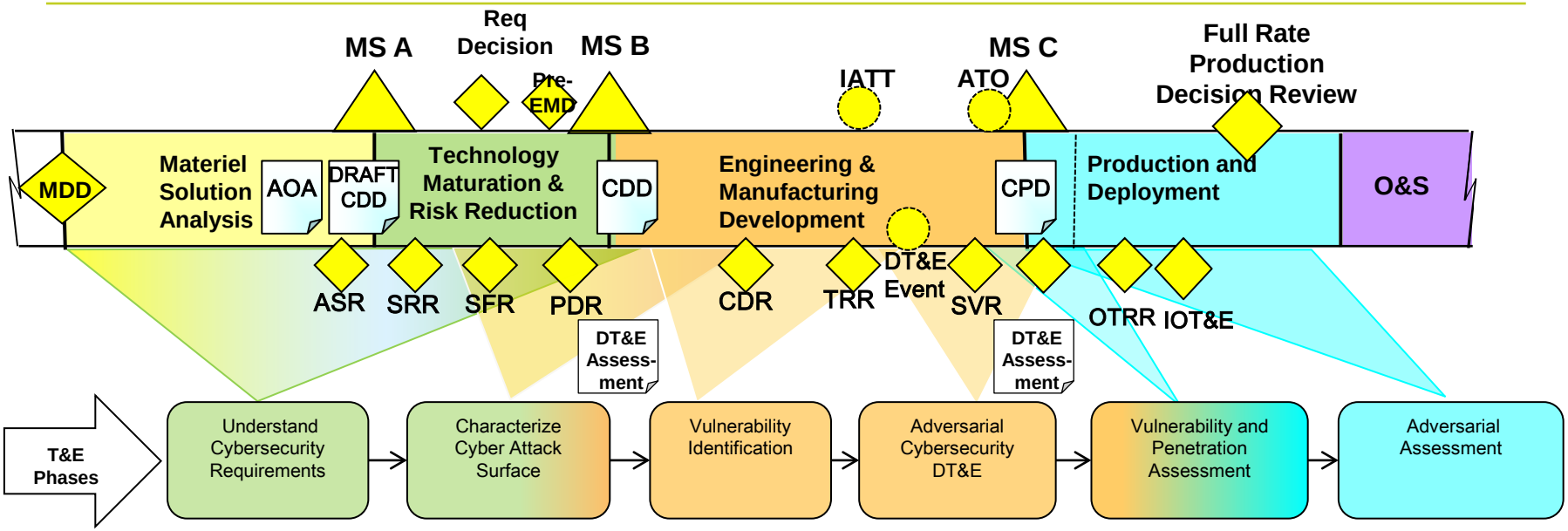
RMF Steps 4 and 5 Necessary But Not Sufficient To Understand Systems Real Cybersecurity Posture!



Graphics Source: DoDI 8510.01 – Risk Management Framework (RMF) for DoD IT: Issued 14 Mar 2014

MITRE

Cybersecurity T&E Phases

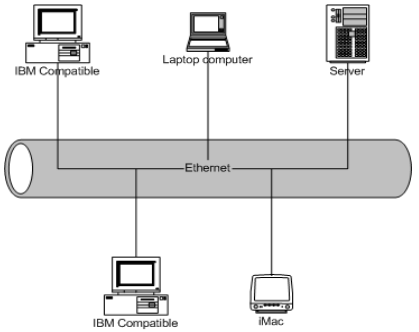


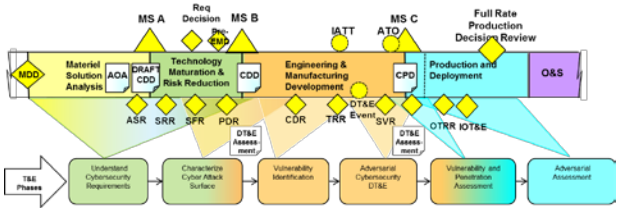
- Phases as depicted are notionally mapped to milestones and design reviews
- Phases are incremental and iterative as system matures
- *Phases 3/5 DT&E and 4/6 OT&E analogous with different objectives!*
  - DT&E S*hifts "vulnerability discovery" earlier in acquisition life cycle to help PM achieve acquisition goals!*

Cybersecurity T&E Complements SSE and RMF to Positively Impact Cost Schedule and Performance!

- **Cybersecurity T&E should be "Multi Purposed"**
  - Collaborative activity involving all "responsible" stakeholders
  - Started as early as possible in Acquisition
  - Verify requirements and baseline capabilities
  - Evaluate exposed "Attack Surface"
  - Identify and help close exposed vulnerabilities
  - Evaluate system resilience in operational context
  - Provide early feedback to "responsible" stakeholders
  - Reduce Cost, improve schedule and inform LRIP
  - Improve OT&E Outcomes

Graphic Source: WIKIPEDIA Commons





MITRE

Phase 1 - Understand Cybersecurity Requirements

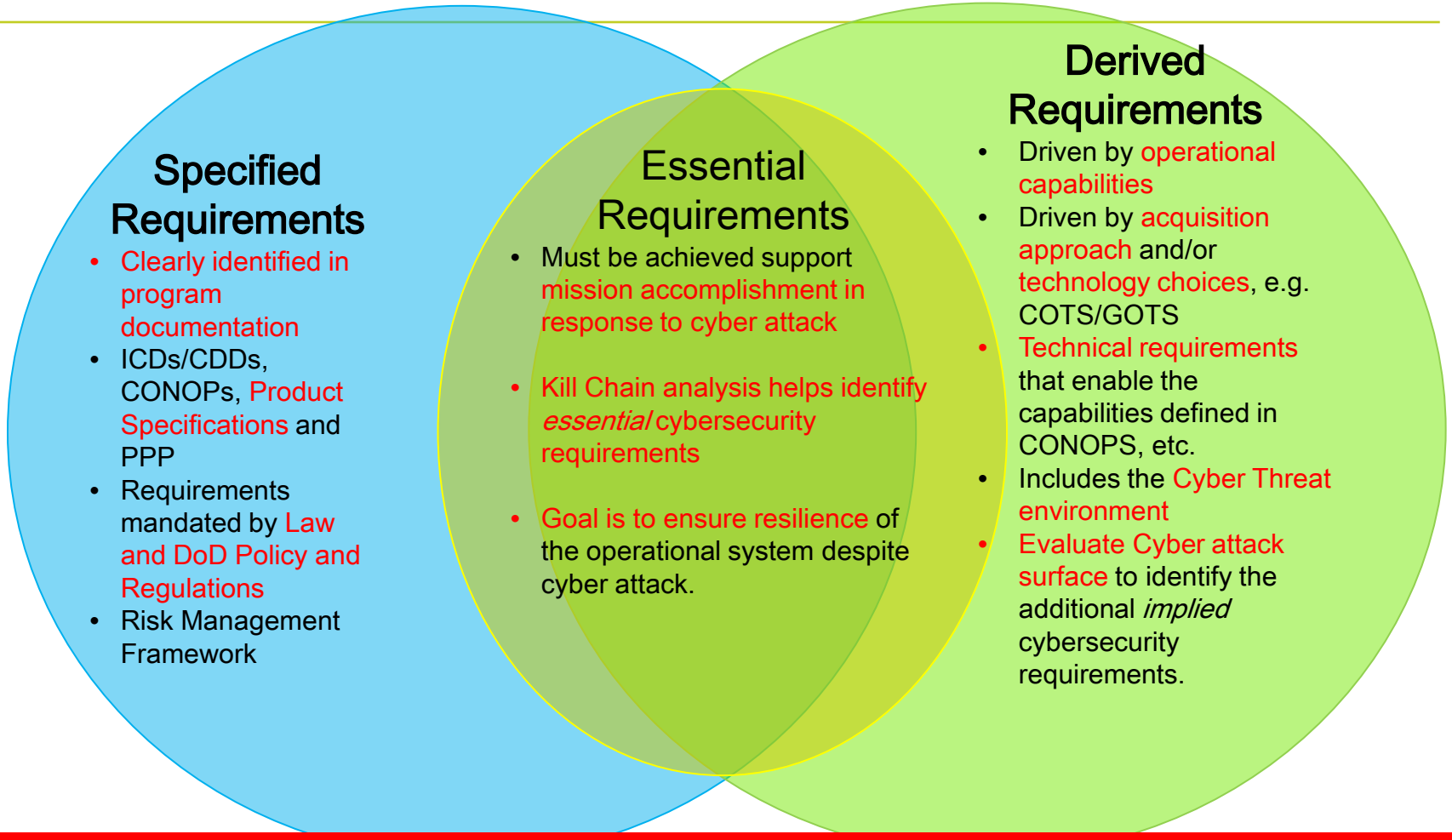
T&E WIPT develop Cybersecurity T&E Strategy

