Introduction to Cybersecurity Test & Evaluation

T&E Learning Seminar Series

February 17, 2016

Homeland Security

Science and Technology

James Wells

Alex Hoover

Office of Test & Evaluation
Science and Technology Directorate

Procedures for Cybersecurity OT&E

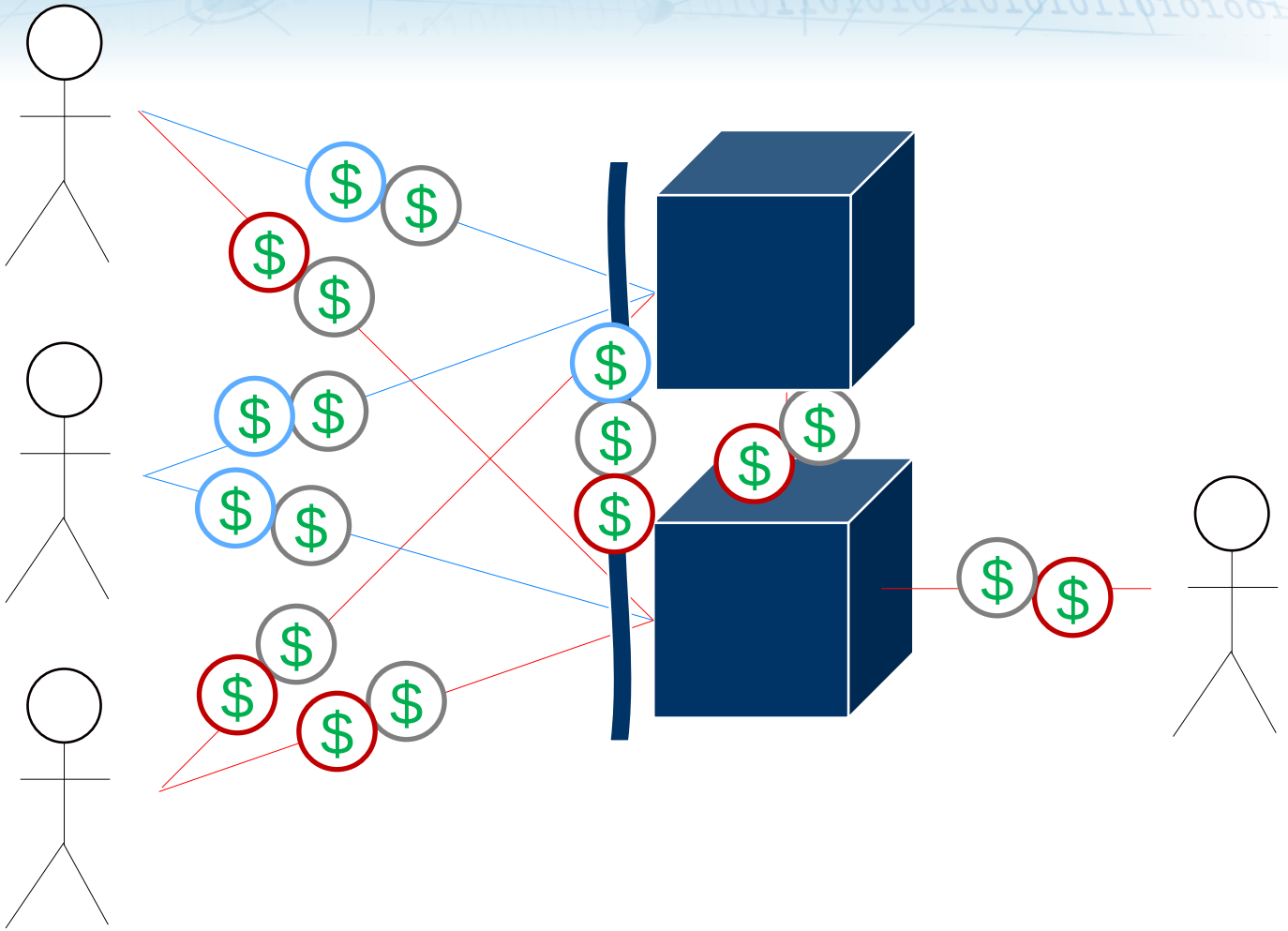
Purpose. Improve operational resilience of network-enabled capabilities and inform major acquisition decisions.

Applicability. Acquisition programs subject to DOT&E oversight will incorporate these procedures into all future TEMPs and OT&E Plans.

- Programs will include cybersecurity in TEMPs
  - Mission context, threat description, stakeholders, evaluation framework, integrated T&E, and resources
- OTAs will include cybersecurity in OT&E concepts, plans, & reports
  - Realistic threat portrayal to determine mission effects
- DOT&E will include cybersecurity in LOAs
  - Effectiveness, Suitability, & Cybersecurity

