Cybersecurity Test & Evaluation

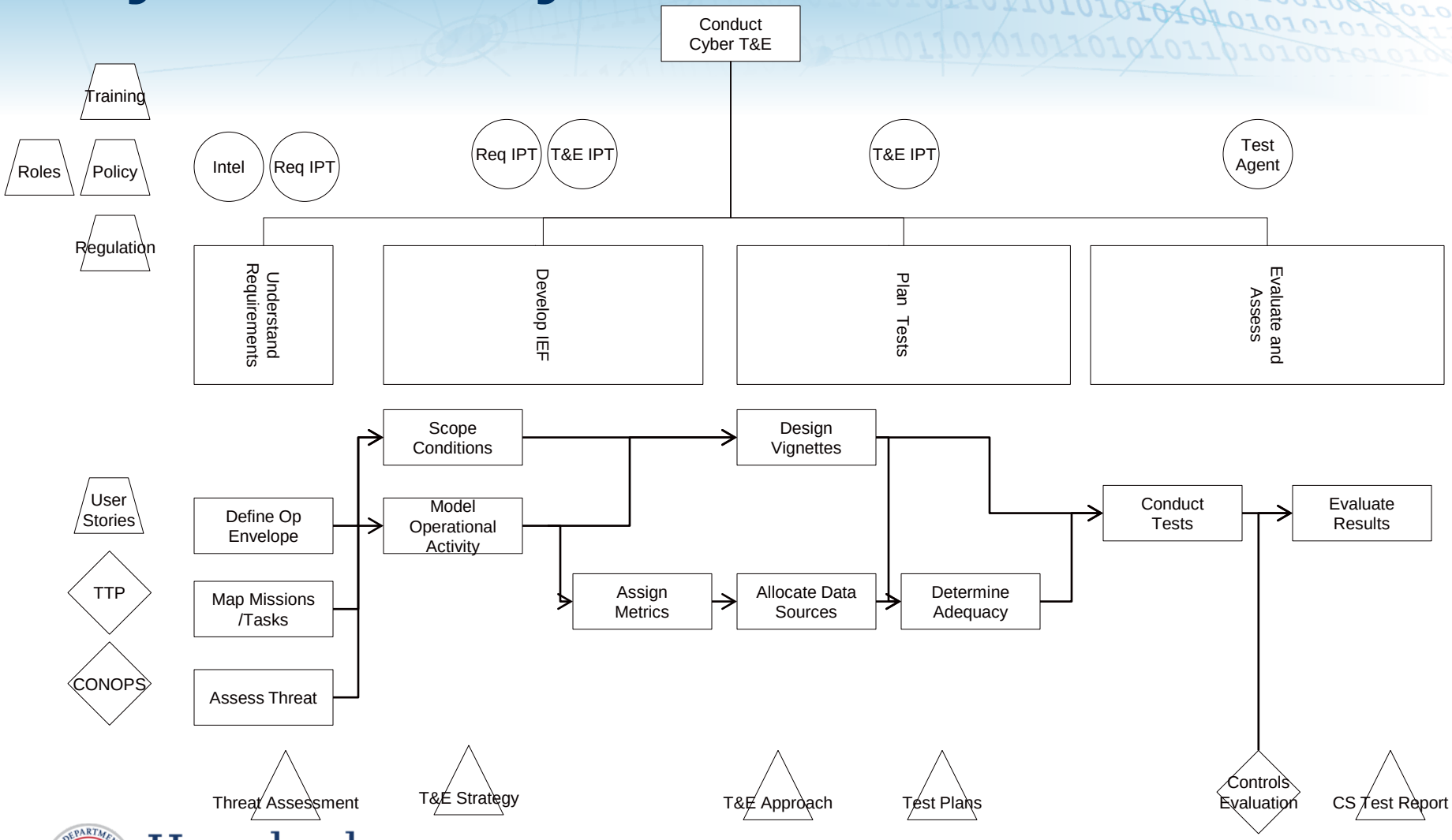
Homeland Security

Science and Technology

Alex Hoover

Office of Systems Engineering
Science and Technology Directorate

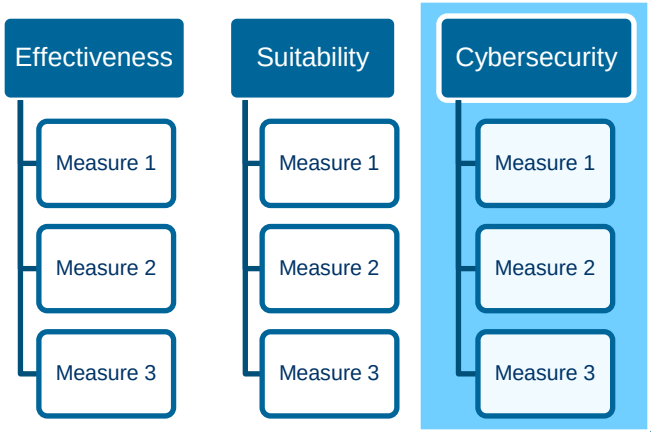
Cybersecurity in T&E



Homeland Security
Science and Technology

Sample Cybersecurity Evaluation Structure

Understand Collective Impact on Mission/Task Accomplishment



Cybersecurity

Is this capability resilient to cyber attack?

Denial of Service (Mission Impact)

- Probability of Occurrence
- Duration
- Repeatability
- Attack Resources

Degradation of Service (Task Impact)

- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Degree of Degradation
- Attack Resources
- Defend Resources

Data Manipulation (Task Impact)

- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Degree of Manipulation
- Attack Resources
- Defend Resources

Data Exfiltration (Enterprise Impact)

- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Significance of Exfiltration
- Attack Resources
- Defend Resources

External Pivoting (Enterprise Impact)

- Probability of Occurrence
- Duration
- Repeatability
- Probability of Detection
- Attack Resources
- Defend Resources

Homeland Security
Science and Technology

Capabilities

		Minimal	Limited	Moderate	Advanced
Knowledge	General Systems	Home market hardware, networks and, general-purpose languages. Basic user OS and applications. Public cryptography/ authentication. Public exploits of known vulnerabilities.	Common hardware, firmware, and defensive devices. Enterprise network and OS. Industry data protocols. 0-day exploits of less common/more vulnerable software, custom software.	Custom hardware, embedded systems, and less common network/protocols, specialized firmware. Biometric-based authentication. 0-day exploits of more common/less vulnerable software.	Classified systems, platforms, and software. Cross-domain devices, cryptography and associated hardware. 0-day exploits of restricted government systems and industrial control systems.
	Target Network and Systems	Information found from commonly available open sources or from external reconnaissance of target organization.	Knowledge of network and system specifications and type/configuration of host-based defenses equivalent to an authorized user in the target environment.	Knowledge of network and system specifications and type/configuration of networked defenses equivalent to an authorized administrator in the target environment.	Knowledge of network and system specifications and defenses equivalent to an authorized domain administrator in the target environment.
