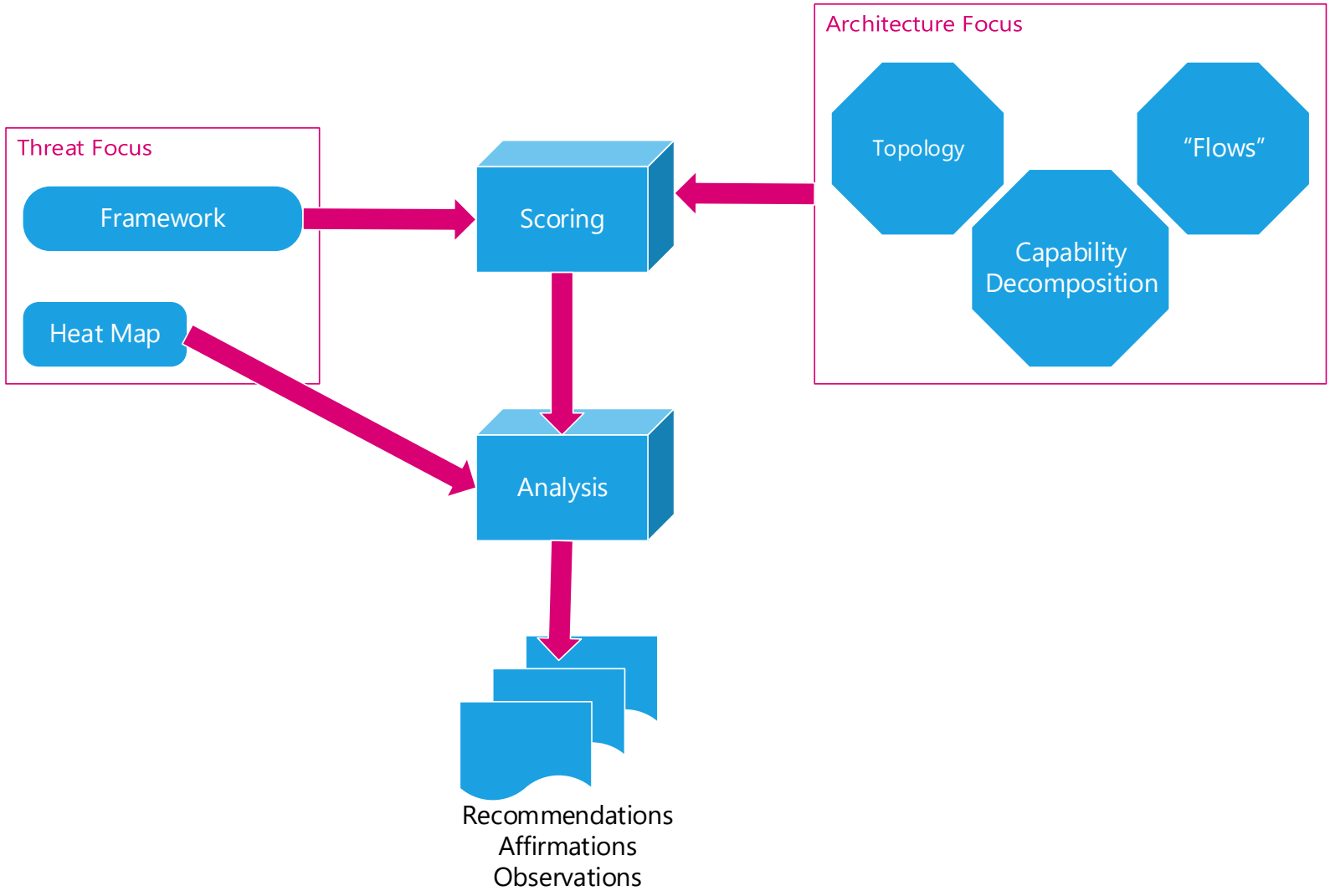
Architecture, Flows, and Capabilities for .govCAR Spin 5 (Mobile)