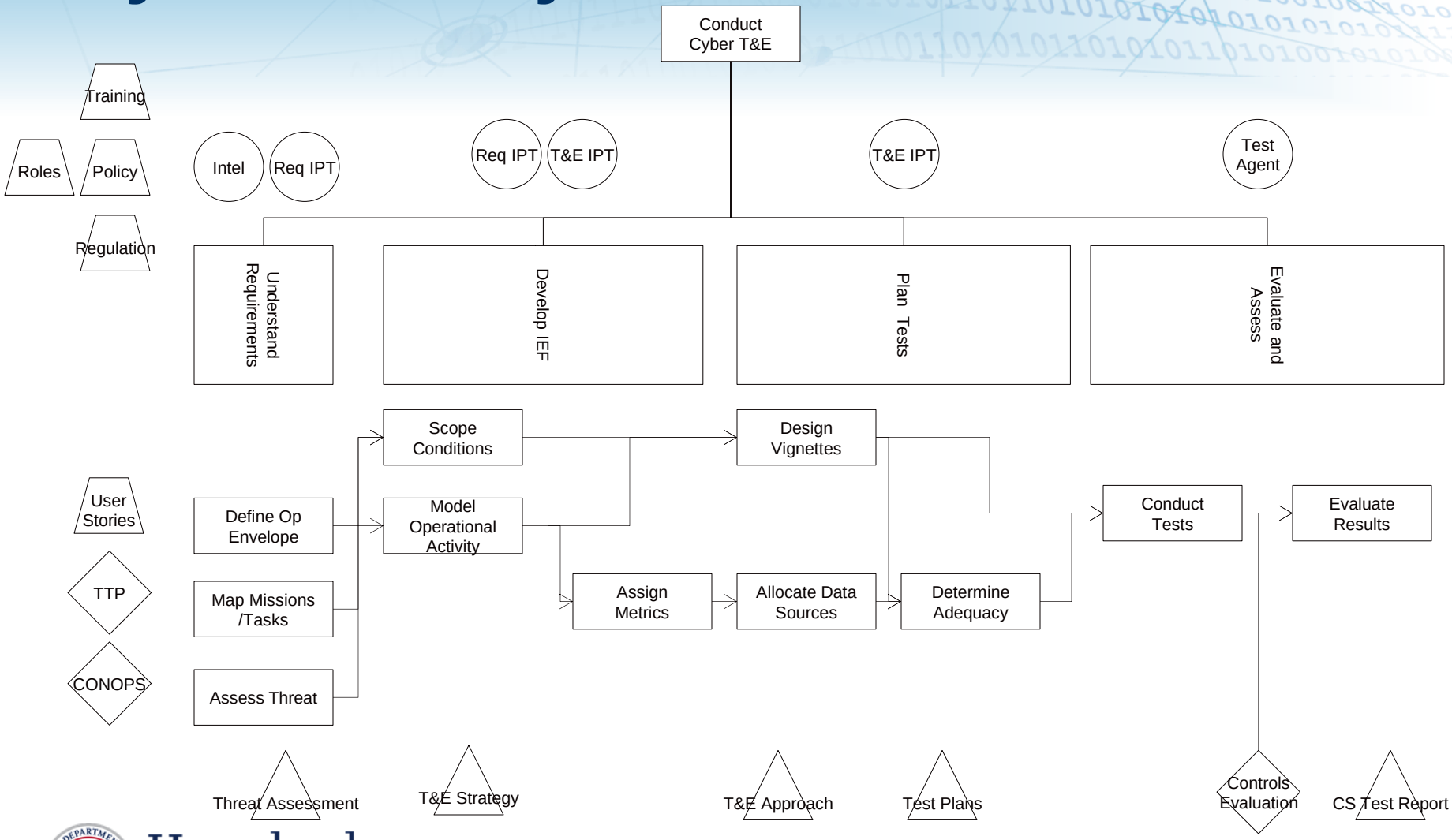

Homeland Security

Science and Technology



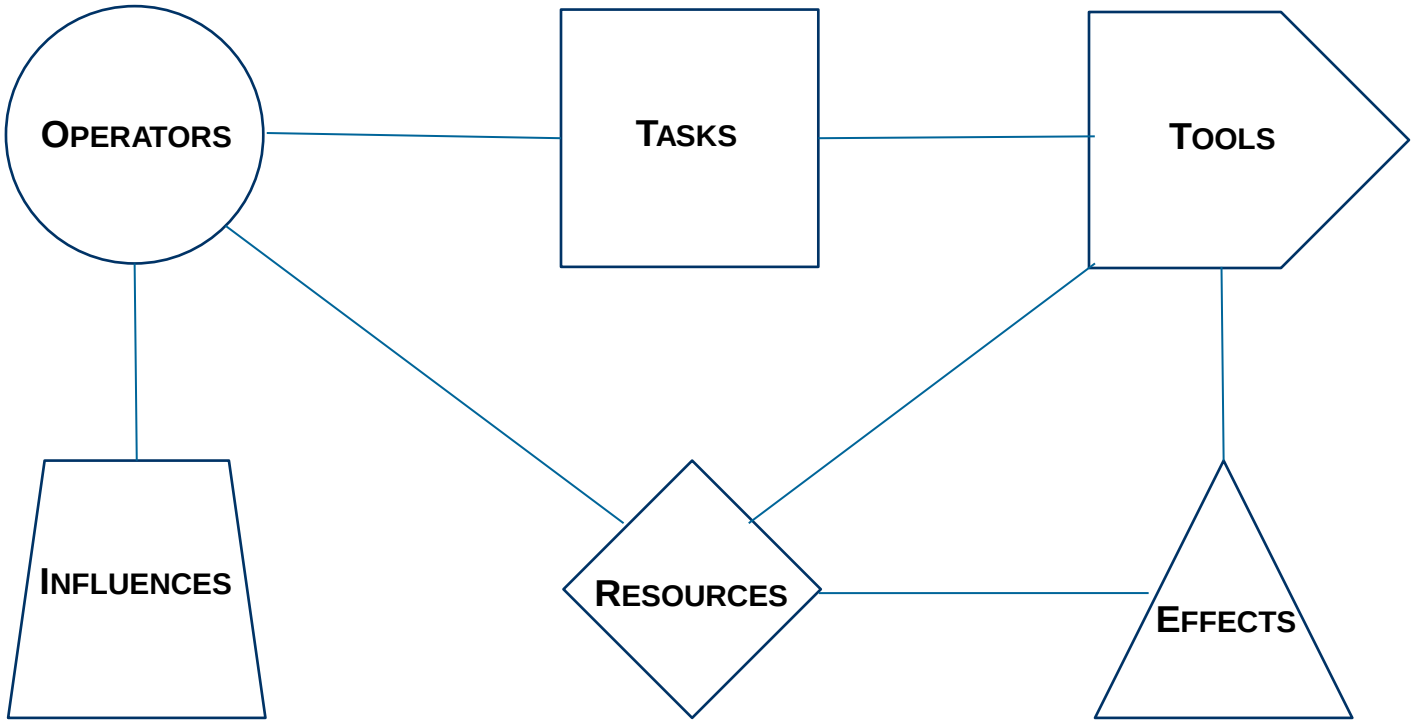
Homeland Security
Science and Technology

Cybersecurity in T&E



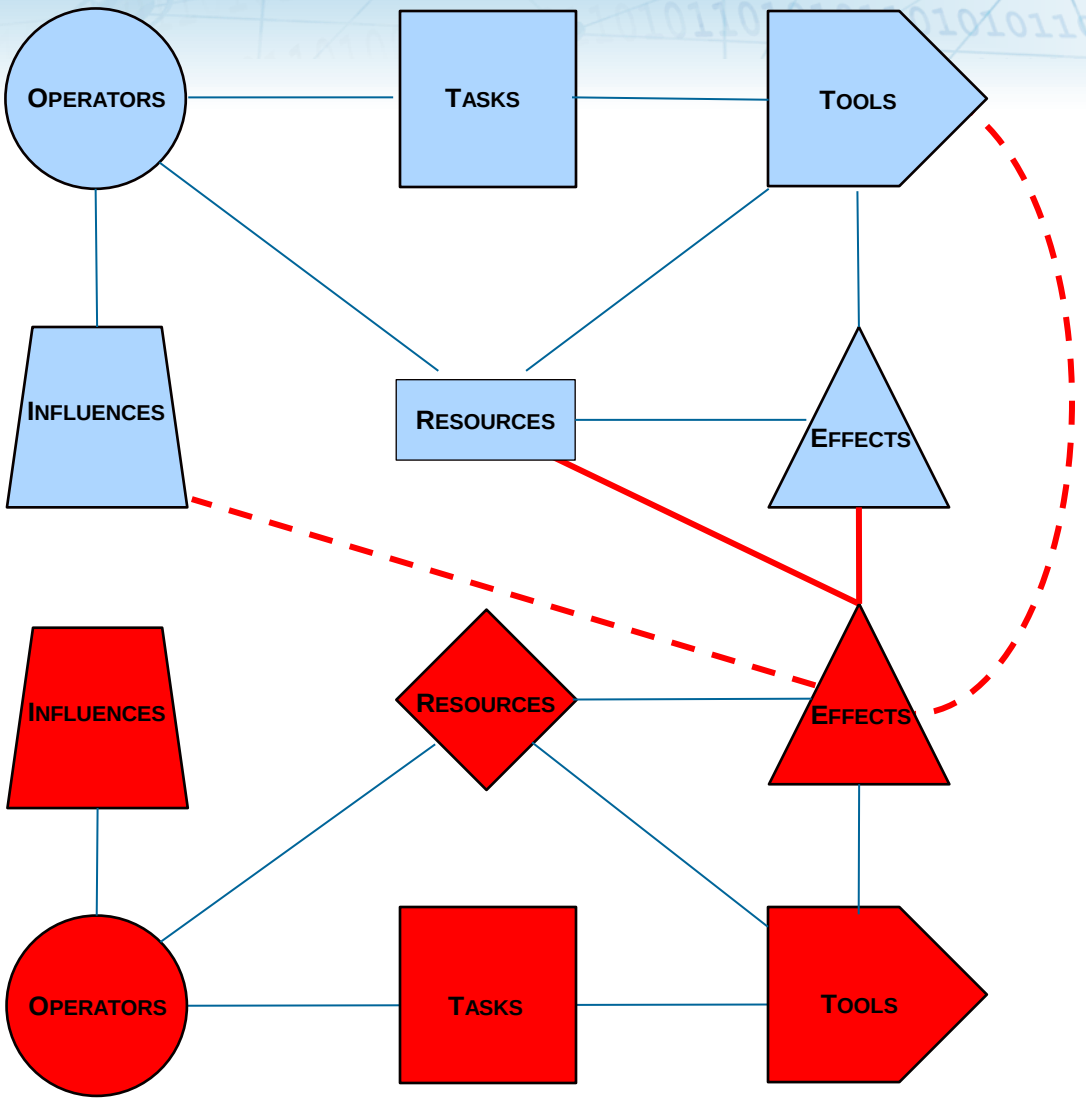
Homeland Security
Science and Technology