- **Understand Program Protection Plan and Cybersecurity Strategy**
  - Critical Components, Software, RMF Security Categorization, etc.
- **Identify cybersecurity requirements for Cybersecurity T&E**
  - Critical Operational Missions and supporting systems
  - Critical data exchanges and interfaces
  - Additional implied (derived) and essential requirements
- **Identify cybersecurity test organization(s)**
  - Security Controls Assessor, Vulnerability Identification/Assessment Teams
- **Identify Cybersecurity T&E Resources**
  - Cyber range resources(e.g., National Cyber Range (NCR), DoD Cybersecurity Range, Joint Information Operations Range (JIOR))
  - Cybersecurity Test Tools, M&S needs
- **Plan to integrate Cybersecurity into overarching T&E Strategy**

T&E WIPT should engage SMEs in a Core Team to execute!

MITRE

Essential Cybersecurity Requirements "Distilled" from Both Specified and Derived Requirements



T&E WIPT collaborates to confirm requirements, testability, identify test resources and plan T&E events!

MITRE

Phase 2 - Characterize the Cyber Attack Surface

Identify the seams and gaps between the Cybersecurity Strategy/RMF Artifacts and "Verify" the system as planned/built

- Utilize cybersecurity SMEs to assist
- Review Technical Requirements, Security Architectures, Preliminary/Critical Designs
- Examine system Capabilities Documents, CONOPS and Operational Architectures
  - OV-3 Operational Information Exchanges, OV-6 Critical Missions
- Examine ISP and system architecture products
  - SV-1, SV-6 viewpoints identify interfacing systems, services, and data exchanges

E-2C+ Hawkeye

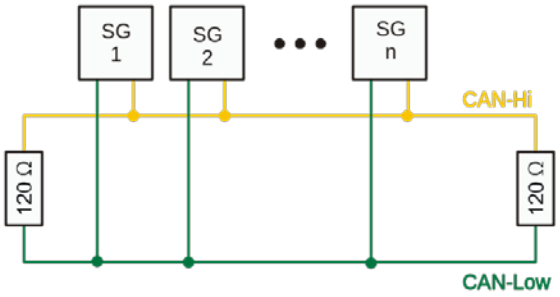
U.S. Navy Photo (RELEASED)

USMC Tactical Vehicle

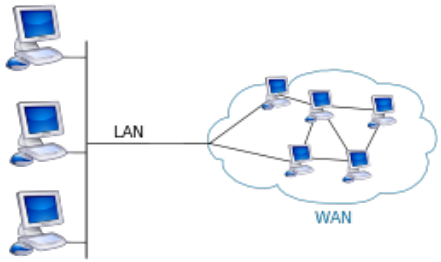
U.S. Navy Photo (RELEASED)

MITRE

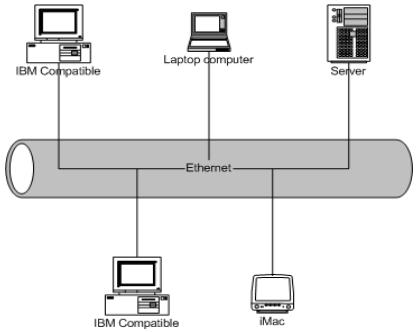
Working Definition: Attack Surface



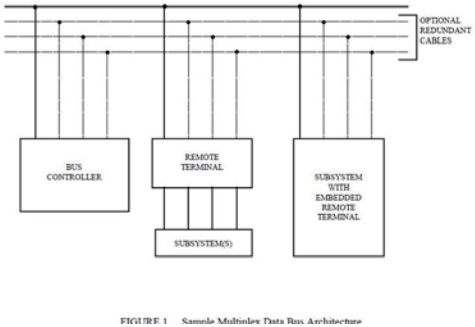
CAN-Bus



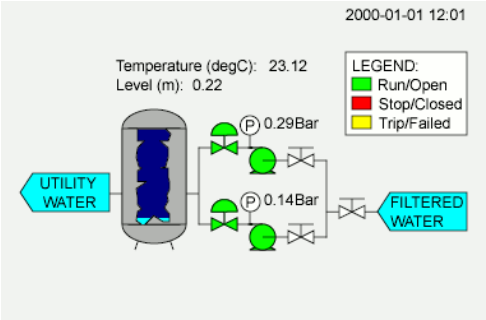
LAN-WAN



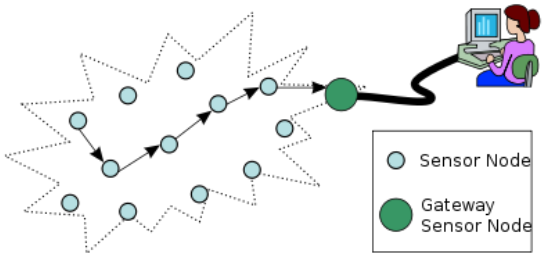
Ethernet LAN



1553 Data Bus



SCADA Network



Multi-hop Wireless Sensor Network

Attack Surface: A system's exposure to reachable and exploitable cyber vulnerabilities