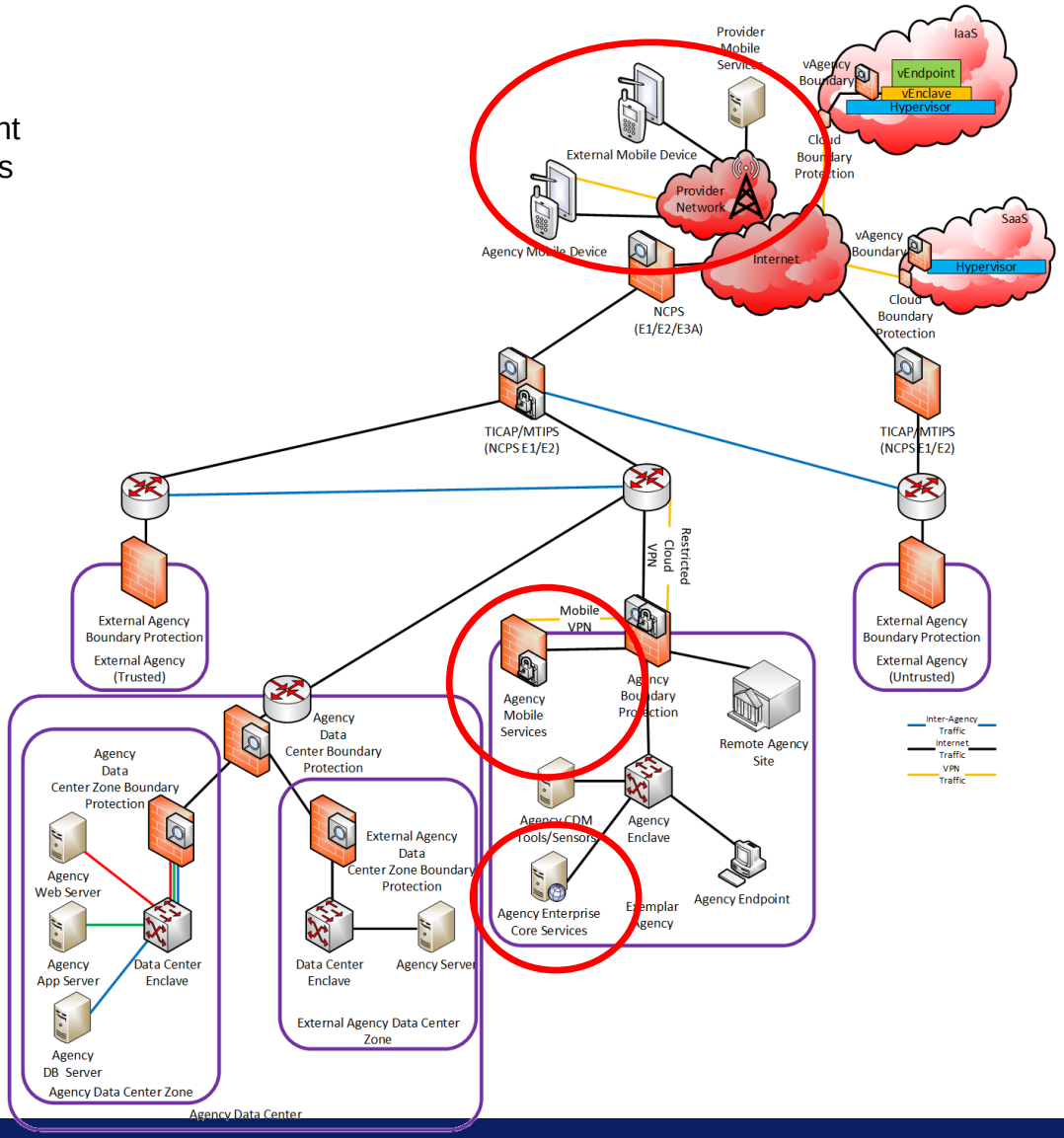
Aug 2018

.govCAR Methodology

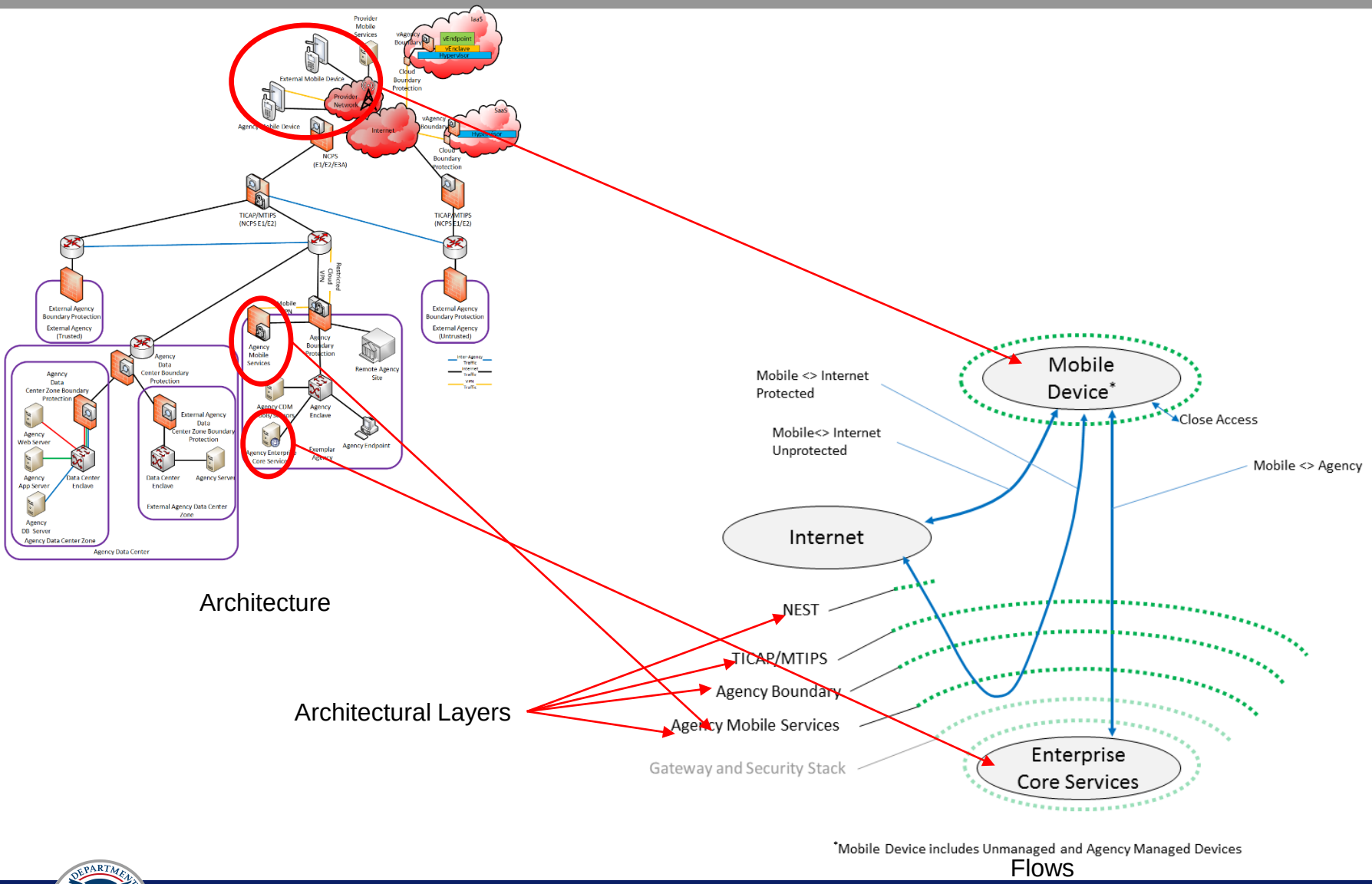


Spin 5 Architecture View

SPIN 1 = Einstein, TIC, related network services
SPIN 2 = Exemplar Agency Endpoint environment
SPIN 3 = Cloud (IaaS and SaaS) basic structures
SPIN 4 = Exemplar Agency Data Center
SPIN 5 = Mobile



Architecture and Flows Relationship



Agency Mobile Device to Internet (Protected) Capabilities

Current

NCPS/EINSTEIN:
E1 Collector & Analytics
E2 Flow, IDS, PCAP, SIEM
E3A IPS (SMTP & DNS)