Operational Ontology



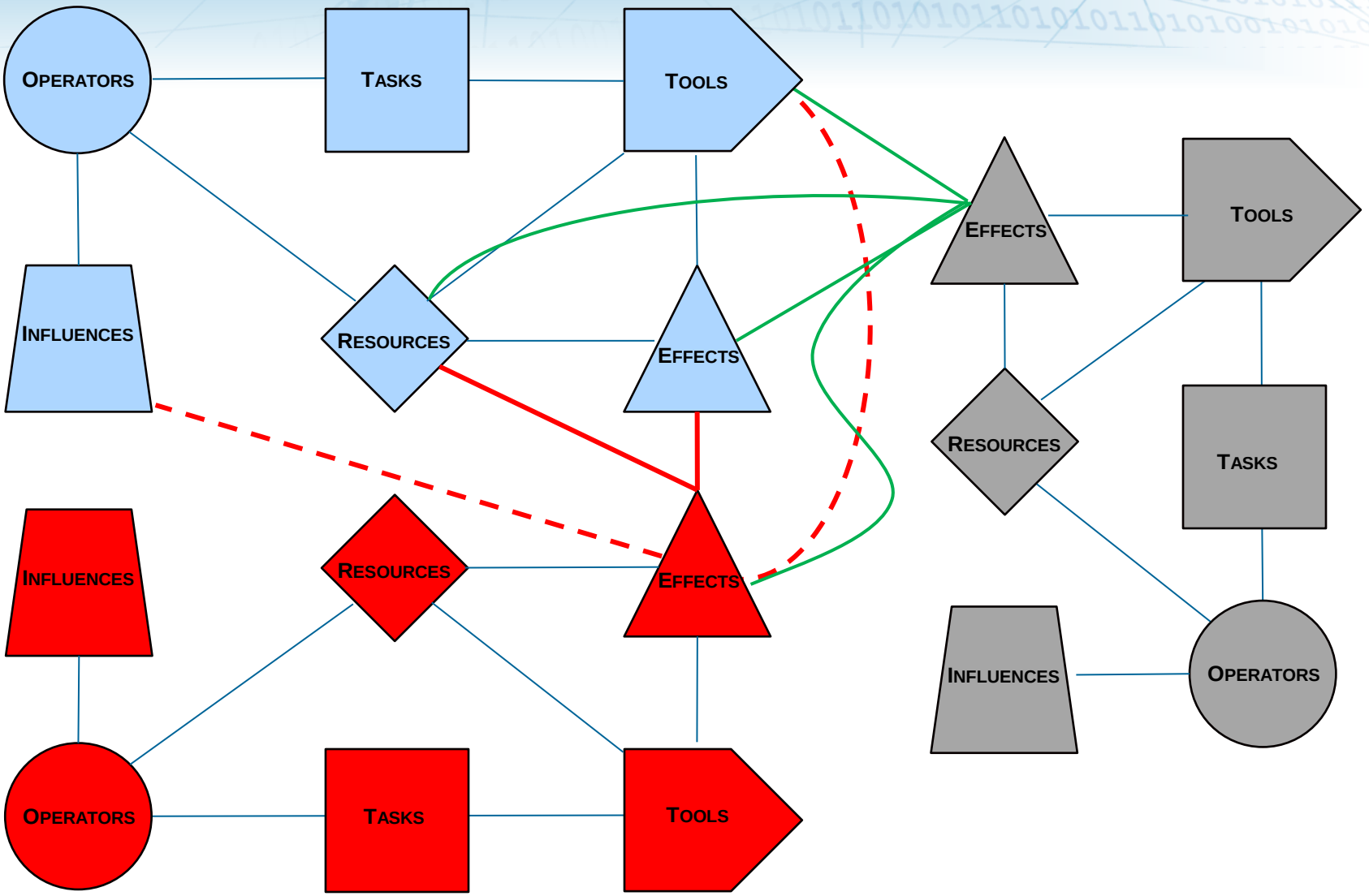
Homeland Security
Science and Technology

Adversarial Operational Ontology



Homeland Security
Science and Technology

Cyber Operational Ontology



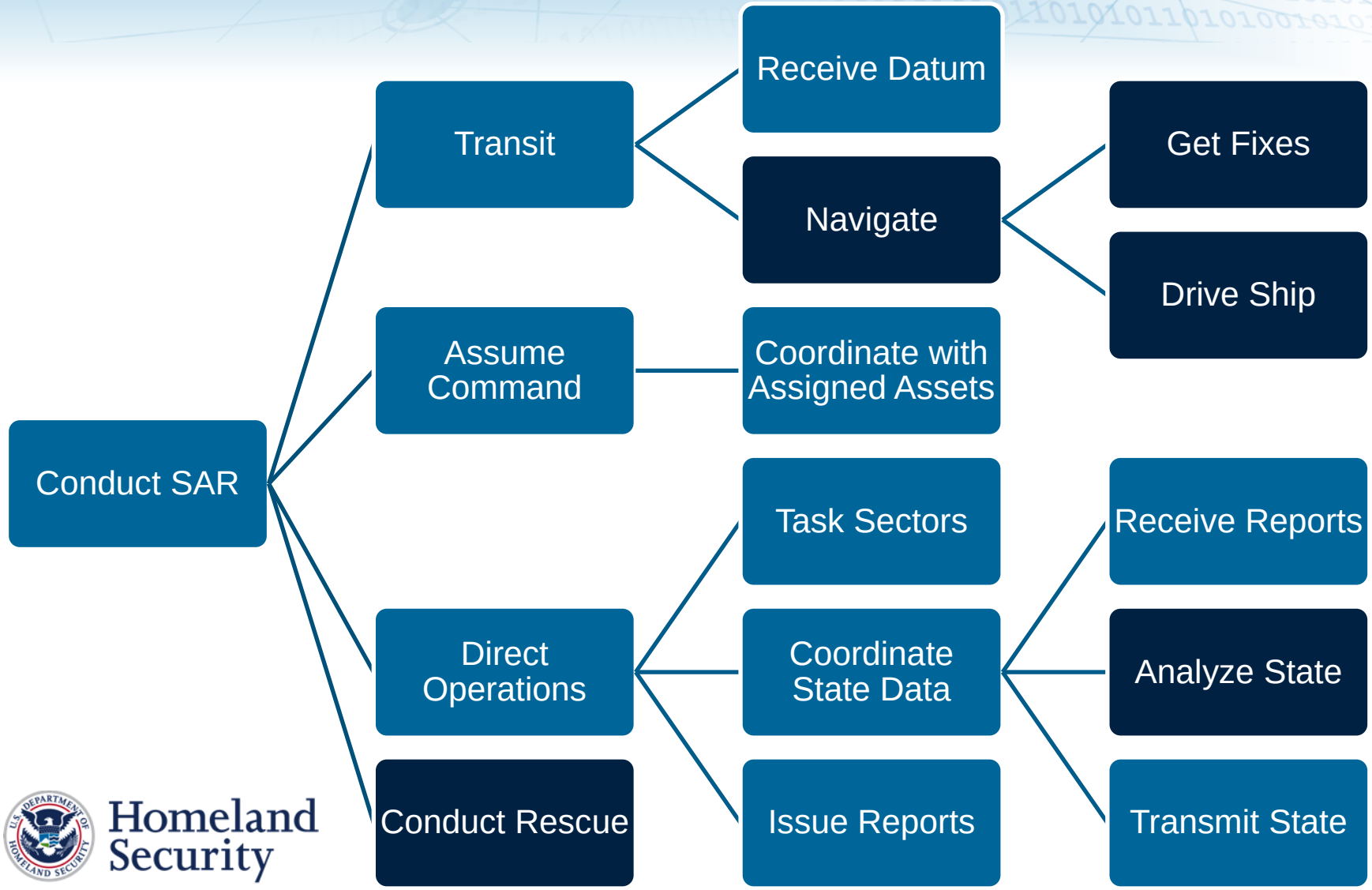
National Security Cutter (WMSL)

Search and Rescue (SAR) Mission from the ORD

2.2.2.7 Search and Rescue: While conducting training off the Northern California coast, a WMSL is diverted by the D11 Rescue Coordination Center to investigate an Emergency Position-Indicating Radio Beacon (EPIRB), registered to a sailboat sailing from Honolulu to San Francisco. Additional SAR assets are mobilized to support the effort, including USCG HC-130s and USN P-3s. The first fixed wing asset on scene reports debris in the water, but no presence of survivors.