Source: SANS Attack Surface Problem: http://www.sans.edu/research/security-laboratory/article/did-attack-surface

Graphics Sources: WIKIPEDIA Commons

MITRE

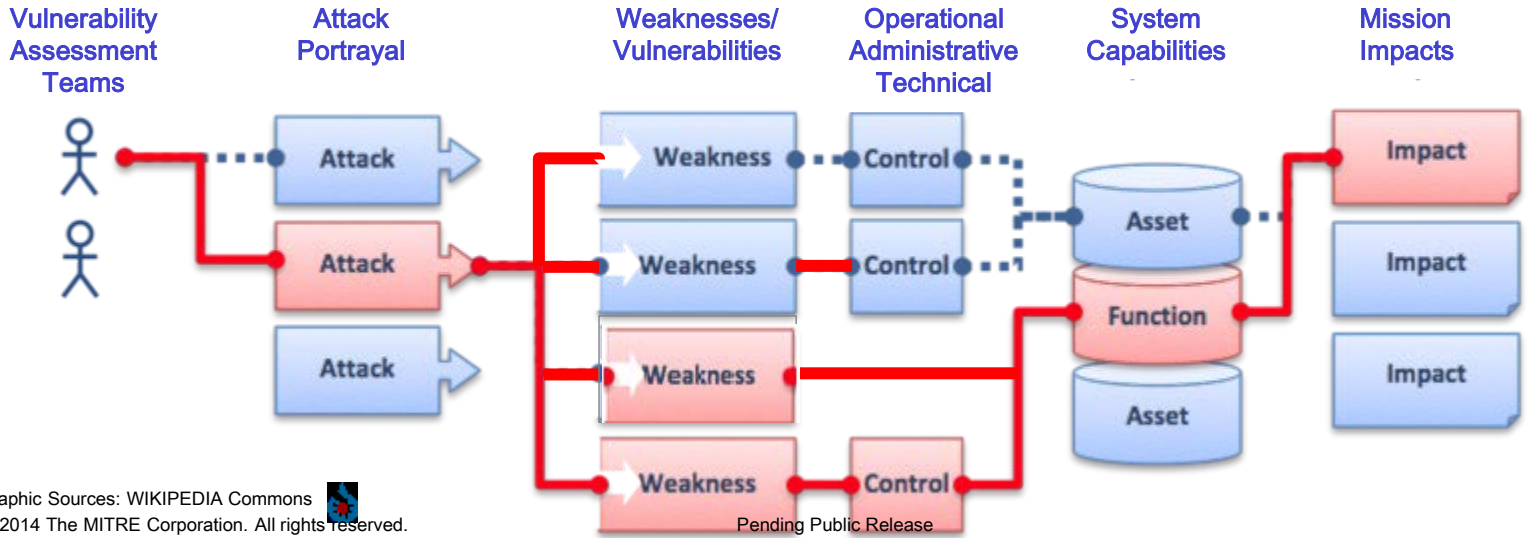
Phase 3 – Vulnerability Identification

- Evaluate Baseline Performance and Identify and Close exposed vulnerabilities in a SOS Context
- Confirm "Baseline Performance"
  - Functional test data
  - Evaluate SW/HW Cybersecurity test data
  - RMF security controls assessment data
  - Enumerate and close vulnerabilities
- Team has full knowledge/access to system
  - Works collaboratively to perform assessment
- Conduct cybersecurity testing in SOS context
  - Include or emulate the CNDSP in test infrastructure
  - Exercise Mission Threads
  - Use Kill Chain Model to portray cyber threats
  - Enumerate residual vulnerabilities and evaluate mission impact
  - Provide results to SE Team for remediation

T&E WIPT must engage vulnerability assessment team to plan and execute Phase 3!

Vulnerability Identification and Adversarial T&E

- Verifies RMF Controls and validates them as implemented
- Identifies exposed vulnerabilities
  - Technical Vulnerabilities require resources to mitigate
  - Operational and Administrative Vulnerabilities impact CONOPS, TTPs and Training
- Threat Portrayals are developed by Vulnerability Assessment Teams
  - Teams have “Full Knowledge” of the System and Mission
- Threat Agents exploit weaknesses/vulnerabilities in controls to capabilities
  - Cyber Attacks are portrayed by Vulnerability Assessment Teams
- Exploits ultimately impact system resiliency and operational missions



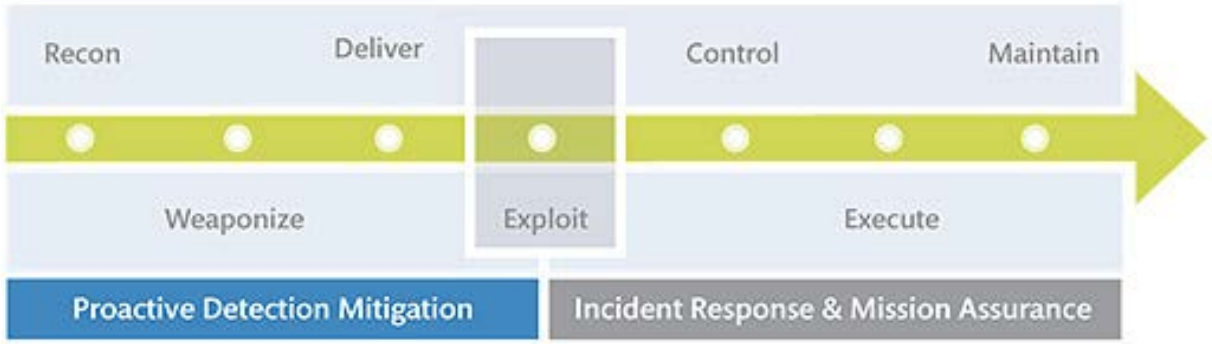
Graphic Sources: WIKIPEDIA Commons

Cybersecurity Testing Resources

(SCA) Security Controls Assessors	(Blue Team) Cooperative Vulnerability Identification	(Red Team) Adversarial Vulnerability Exploitation
Focus is compliance with RMF controls	Cooperative and comprehensive assessment with full knowledge and access to system	Non cooperative and adversarial assessment to exploit known or suspected weaknesses
Executes the Security Assessment Plan (SAP)	Exposes known/discovers new vulnerabilities present in systems	Attention on specific problem or attack vector
Linked to the Certification and Accreditation system	Reveals systemic weaknesses in security program	Develops an understanding of inherent weaknesses of system
Based on Security Technical Implementation Guides (STIGs) or similar documentation	Focused beyond adequacy & implementation of technical security controls and attributes	Both internal and external threats
Can be determined by multiple methods: hands-on testing, interviewing key personal, etc.	Multiple methods used: hands-on testing, interviewing key personal, or examination of relevant artifacts	Model actions of a defined internal or external hostile entity
Includes a review of operational and management security controls	Feedback to developers, system engineers and administrators for system remediation and mitigation	Report at the end of the testing
Conducted with full knowledge and assistance of systems administrators, owner and developer	Conducted with full knowledge and cooperation of systems administrators	Conducted covertly with minimal staff knowledge
No harm to systems	May harm systems and components and require clean up	May harm systems, may not harm people