E3A DGA Analytic
E3A EXE-MANA

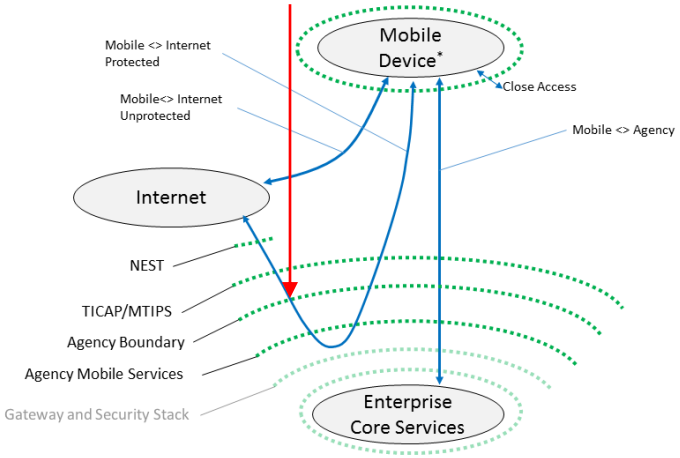
TICAP/MTIPS:
FW
Passive Sensor
WCF
Ib/Ob SMTP Proxy
Recursive DNS Proxy
Auth DNS Proxy

Agency Boundary:
NGFW
Passive Sensor
WCF
Ib/Ob SMTP Proxy
Recursive DNS Proxy
Auth DNS Proxy

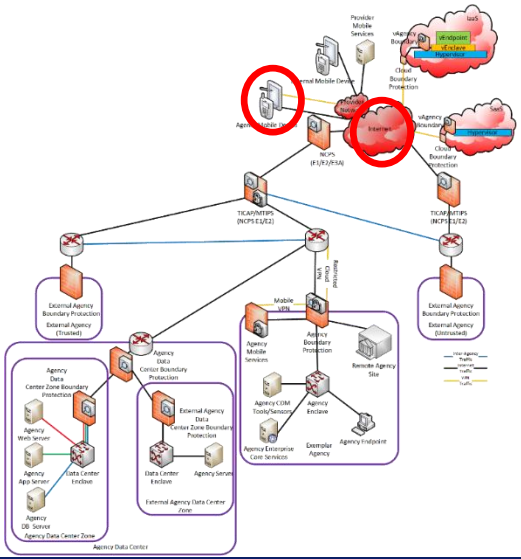
Agency Mobile Services:
MDM
MAM VPN

MIM DLP

Agency Mobile Device:
Container
App Wrapping



*Mobile Device includes Unmanaged and Agency Managed Devices



Planned

NCPS/EINSTEIN:
E1 Collector & Analytics
E2 Flow, IDS, PCAP, SIEM
E3A IPS (SMTP & DNS)
E3A IPS (WCF)
E3A DGA Analytic
E3A EXE-MANA Enh Analytic
E3A APT Detections Analytic

TICAP/MTIPS:
FW Enh
Passive Sensor
WCF Enh
Ib/Ob SMTP Proxy Enh
Recursive DNS Proxy
Auth DNS Proxy Enh

Agency Boundary:
NGFW
Passive Sensor
WCF Enh
Ib/Ob SMTP Proxy Enh
Recursive DNS Proxy
Auth DNS Proxy Enh

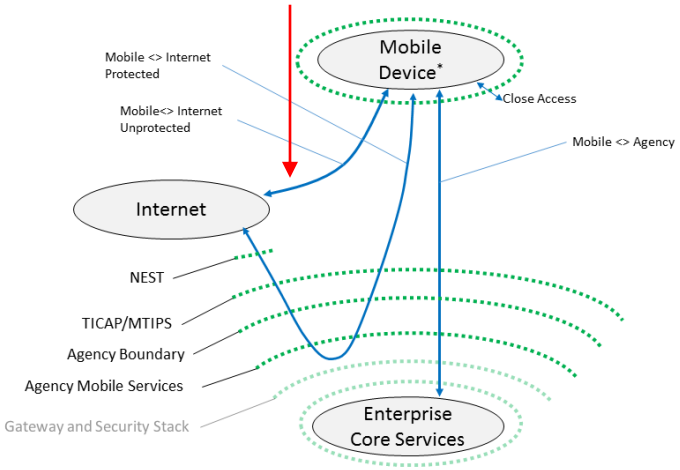
Agency Mobile Services:
MDM IDS
MAM Enh MTD VPN
MAV
MIM DLP