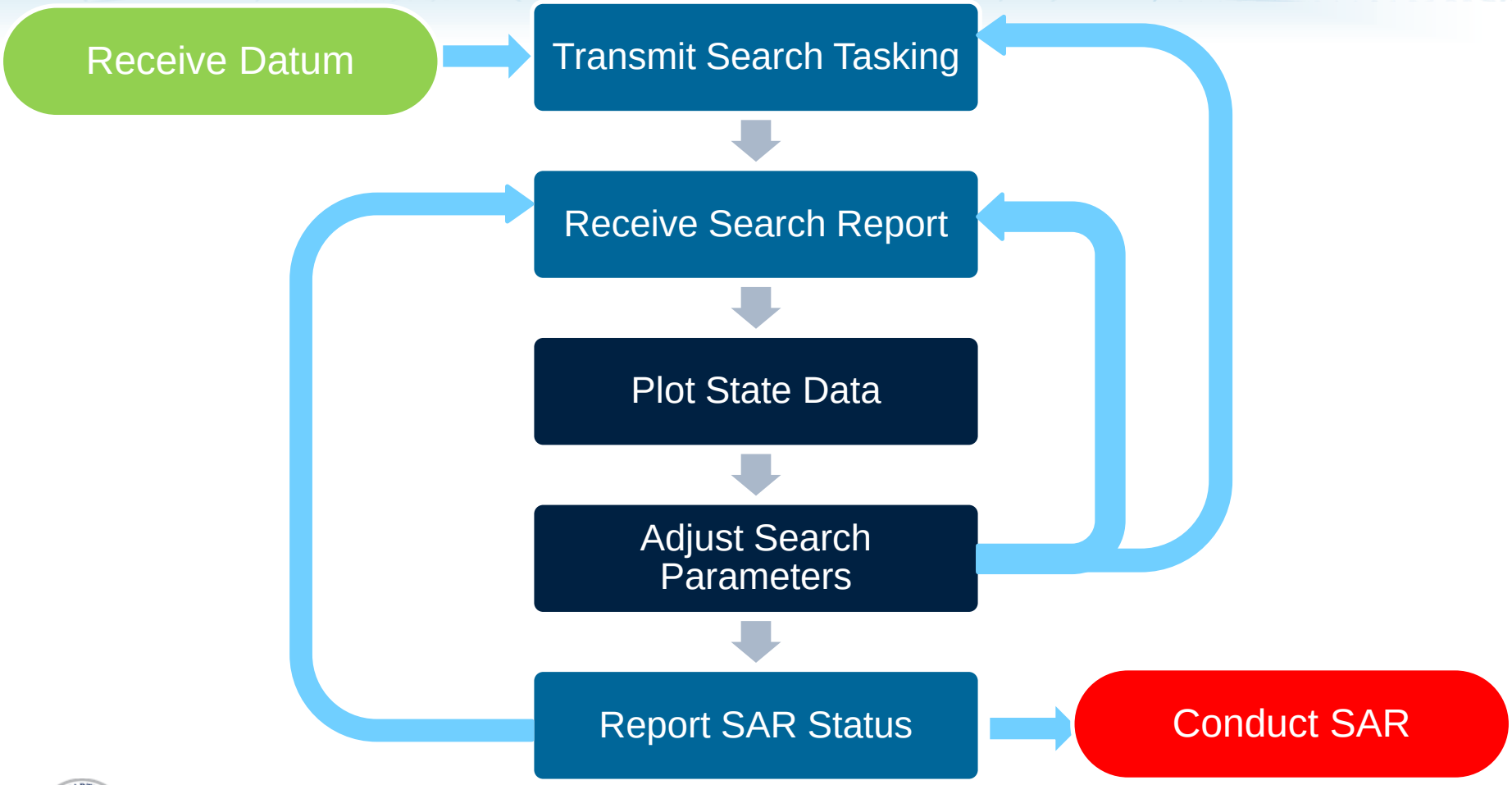
When the WMSL reaches the search area it assumes duties as OSC and begins to coordinate the search effort. The WMSL arrives at the beacon position and confirms debris in the water, but no presence of survivors. The search area is expanded and additional Coast Guard, U.S. Navy, and Automated Mutual-assistance Vessel Rescue system assets are diverted. Eventually, a USN P-3C locates a life raft with 3 passengers 16 miles south of the initial beacon report and the WMSL vectors its helicopter to the area. The helicopter uses the hoist and basket to recover all 3 passengers. The helicopter lands on the WMSL and the passengers are carried to the ship's sick bay, where they are examined by the ship's corpsman who determines that one of the passengers needs to be evacuated as soon as possible. WMSL proceeds at maximum speed to shore, and when within range, the ship's helicopter transports the patient to a nearby hospital. The WMSL then proceeds to enter port and delivers the other passengers to another hospital for care.