Working Definition: Cyber Attack Lifecycle

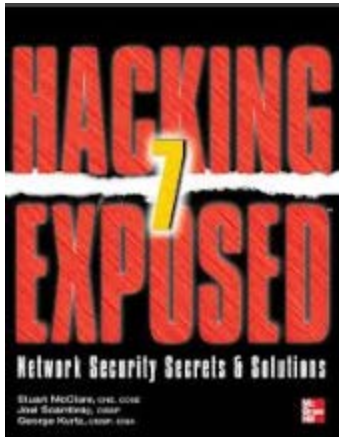
MITRE: Cyber Attack Lifecycle



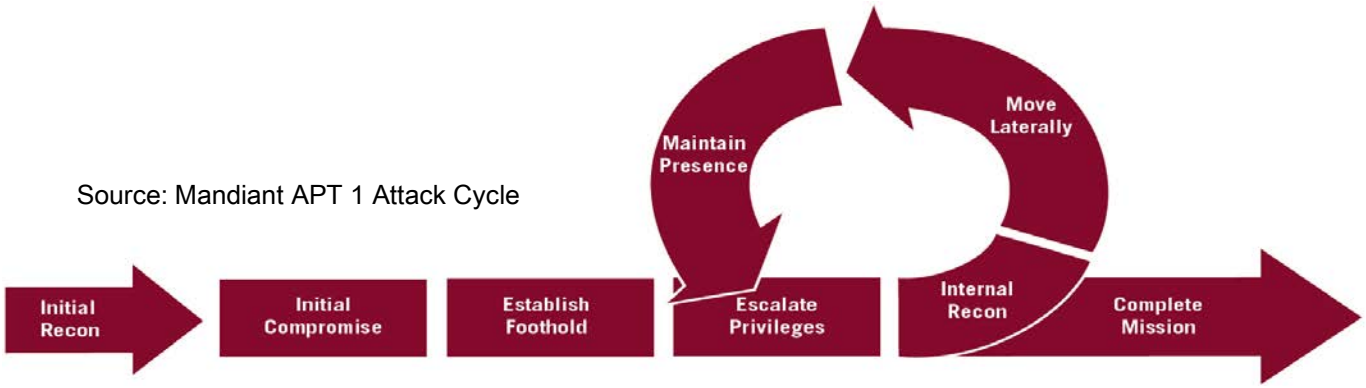
Cyber Attack Lifecycle: Framework to understand and anticipate the moves of cyber adversaries at each stage of an attack.

Typical adversary attack stages include:

Reconnaissance, weaponization, delivery, exploitation, control, execution, and persistence.

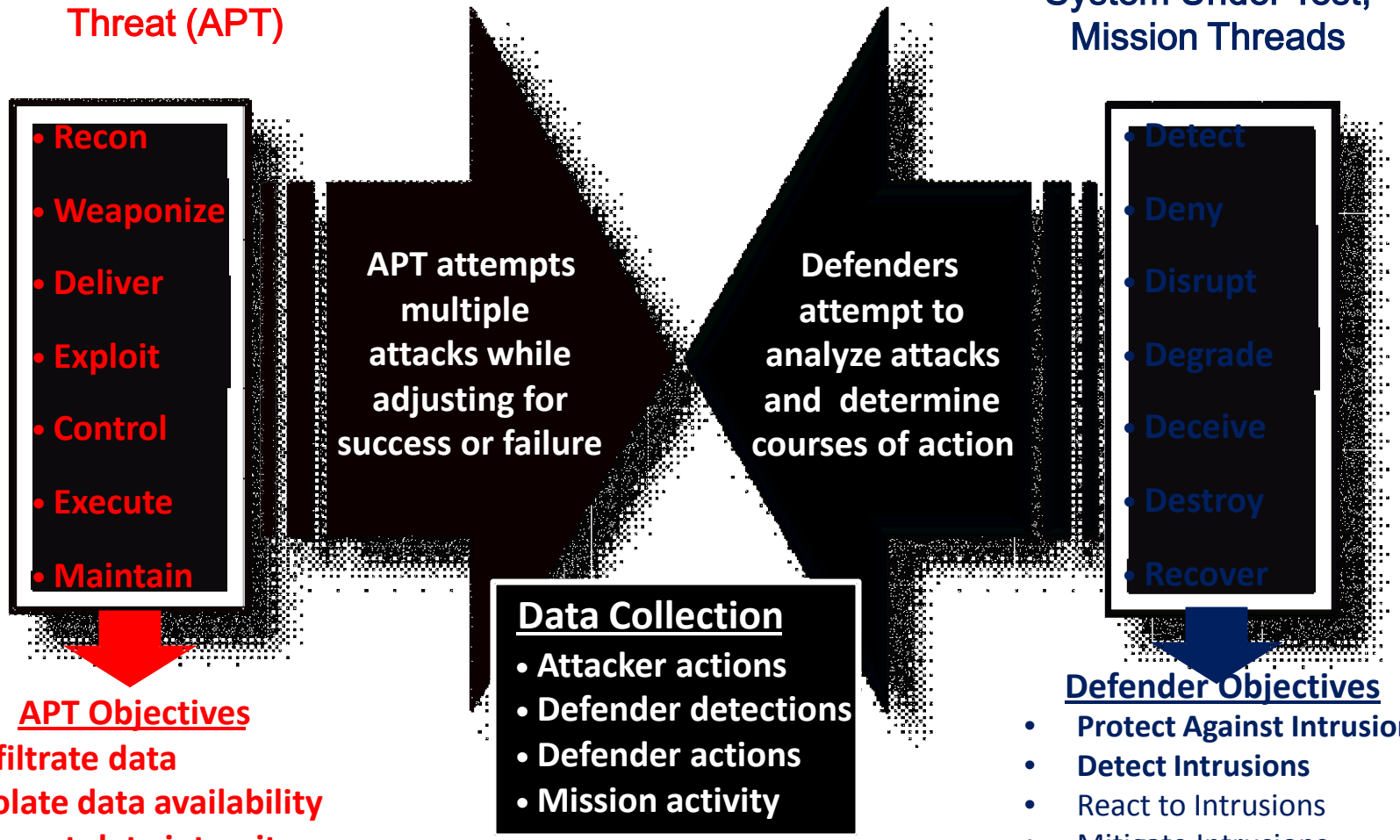


Source: Mandiant APT 1 Attack Cycle



MITRE

Vulnerability Assessment Teams "Portray" Cyber Attack Lifecycle



Source: Institute for Defense Analysis (IDA), February 2013

Phase 4 – Adversarial Cybersecurity DT&E

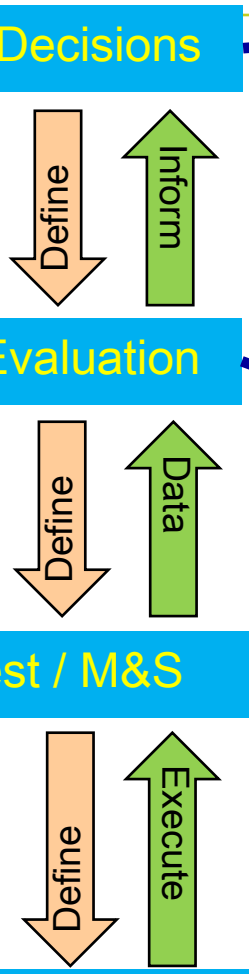
"Adversarial" Assessment to evaluate "Cyber Resiliency" in mission context!