Agency Mobile Device:
Container
App Wrapping
TPM

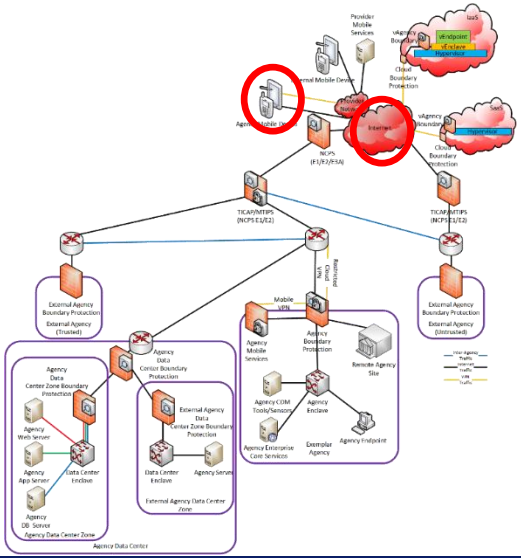
UNCLASSIFIED

Agency Mobile Device to Internet (UnProtected) Capabilities

Current



*Mobile Device includes Unmanaged and Agency Managed Devices



Planned

Agency Mobile Services:
MDM
MAM VPN

MIM DLP

Agency Mobile Device:
Container
App Wrapping

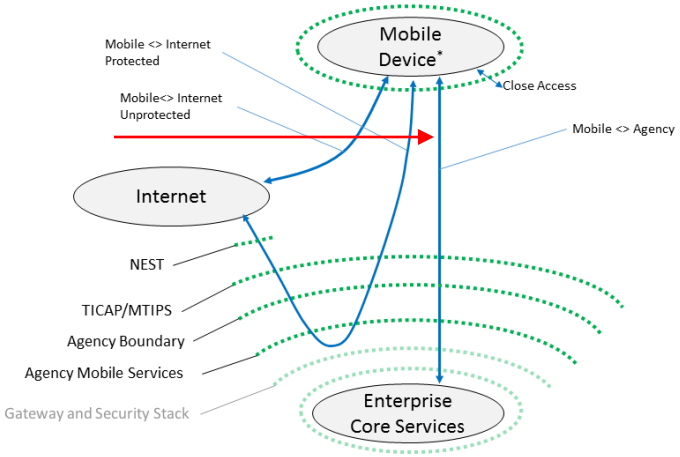
Agency Mobile Services:
MDM IDS
MAM Enh MTD VPN
MAV
MIM DLP

Agency Mobile Device:
Container
App Wrapping
TPM

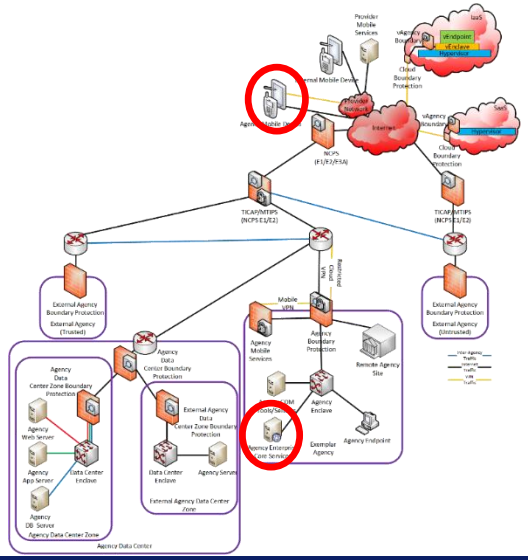
Agency Mobile Device to Agency Capabilities