Tasks – Partitioning



Homeland Security
Science and Technology

Tasks – Flows

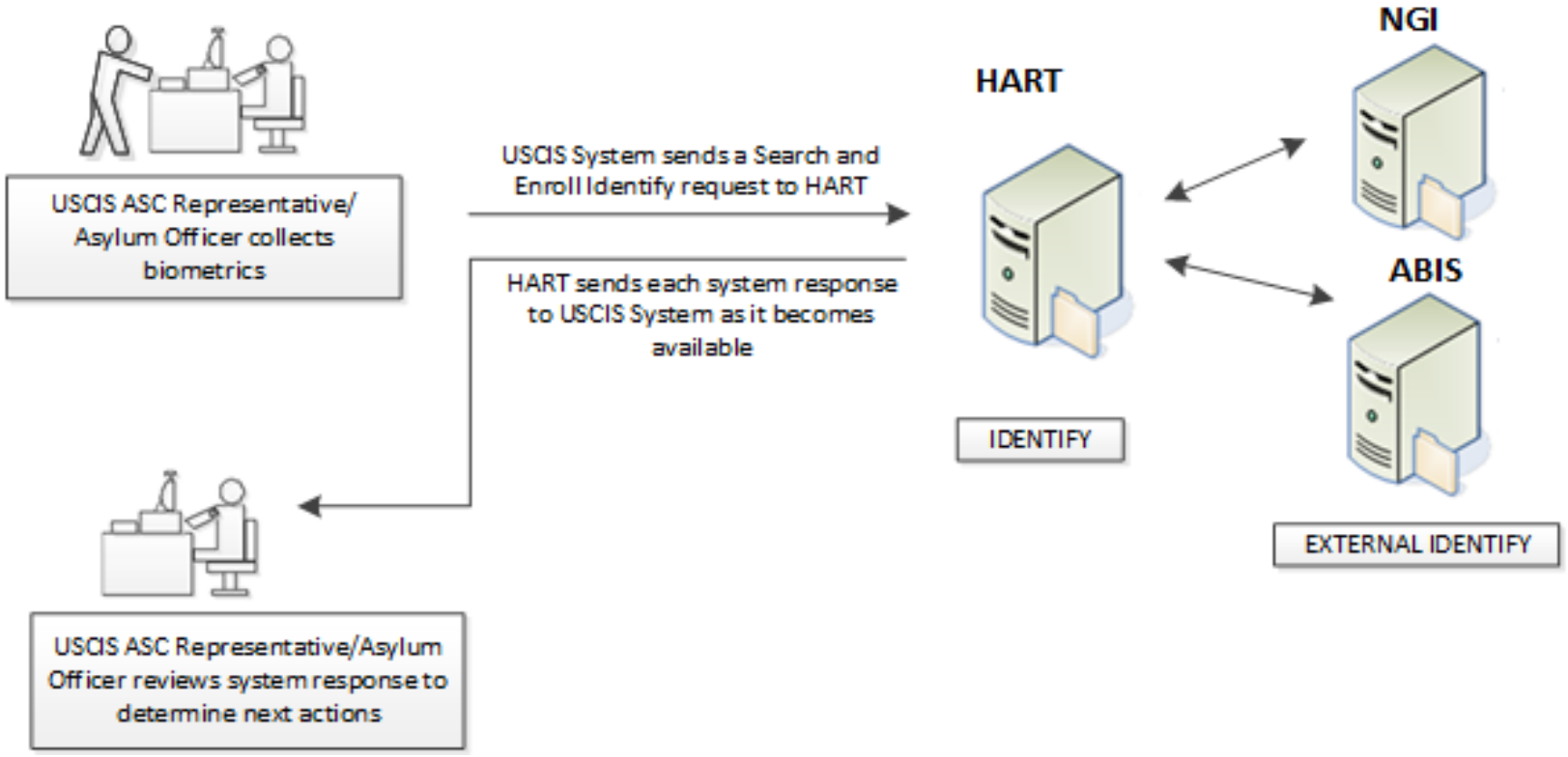


Homeland Security
Science and Technology

Customer Use Case Example (cont'd)

Homeland Advanced Recognition Technology (Use Case)

USCIS Biometric Enrollment with External Search (ASC and Asylum)

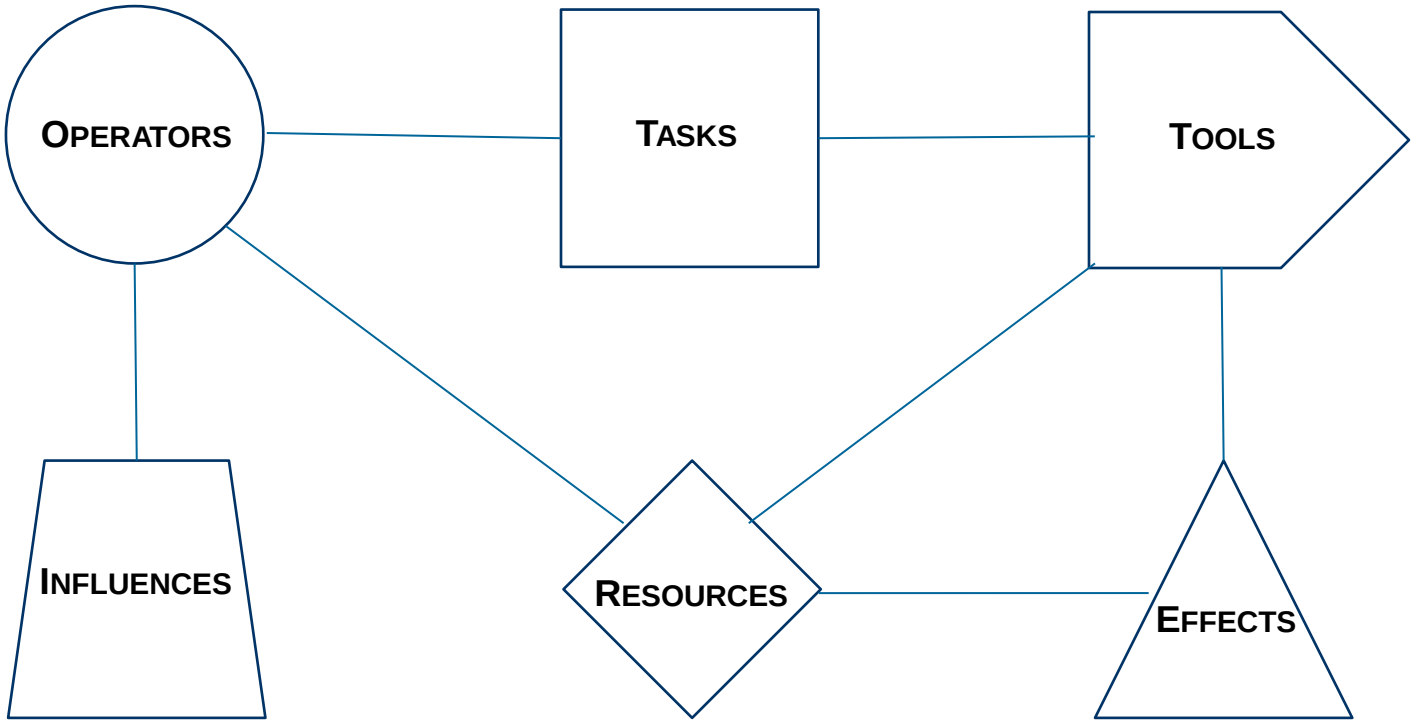


Customer Use Case Example

Homeland Advanced Recognition Technology (Use Case)

Use Case: USCIS Biometric Enrollment with External Search	
Primary Actor (Persons, Systems)	USCIS ASC Representative/Asylum Officer, USCIS System, OBIM HART System
Secondary Actor (Persons, Systems)	DOJ NGI, DoD ABIS
Goal	The goal is to successfully enroll an individual applying for a USCIS benefit at an Application Support Center (ASC).
Pre-Conditions	• Individual has fingers with readable prints. OR • Individual has readable irises (if fingerprints are not available). • The workstation device is available to the officer and is operational. • The mode of information transmission is operational.
Main Success Scenario Description	• Action 1: USCIS ASC Representative/Asylum Officer collects applicant's available biometrics (fingerprints, iris, and facial) at a workstation. • Action 2: USCIS System submits collected biometrics to OBIM HART with request to search and enroll in OBIM HART and search NGI and ABIS. • Action 3: OBIM HART executes an IDENTIFY with enrollment and generates an EXTERNAL IDENTIFY to NGI and ABIS. • Action 4: OBIM HART sends system responses to USCIS. • Action 5: If a match is not found in OBIM HART, the system creates a new identity with USCIS encounter. If a match is found to an existing identity, OBIM HART associates a USCIS encounter to that identity.
Alternate Scenario Description	• No alternate scenario.
Post-Conditions	• USCIS encounter with submitted biometrics is created in OBIM HART.