- **Assessment Team identifies and evaluates remaining and or residual vulnerabilities**
  - Include or emulate the CNDSP in test infrastructure
  - Include typical users if available and exercise Mission Threads
  - Portray threats in a contested cyber domain
  - Team emulates the threat adversary TTPs to exercise Cyber Attack Lifecycle
  - Analyze results to determine impact to mission
  - Recommend corrective actions to improve resilience

"Cyber Resiliency" ability of a nation, organization, or mission or business process (and supporting systems) to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function.

T&E WIPT must engage Vulnerability Assessment Team to plan/execute Phase 4!

Developmental Evaluation Framework



Developmental Evaluation Objectives	System Requirements and T&E Measures		Decisions Supported							
			Decision #1		Decision #2			Decision #3	Decision #4	
			DSQ #1	DSQ #2	DSQ #3	DSQ #4	DSQ #5	DSQ #6	DSQ #7	DSQ #8
Functional evaluation areas System capability categories	Technical Reqmts Document Reference	Description	Identify major decision points for which testing and evaluation phases, activity and events will provide decision supporting information. Cells contain description of data source to be used for evaluation information, for example: 1) Test event or phase (e.g. CDT1....) 2) M&S event or scenario 3) Description of data needed to support decision 4) Other logical data source description							
Performance										
Performance Capability #1	3.x.x.5	Technical Measure #1	DT#1		M&S#2				DT#4	M&S#2
	3.x.x.6	Technical Measure #2	M&S#1		DT#3				DT#4	M&S#2
Performance Capability #2	3.x.x.7	Technical Measure #3				DT#3			IT#1	
	3.x.x.8	Technical Measure #4				M&S#4			IT#1	
Interoperability										
Interoperability Capability #3	3.x.x.1	Technical Measure #1				DT#3		DT#4		
	3.x.x.2	Technical Measure #2		IT#2		M&S#4		DT#4		
Interoperability	3.x.x.3	Technical Measure #3		IT#2				IT#1		M&S#2
	3.x.x.4	Technical Measure #4						IT#1		DT#3
Cybersecurity										
SW/System Assurance	PPP 3.x.x	SW Assurance Measure #1			SW Dev Assess		SW Dev Asses	SW Dev Assess		
RMF		RMF Contol Measure #1	Cont Assess		Cont Assess	Cont Assess	Cont Assess			
Vulnerability Assess		Vul Assess Measure #1				Blue Team			Blue Team	
Interop/Exploitable Vuln.		Vul Assess Measure #2				Red Team			Red Team	
Reliability										
	4.x.x.1	Technical Measure #11		M-demo#1						IT#5

T&E WIPT should engage SMEs in a core team to help develop Cyber Evaluation Framework!

Cyber Evaluation Framework Expands on DEF's "Security" Decision Support Questions

	Critical Developmental Issues (Enterprise)	*Can terminals communicate with PL?*	*Is CAPS capable of mission planning?*	*Can CAPS command and control PL using in-band?*	*Is CAPS capable of utilizing out-of-band T&C through the Host interface?*	*Is GW capable of connecting polar users and mid-lat users?*	*Is EPS secure?*	*Is EPS sustainable?*
	Integration Test Event	ISTs E0100/ E0830	IST E0250	ISTs E0250/E0810	ISTs E0350/E0800	GW FQT/IQT/IST E0830	GW FQT/CAPS FAT/IST E0280	
Developmental Test Objectives	**Measures***							
Capacity and throughput	**Full Service Capacity**	x	x	x		x		
	GW Throughput					x		
	CAPS Max CPU Utilization			x				
	# of planned and active Terminals	x	x	x				
Coverage	Constellation	x	x	x				
	Service Coverage Region	x	x	x				
Unstressed Communications	Data rate, Error Rate, EIRP, RRIP, **Uplink**	x	x	x				