Current

Planned



*Mobile Device includes Unmanaged and Agency Managed Devices



TICAP/MTIPS:
FW
Passive Sensor

Agency Boundary:
NGFW
Passive Sensor

Agency Mobile Services:
MDM
MAM VPN
MIM DLP

Agency Mobile Device:
Container
App Wrapping

TICAP/MTIPS:
FW Enh
Passive Sensor

Agency Boundary:
NGFW
Passive Sensor

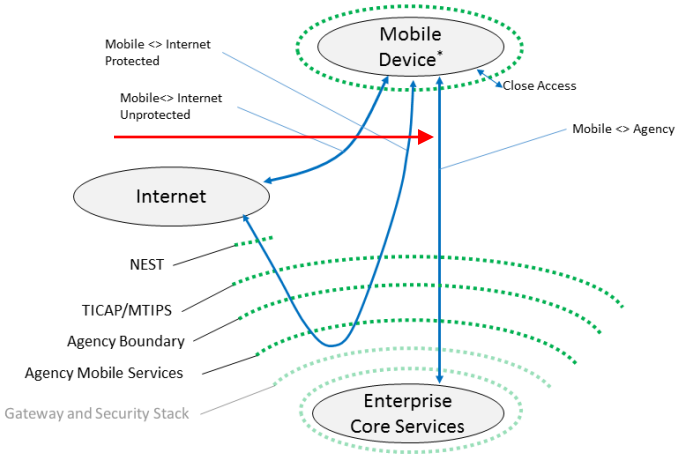
Agency Mobile Services:
MDM IDS
MAM Enh MTD VPN
MAV
MIM DLP

Agency Mobile Device:
Container
App Wrapping
TPM

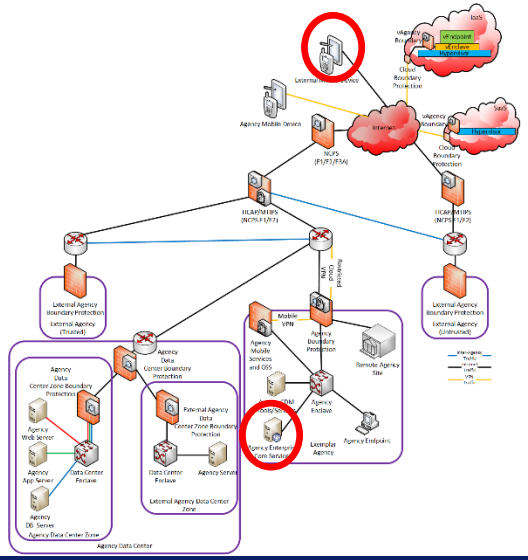
External Mobile Device to Agency Capabilities

Current

Planned



*Mobile Device includes Unmanaged and Agency Managed Devices



TICAP/MTIPS:
FW
Passive Sensor

Agency Boundary:
NGFW
Passive Sensor

Agency Mobile Services:
MDM
MAM

MIM DLP

Agency Mobile Device:
Container
App Wrapping

TICAP/MTIPS:
FW Enh
Passive Sensor

Agency Boundary:
NGFW
Passive Sensor

Agency Mobile Services:
MDM IDS
MAM Enh
MAV
MIM DLP

Agency Mobile Device:
Container
App Wrapping

.govCAR Process [Threat Framework]