Six Components, Seven Relationships

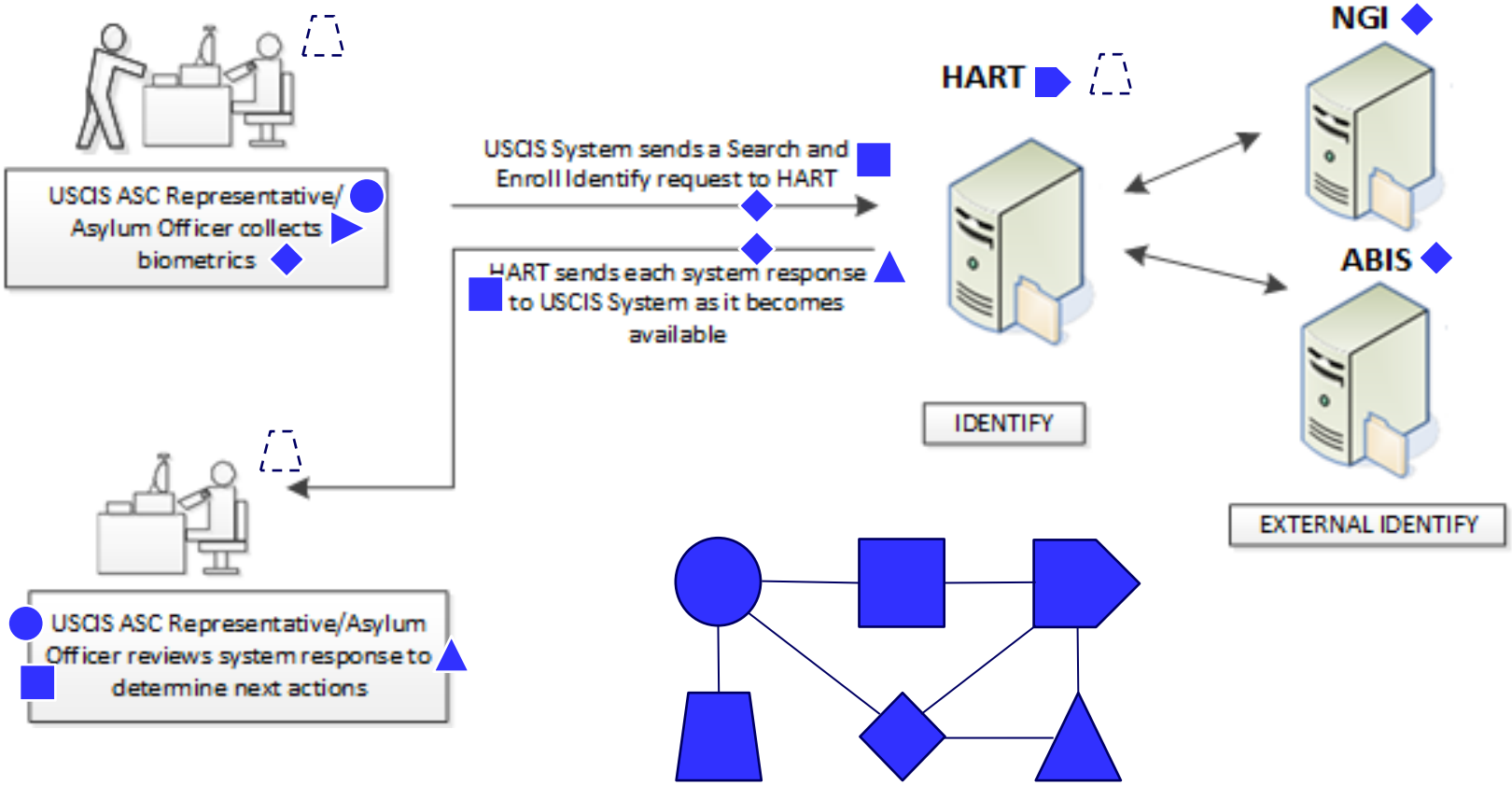


Homeland Security
Science and Technology

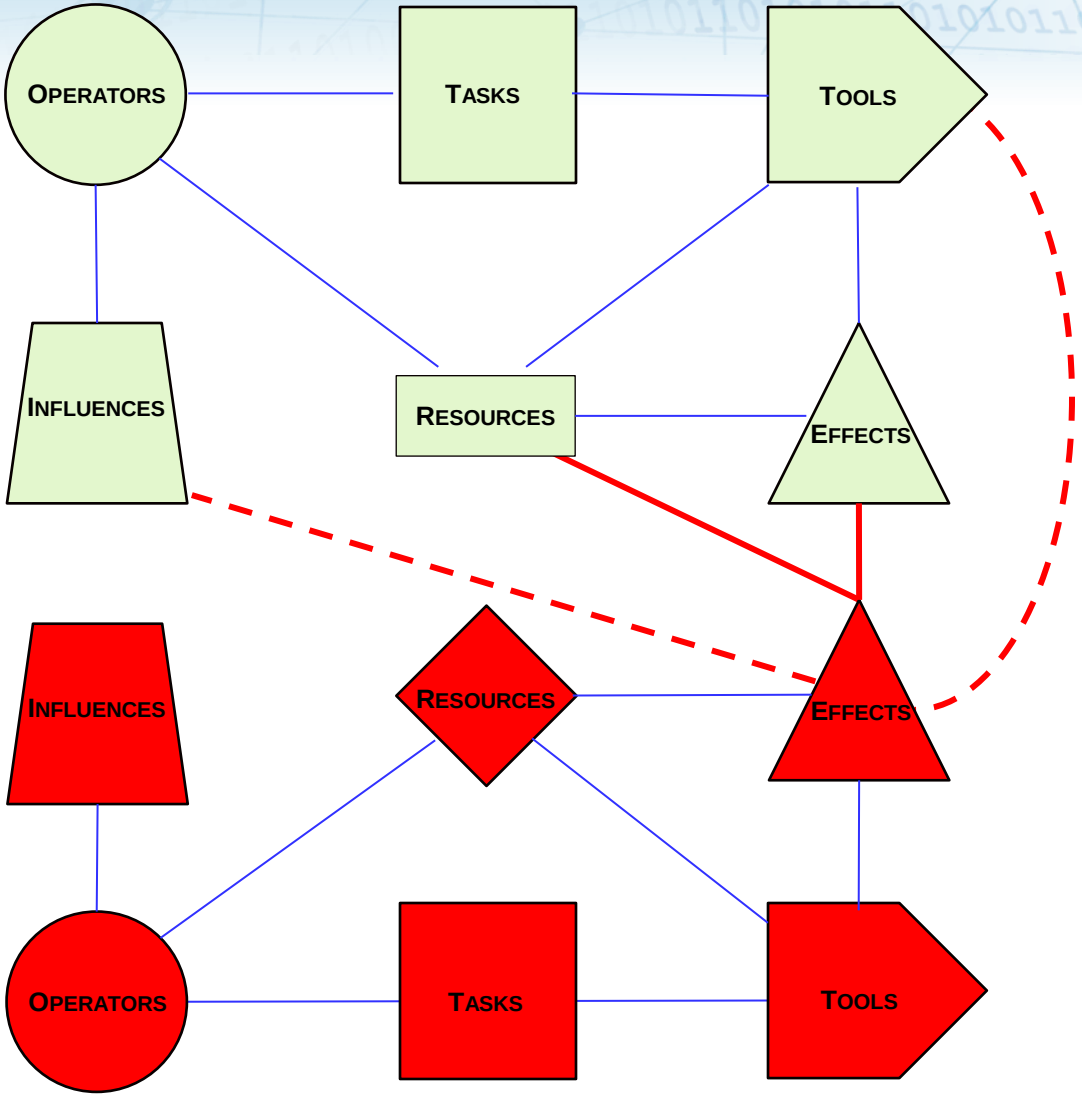
Customer Use Case Example (cont'd)

Homeland Advanced Recognition Technology (Use Case)

USCIS Biometric Enrollment with External Search (ASC and Asylum)



Adversarial Operational Ontology



Threat Assessment

- Them
  - Intent – Threat to the mission
  - Actors – Those with intent
  - Capabilities – Resources available to actors
- Us
  - Key Cyber Terrain – Capability's assets
  - Attack Surface – Accesses to assets
- Them & Us
  - Kill Chain – Adversarial activity model

Intent

- Denial – Blocking completion of mission tasks.
- Degradation – Decreasing the speed, quality, or other performance characteristics for mission tasks.
- Manipulation – Altering the information available to decision makers.
- Exfiltration – Gaining information about mission details to be exploited against other assets.
- Pivot – Using access to one system/network to gain access to a partner system/network.

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.