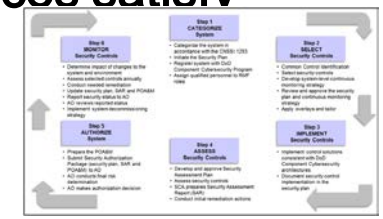
Cyber Technical Capability/ Evaluation Activity Categories	DT Objectives - Cyber Technical Capabilities	Is the system and software developed securely?	Does [illegible] baseli[illegible] techni[illegible] IA	Do exposed vulnerabilities adversely effect system resiliency?	Is the system mission capable and interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities?	Test Activity / Data Source
Systems and Software Assurance	Software Vulnerabilities Mitigated in critical components	Program Protection Plan (PPP) Table 5.3.3. Example Software Metrics include: Number/Category outstanding SDRs %Code Static Analysis Planned/Inspected %Code Planned/Inspected %SW LOC Planned/Inspected CVE %SW LOC Planned/Inspected CAPEC %SW LOC Planned/Inspected CWE %SW LOC Planned/Pen Tested %SW LOC Tested (Coverage)				Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E PPP, CDRLs from CTR and government.
	Software Vulnerabilities Mitigated in Operational System	~~PPP Table~~ 5.3.3 Example Operational System Metrics for CPI, Critical Functions, Developmental SW and COTS/NDI include: Fault Isolation Planned/Implemented Least Privilege Planned/Implemented System Element Isolation Planned/Implemented Input Checking/Validation Planned/Implemented SW Lead Key (Signed) Planned/Implemented				Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E PPP, CDRLs from CTR and government.
	Software Vulnerabilities Mitigated in Development Environment	~~PPP Table~~ 5.3.3 Example Development Environment Metrics based upon SW Products selected including Compiler, Automated Testing Tools, Configuration Management System, Test Results Database, etc.				Contractor T&E/ Functional Qualification Testing (FQT)/ Government ST&E PPP, CDRLs from CTR and government.
	Anti-Tamper Vulnerabilities Mitigated	PPP Table 5.3.3, PPP Section 5.3.1 and/or Appendix D: Anti-tamper Plan. Metrics derived for appropriate CPI, Critical Components				Anti-Tamper Implementation Plan/Report PPP, CDRLs from CTR and government.
	Supply Chain Risks Mitigated	PPP Section 5.3.4 Supply Chain Risk Management (SCRM) Metrics derived from SCRM V&V Plan for appropriate CPI, Critical Components etc.				Supply Chain Risk Management/Reports PPP, CDRLs from CTR and government.
RMF Controls and Attack Surface Standards Verification	RMF Control Categories include: Access Control Awareness and Training Audit and Accountability Configuration Management Contingency Planning Identification and Authentication Incident Response Media Protection Maintenance Physical and Environmental Protection Planning Security Assessment and Authorization Personnel Security Risk Assessment System and Services Acquisition System and Communications Protection System and Information Integrity ~~Program Management~~		RMF Metrics and measures can be derived from several source documents including Capabilities Documents, PPP, Cybersecurity Strategy, Security Controls Assessment Plan, Performance Specifications etc. Example metrics by control category may include: % of controls verified # and Category Deficiencies % of inherited controls verified # and Category Inherited Deficiencies		ST&E/ Security Controls Assessor/ Step 3/4 Vulnerability Assessment
	Attack surfaces to be evaluated based on Step 2 analysis. Potential Attack Surfaces include: Connecting systems explicitly identified in Cybersecurity Strategy RF Interfaces (Data Links, Wi-Fi, Bluetooth) SCADA Interfaces (Control Net, Device Net, Fieldbus, Zig Bee, etc.)		Metrics and measures can be developed from DIACAP/RMF and technical standards appropriate for the exposed Attack Surface.		ST&E/ Security Controls Assessor/Step 3 Vulnerability Assessment. Contractor ST&E and Government Technical Standards Testing as appropriate
Cyber Kill Chain Vulnerability Assessment	Cyber Kill Chain Vulnerability and System Interoperability and functionality in response to exploited cyber vulnerabilities shall be evaluated in operational scenarios: Operational scenarios and critical missions should be based on authoritative sources including CONOPS and capabilities documents. Representative cyber threats should be developed based upon STARs and cyber attack scenarios developed by vulnerability assessment teams and approved by appropriate authoritative source. Cyber kill chain as exercised by the adversary includes the following steps: Reconnaissance, Weaponization, Delivery, Exploit, Control, Execute, Maintain. Cyber Defense in response to adversarial actions include actions to redirect, obviate, impede, detect, limit, and expose adversarial actions. The lexicon reference is Intended Effects of Cyber Resiliency Techniques on Adversary Activities			ITT will develop measures in collaboration with other program stakeholders. Critical Missions may be derived from CONOPS, Capabilities Documents, PPP, etc. Interoperability metrics and measures should be derived from the NR-KPP. Metrics include: - Support to military operations - Enter and be managed in the network - Exchange information - Support net-centric military operations. Sources for cyber security metrics and measures may be derived from program technical documentation, or other authoritative sources including the DoD Strategy for Operating in Cyberspace and Resilient Military Systems Cyber Threat Defense Science Board Task Force. The below measures are derived from MP 120053, Rev 1, Cyber Resiliency Metrics, dated Apr 2012. Additional metrics will be selected by the ITT in collaboration with other Stakeholders. Initial planned metrics include: - % cyber resources properly configured (Configuration varies by resource) - % attempted intrusions stopped at network perimeter/ deflected - % mission-essential capabilities for which multiple instantiations available - Avg Length of time between initial disruption and restoration - Quality of restored data - Quality of choices made during design and engineering that affect resiliency - % mission-essential datasets for which all items effectively have two or more independent external data feeds - % mission-essential data stores for which a master copy exists - % data value assertions in a mission-essential data store for which a master copy exists		Step 3 Vulnerability Assessment: Team has full knowledge and access to the System and all supporting components (Blue Team)
System interoperability and functionality in response to exploited cyber vulnerabilities						Step 4 Vulnerability Assessment: Team functions as an adversary without knowledge or access to the system (Red Team)

Example Cyber Evaluation Framework Decision Support Questions and Evaluated Cyber Capabilities

- **Is the system and software developed securely?**
  - Software Vulnerabilities Mitigated in critical components
  - Software Vulnerabilities Mitigated in Operational System
  - Software Vulnerabilities Mitigated in Dev. Environment
  - Anti-Tamper Vulnerabilities Mitigated
  - Supply Chain Risks Mitigated

Program Protection Plan

- **Does the system and associated Attack Surfaces & Interfaces satisfy baseline Cybersecurity technical standards?**
  - RMF Controls Verification
  - RMF Interfaces Verified
  - Other Attack Surfaces Verified (Based on Phase 2 analysis)
  - Examples: GPS, Data Links, Wi-Fi, Bluetooth, ICS, SCADA Interfaces

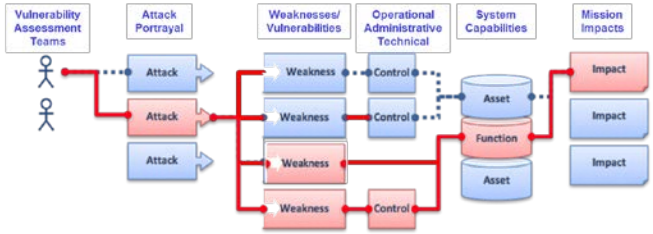


RMF

MITRE

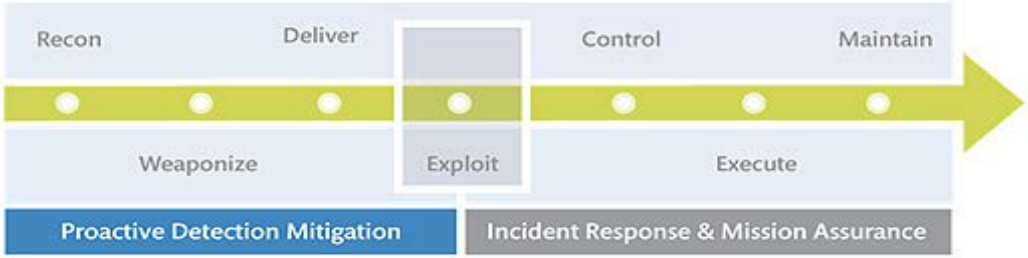
Cyber Evaluation Framework Decision Support Questions and Cyber Capabilities Evaluated

- **Does Baseline Performance support Critical Missions and are exposed vulnerabilities identified and closed?**
  - Exercise Critical Missions
    - Derived from CONOPS, Capabilities Documents, PPP, etc.
  - Identify Number and Severity of Exposed Vulnerabilities



- **Is the system mission capable, interoperable and resilient in response to exploited cyber vulnerabilities?**
  - Evaluate mission performance in context of Cyber Attack Lifecycle