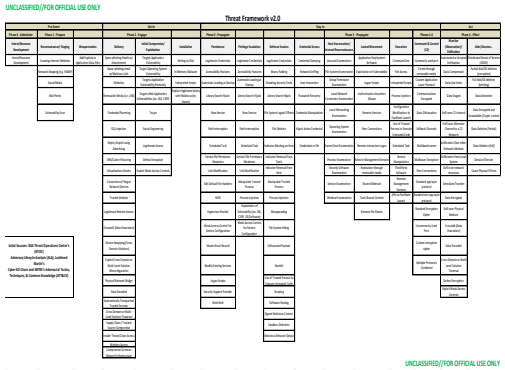
Cyber Threat Framework

STAGES
The progression of cyber threats over time to achieve objectives

OBJECTIVES
The purpose of conducting an action or a series of actions

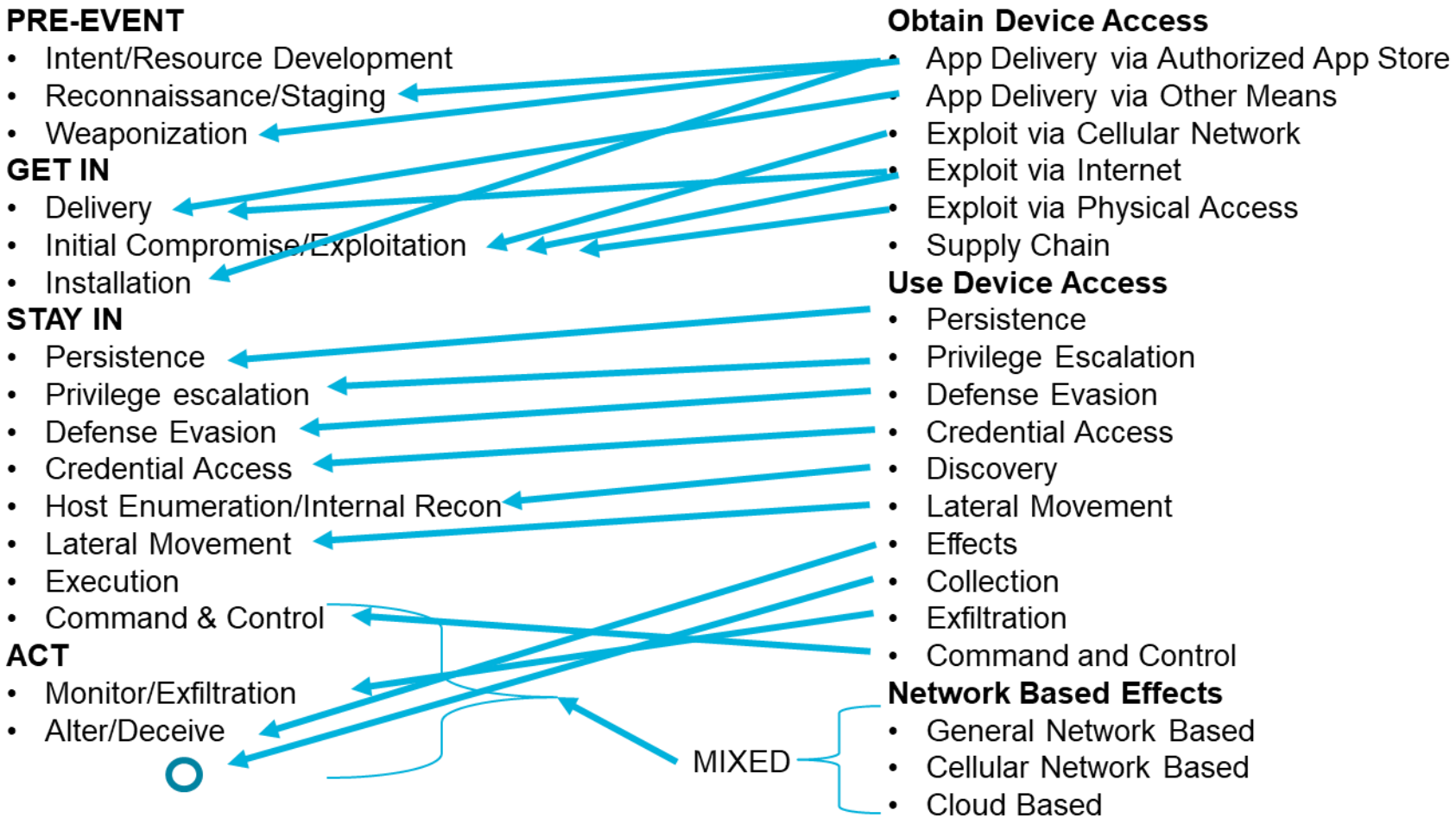
ACTIONS
Actions and associated resources used by a threat actor to satisfy an objective

Pre-event	Get-in	Stay-In	Act
Intent/Resource Development 1	Delivery 23	Persistance 18	Monitor/ Exfiltration 17
Reconnaissance/ staging 5	Initial Compromise/ Exploitation 9	Privilege Escalation 13	Alter/Deceive 9
Weaponize 1	Installation 4	Defense Evasion 21	
		Credential Access 7	
		Host enumeration/ Internal Recon 11	
		Lateral Movement 12	
		Execution 11	
		Command & Control 15	