Abridged Example

Next Generation Government Emergency Telephone System (TEMP)

Hazard Event	Frequency	Infrastructure Physical Damage (repairable)	Infrastructure Power Cut (physical break)	Infrastructure Power Loss(no physical damage, no power)	Infrastructure Loss(must be replaced)	Congestion
Pandemic	L	Unlikely - Light	Unlikely – Light	Unlikely - Light	Unlikely - Light	Unlikely - severe
Theater Cyber War	L	Unlikely - Light	Moderate - Moderate	Moderate - Moderate	Unlikely - Light	Likely - significant
Electromagnetic Flux	Moderate (M)	Moderate - moderate	Unlikely – Light	Likely - Moderate	Unlikely - Light	Unlikely - severe
Strategic Cable Cut	M	Likely - light	Unlikely – Light	Unlikely - Light	Likely - Light	Unlikely - Very Light
Special Operations	M	Unlikely - Light	Unlikely – Light	Unlikely - Light	Unlikely - Light	Unlikely - Very Light
Terrorism (includes Cyber)	M	Moderate - Moderate	Unlikely – Light	Moderate - Moderate	Moderate - Moderate	Likely - significant
Civil Disorder	M	Unlikely - Light	Unlikely – Light	Unlikely - Light	Unlikely - Light	Likely - Moderate
Hurricanes	Very High (VH)	Likely - Significant	Likely - Significant	Likely - Severe	Likely - Moderate	Unlikely - Moderate
Power Outage	VH	likely - light	Likely - Moderate	Likely - Moderate	Unlikely - Light	Unlikely - Very Light
Cable cut	VH	likely - light	Unlikely – Light	Unlikely - Light	Unlikely - Light	Unlikely - Very Light
KEY	Frequency: • VL- 1/100+ years • Low 1/10 years • M 1/2.5 years • H 1/year • VH <1/year				Congestion: • Severe - widespread/national • Significant - region • Moderate - multiple locals jurisdictions • Light - single local jurisdiction • Very Light - w/I 1 mile of event site	

Homeland Security
Science and Technology

Threat Description Example

Next Generation Government Emergency Telephone System (TEMP)

- Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example

Next Generation Government Emergency Telephone System (TEMP)

- Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example

Next Generation Government Emergency Telephone System (TEMP)

- Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Threat Description Example

Next Generation Government Emergency Telephone System (TEMP)

- Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

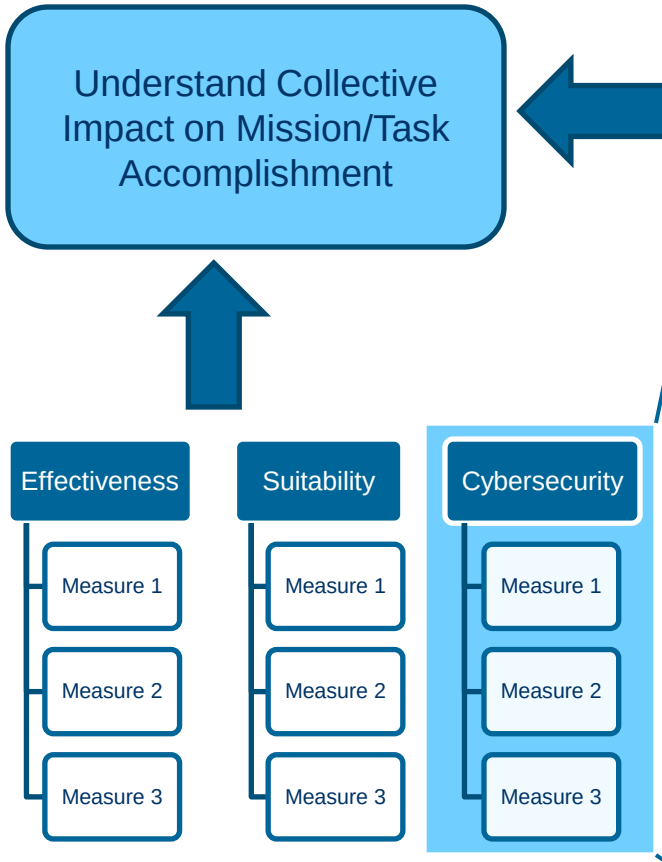
Threat Description Example

Next Generation Government Emergency Telephone System (TEMP)

- Special Operations: Such a threat could consist of a DoS attack or RF jamming of one or more cell sites to bar WPS/GETS users in a limited geographic area or to only one of the WPS/GETS service providers. This action could be undertaken to potentially compliment a kinetic terrorist attack (e.g., bomb) with the goal of disabling NS/EP wireless (and potentially wireline) services in a given area on one or more service providers to enhance or increase the impact or disruption of the primary attack. However, NS/EP users in such an area of attack will most likely be subscribed to different WPS/GETS providers and therefore not all NS/EP users in the area of attack may be barred from WPS/GETS services or only WPS services on one service provider may be disrupted depending on their multiple frequency resources, area of attack (e.g., urban, suburban, rural), and deployment/density of infrastructure (e.g., small cells). As a result, such an event could be more moderate in frequency but only have the ability to congest a small area around the attack on the order of a mile or so.

Homeland Security
Science and Technology

Sample Cybersecurity Evaluation Structure



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

Mapping

		Operational Tasks					
		Mission Area 1			Mission Area 2		
		Task A	Task B1	Task B2	Task A	Task B	Task C
Effectiveness	Performance						
	Interoperability						
Suitability	Availability						
	Throughput						
	Usability						
Security	Denial						
	Degradation						
	Manipulation						
	Exfiltration						
	Pivoting						

Conditions

		Operational Tasks					
		Mission Area 1			Mission Area 2		
		Task A	Task B1	Task B2	Task A	Task B	Task C
Effectiveness	Performance						
	Interoperability						
Suitability	Availability						
	Throughput						
	Usability						
Security	Denial						
	Degradation						
	Manipulation						
	Exfiltration						
	Pivoting						

Conditions

		Operational Tasks									
		Mission Area 1						Mission Area 2			
		Task A		Task B1	Task B2			Task A	Task B		Task C	
		α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance											
	Interoperability											
Suitability	Availability											
	Throughput											
	Usability											
Security	Denial											
	Degradation											
	Manipulation											
	Exfiltration											
	Pivoting											

Modes

		Operational Tasks										
		Mission Area 1						Mission Area 2				
		Task A		Task B1	Task B2			Task A	Task B		Task C	
		α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance ?											
	Interoperability ?											
Suitability	Availability											
	Throughput											
	Usability											
Security	Denial											
	Degradation											
	Manipulation											
	Exfiltration											
	Pivoting											

Modes

			Operational Tasks										
			Mission Area 1						Mission Area 2				
			Task A		Task B1	Task B2			Task A	Task B		Task C	
			α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance	2											
		1											
	Interoperability	C											
		B											
		A											
Suitability	Availability												
	Throughput												
	Usability												
Security	Denial												
	Degradation												
	Manipulation												
	Exfiltration												
	Pivoting												