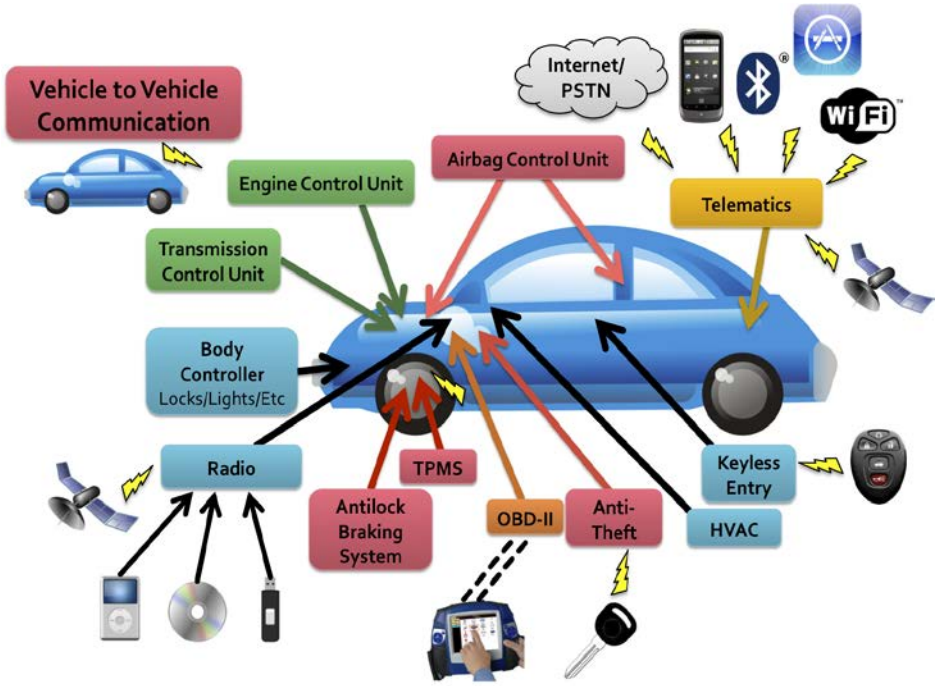
MITRE: Cyber Attack Lifecycle



MITRE

"Simple" Example: Comprehensive Experimental Analyses of Automotive Attack Surfaces

- **Modern automobiles pervasively computerized**
  - Engine, Transmission, Body, Airbag, Antilock Brakes, HVAC, Keyless Entry Control, etc.
- **Attack surface extensive**
  - Telematics: Blue Tooth, Cellular, Wi-Fi, Keyless Entry
- **Attack Surface easily exploited**
  - OBD Diagnostics, CD players, Bluetooth
- **Example:**
  - Cellular radio/ Wi-Fi exploits permit….
  - Long distance vehicle control, location tracking, in-cabin audio exfiltration



Aug 2011: Comprehensive Experimental Analyses of Automotive Attack Surfaces
Source: University of California, San Diego, University of Washington

Example Phase 1: Understanding Cybersecurity Requirements/Develop T&E Approach

Urban Assault Vehicle

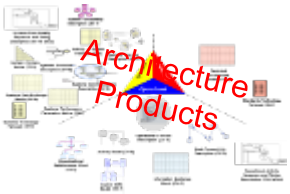
Graphic Sources: WIKIPEDIA Commons

Example Requirements Resources

- CONOPS
- Capabilities Documents
- Information Support Plan
- Systems Requirements Documents
- ***Program Protection Plan***
- Cybersecurity Strategy
- RMF Packages
- Contract Specs/Technical Requirements Documents

Plan Cybersecurity T&E to

- Engage with SE Team Early
- Engage with SE/SSE Activities/Processes
- Requirements Reviews, Contracting, SETRs etc.
- Plan Verification DT&E to close Attack Surface
- Conduct “Kill Chain Vulnerability Assessments” (Blue Team and Red Team) to evaluate mission performance
- Verify Production Readiness at MS C
- OT&E post MS C



MITRE: Cyber Attack Lifecycle

MITRE

Example Phase 2: Characterize the Attack Surface

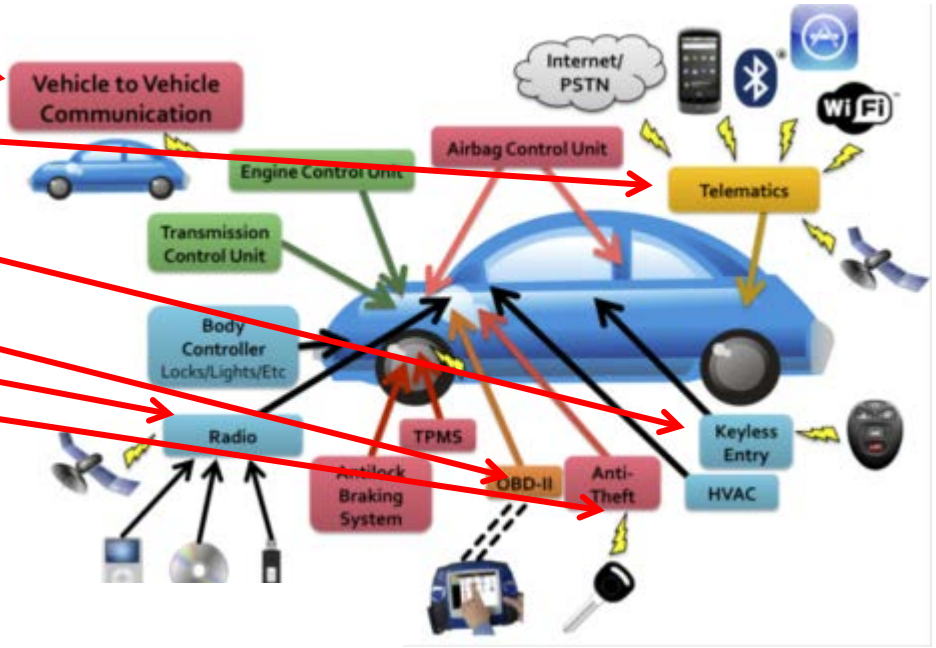
Stakeholders Identify Vehicle Attack Surface

1. Vehicle to Vehicle Comms
2. Telematics
3. Keyless Entry
4. OBD II
5. Radio
6. Anti Theft

Refine T&E Strategy to Understand

- All systems interfaces
- Likelihood of attack?
- What happens if/when exploited?
- Approach to close/mitigate vulnerabilities
- Adequacy of Cybersecurity T&E Approach

Urban Assault Vehicle Attack Surface



Aug 2011: Comprehensive Experimental Analyses of Automotive Attack Surfaces
Source: University of California, San Diego, University of Washington

Missions	Critical Functions	Supporting HW/SW/Firmware	System Impact
Mission 1	Data Fusion	Processor X SW Module Y	2 1
Mission 1	Fire Control	Database Z SW Module Y	3 1
Mission 2	Critical Function 3	Sensor A Radar B	1 1