Set of Threat Actions requiring counteraction by Protect / Detect / Respond

Mapping ATT&CK Mobile to NSA 2.0 Structure



ATT&CK Mobile in *CAR Structure

Pre-Event			Get In			Stay In								Act		
Intent/Resource Development	Reconnaissance/ Staging	Weaponization	Delivery	Initial Compromise/ Exploitation	Installation	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration/ Internal Reconnaissance	Lateral Movement	Execution	Command & Control (C2)	Collection	Monitor (Observation)/ Exfiltration	Alter/Deceive…
App Delivery via Authorized App Store: Fake Developer Accounts	App Delivery via Authorized App Store: Stolen Developer Credentials or Signing Keys	App Delivery via Authorized App Store: Detect App Analysis Environment	App Delivery via Other Means: App Delivered via Email Attachment	Exploit via Physical Access: Biometric Spoofing	App Delivery via Other Means: Abuse of iOS Enterprise App Signing Key	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Abuse Accessibility Features	Application Discovery	Attack PC via USB Connection		Alternate Network Mediums	Abuse Accessibility Features	Alternate Network Mediums	Encrypt Files for Ransom
		App Delivery via Authorized App Store: Repackaged Application	App Delivery via Other Means: App Delivered via Web Download	Exploit via Physical Access: Device Unlock Code Guessing or Brute Force	App Delivery via Authorized App Store: Remotely Install Application	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Disguise Root/Jailbreak Indicators	Access Sensitive Data in Device Logs	Device Type Discovery	Exploit Enterprise Resources		Commonly Used Port	Access Calendar Entries	Commonly Used Port	Generate Fraudulent Advertising Revenue
		Supply Chain: Malicious Software Development Tools	App Delivery via Other Means: Repackaged Application	Exploit via Physical Access: Lockscreen Bypass		Modify OS Kernel or Boot Partition		Download New Code at Runtime	Access Sensitive Data or Credentials in Files	File and Directory Discovery			Standard Application Layer Protocol	Access Call Log	Standard Application Layer Protocol	Lock User Out of Device
			Exploit via Internet: Malicious Media Content	Exploit via Internet: Malicious Media Content		Modify System Partition		Modify OS Kernel or Boot Partition	Android Intent Hijacking	Local Network Configuration Discovery				Access Contact List		Manipulate App Store Rankings or Ratings
			Exploit via Internet: Malicious Web Content	Exploit via Internet: Malicious Web Content		Modify Trusted Execution Environment		Modify System Partition	Capture Clipboard Data	Local Network Connections Discovery				Access Sensitive Data in Device Logs		Premium SMS Toll Fraud
			Supply Chain: Insecure Third-Party Libraries	Supply Chain: Insecure Third-Party Libraries		Modify cached executable code		Modify Trusted Execution Environment	Capture SMS Messages	Network Service Scanning				Access Sensitive Data or Credentials in Files		Wipe Device Data
			Supply Chain: Malicious or Vulnerable Built-in Device Functionality	Supply Chain: Malicious or Vulnerable Built-in Device Functionality				Obfuscated or Encrypted Payload	Exploit TEE Vulnerability	Process Discovery				Capture Clipboard Data		General Network-Based: Jamming or Denial of Service
			Exploit via Cellular Network: Exploit Baseband Vulnerability	Exploit via Cellular Network: Exploit Baseband Vulnerability					Malicious Third Party Keyboard App	System Information Discovery				Capture SMS Messages		General Network-Based: Manipulate Device Communication
			Exploit via Cellular Network: Malicious SMS Message	Exploit via Cellular Network: Malicious SMS Message					Network Traffic Capture or Redirection					Location Tracking		General Network-Based: Rogue Wi-Fi Access Points
			Exploit via Physical Access: Exploit via Charging Station or PC	Exploit via Physical Access: Exploit via Charging Station or PC					URL Scheme Hijacking					Malicious Third Party Keyboard App		Cellular network-Based: Jamming or Denial of Service
				Cellular network-Based: Exploit SS7 to Redirect Phone Calls/SMS					User Interface Spoofing					Microphone or Camera Recordings		Cloud-Based: Remotely Wipe Data Without Authorization
				Cellular network-Based: Exploit SS7 to Track Device Location										Network Traffic Capture or Redirection		
				Cellular network-Based: SIM Card Swap										General Network-Based: Eavesdrop on Insecure Network Communication		
				General Network-Based: Downgrade to Insecure Protocols										Cellular network-Based: Rogue Cellular Base Station		
				Cellular Network-Based: Downgrade to Insecure Protocols										Cloud-Based: Obtain Device Cloud Backups		
														Cloud-Based: Remotely Track Device Without Authorization		

Initial Sources:
*** MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)**

100+ Threat Actions