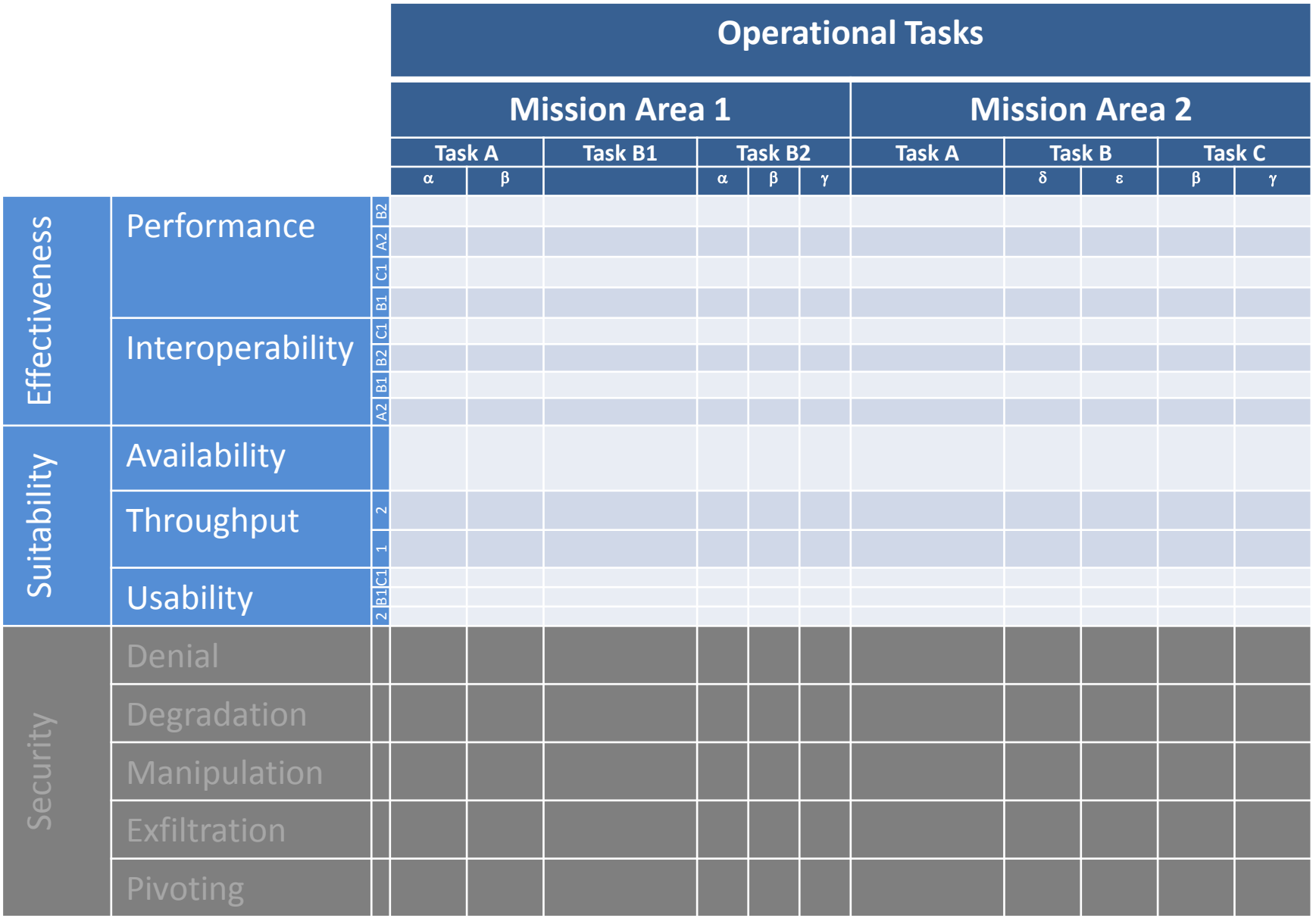
Full Factorial Product

			Operational Tasks										
			Mission Area 1						Mission Area 2				
			Task A		Task B1	Task B2			Task A	Task B		Task C	
			α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance	C2											
		B2											
		A2											
		C1											
		B1											
		A1											
	Interoperability	C2											
		C1											
		B2											
		B1											
		A2											
		A1											
Suitability	Availability												
	Throughput												
	Usability												
Security	Denial												
	Degradation												
	Manipulation												
	Exfiltration												
	Pivoting												

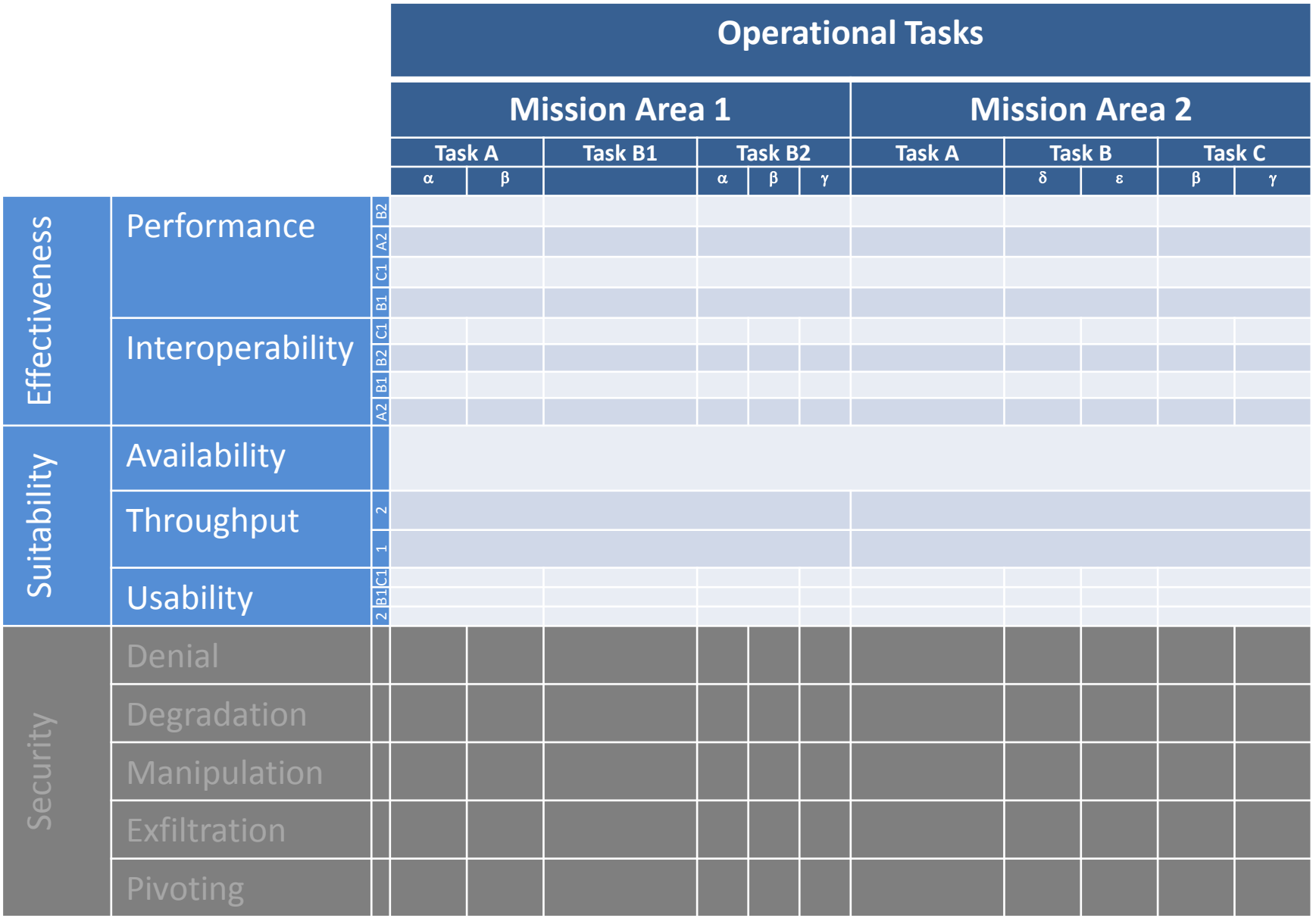
Collection

			Operational Tasks										
			Mission Area 1						Mission Area 2				
			Task A		Task B1	Task B2			Task A	Task B		Task C	
			α	β		α	β	γ		δ	ε	β	γ
Effectiveness	Performance	B2											
		A2											
		C1											
		B1											
	Interoperability	C1											
		B2											
		B1											
		A2											
Suitability	Availability												
	Throughput												
	Usability												
Security	Denial												
	Degradation												
	Manipulation												
	Exfiltration												
	Pivoting												

Assignment


Operational Tasks
Mission Area 1
Mission Area 2
Task A
Task B1
Task B2
Task A
Task B
Task C
α
β
α
β
γ
δ
ε
β
γ
Effectiveness
Performance
Interoperability
Suitability
Availability
Throughput
Usability
Security
Denial
Degradation
Manipulation
Exfiltration
Pivoting

Collapsing


Operational Tasks
Mission Area 1
Mission Area 2
Task A
Task B1
Task B2
Task A
Task B
Task C
α
β
α
β
γ
δ
ε
β
γ
Effectiveness
Performance
Interoperability
Suitability
Availability
Throughput
Usability
Security
Denial
Degradation
Manipulation
Exfiltration
Pivoting
B2
A2
C1
B1
C1
B2
B1
A2
2
1
C1
B1
2

Contact Information

Alex Hoover

Test Area Manager

Cyberspace & Homeland Security Enterprise Programs

202-254-5615

alex.hoover@hq.dhs.gov

Homeland Security

Science and Technology