PPP Criticality Analysis

Example Phase 3: Vulnerability Identification

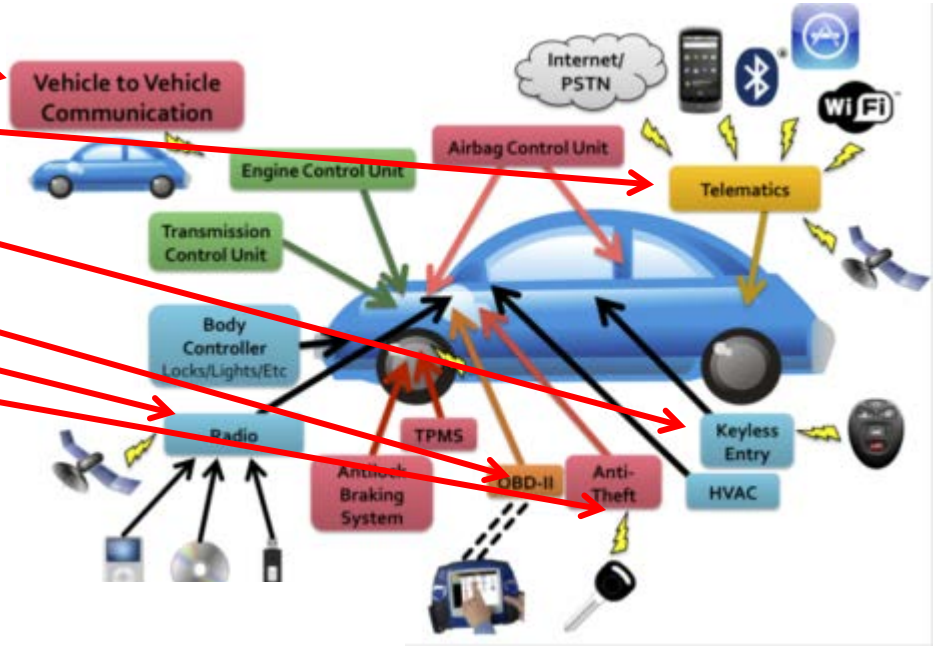
Vehicle Attack Surface

1. Deny Vehicle/Vehicle Comms
2. Intercept Telematics
3. Clone Keyless Entry
4. Corrupt OBD-II
5. Monitor Radio
6. Disable Anti-Theft

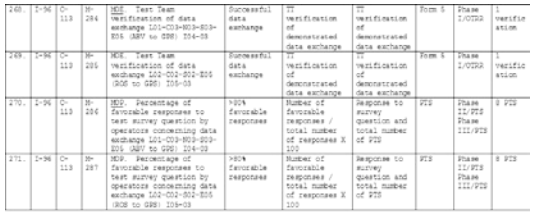
T&E Activities

- Verify/Exercise Critical Missions
- Cooperative "Kill Chain Vulnerability Assessments" (Blue Team)
- ID potential exploits, exposed vulnerabilities/mission impact

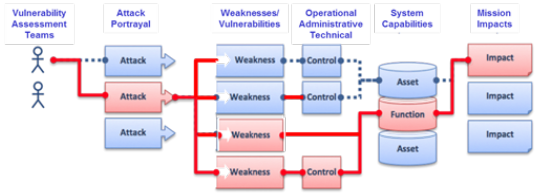
Urban Assault Vehicle Attack Surface



Aug 2011: Comprehensive Experimental Analyses of Automotive Attack Surfaces
Source: University of California, San Diego, University of Washington



Vehicle SV-6 Systems Data Exchange Requirements



Threat Based Testing

Cyber Attack Lifecycle

MITRE

Example Phase 4: Adversarial Cybersecurity DT&E

Exercise Critical Missions

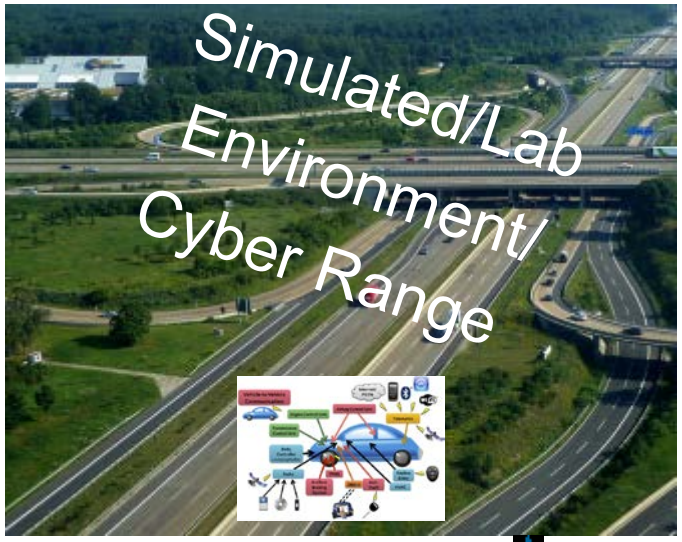
1. Tx/RX Vehicle/Vehicle Comms
2. Cellular Phone Calls
3. Use Keyless Entry
4. Upload/Download OBD II Data
5. Tune Radio
6. Anti Theft

T&E Actions

- Verify/Exercise Critical Missions
- Adversarial "Kill Chain Vulnerability Assessments" (Red Team)
- ID exposed vulnerabilities/mission impact
- Develop DT&E Assessment

Cyber Attack Lifecycle

Urban Assault Vehicle Autobahn Mission



Graphic Sources: WIKIPEDIA Commons

Graphic Sources: WIKIPEDIA Commons

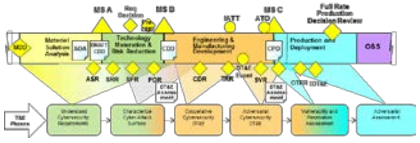
MITRE

Where are we going?

- **DASD DT&E and DASD SE**
  - High level engagement ongoing between principals
  - DT&E Staff Specialist are reviewing PPPs as they surface for review
- **DASD DT&E and OSD DOT&E**
  - Working to update DAG, DAU Course Material etc.
- **DASD DT&E direct "Program Engagement"**
  - DT&E Staff Specialists are leading core teams to assist PMs
  - Significant insight gained
- **DASD DT&E Cybersecurity "Process Improvement"**
  - Cybersecurity Pilot being executed in collaboration with NAVAIR
- **TRMC JMETC provides distributed Cyber T&E capabilities**
  - National Cyber Range

Closing

- **DASD DT&E, SE, and OSD OT&E are collaborating to improve acquisition outcomes**
  - Current policy and procedures are being updated
- **Systems Security Engineering (SSE), RMF and Cybersecurity T&E processes must be aligned and mutually supportive**
  - T&E Community must engage early to influence SSE process
  - T&E must provide feedback in a timely manner to key stakeholders for "assessment and mitigation"
  - Early feedback will positively impact cost schedule and performance!
- **Cybersecurity T&E is not "Controls Compliance"**
  - Evaluates planned and implemented Cybersecurity Measures
    - T&E can help verify baseline security requirements
  - Evaluates exposed "Attack Surface"
    - Identify exposed Vulnerabilities
  - Focuses on critical operational missions
    - Evaluate system resilience



MITRE