	Target Operations	Information found from commonly available open sources or from external reconnaissance of target organization.	Knowledge from more specialized literature or equivalent to prior experience with target operations, including key information or supporting systems.	Knowledge equivalent to substantial prior experience with target operations, including work flow and sub-task objectives.	Knowledge of current target operations equivalent to an experienced authorized operator.
Tools	Hardware	Inexpensive home market hardware.	Hard-ware, clusters, costing $10,000s or dozens of man hours.	Hardware costing $100,000s or hundreds of man hours.	Custom hardware costing $1,000,000s or thousands of man hours.
	Software	Freeware and inexpensive commercial tools.	Commercial software.	Custom software, polymorphic malware, rootkits.	Custom software, firmware-resident malware.
	Infrastructure	Access through publically available infrastructure.	Direct control of leveraged public infrastructure.	Covert remote access tools and loggers.	Covert close access.
Operations	Planning	Opportunistic actions, no planning.	Intent and short-range plans formed on-the-fly as needed.	Organizes one or more operations with specific target systems and associated effects on target organization	Organizes multiple operations against separate targets, synchronizing timing, accesses, and planned second-order effects
	Procedures	No demonstrated stealth, non-attribution or efficient use of resources	Countermeasures for common defensive systems. Non-attribution. Efficiency in use of resources consistent with intent.	Advanced and custom non-attribution tools. Efficiency in use of resources consistent with intent	High degree of control of defensive infrastructure. Non-attribution, false flag operations. Efficiency in use of resources consistent with intent
	Persistence	Intermittent, directed activity.	Gradual, low level passive operations.	Repeated active operations.	24/7 monitoring and control of offensive capabilities.

Contact Information

Alex Hoover

Deputy Director, Cybersecurity and National Protection Programs

Science and Technology/Office of Systems Engineering

202-254-5615

alex.hoover@hq.dhs.gov

Homeland Security

Science and Technology