

**govCAR**  
*think like the adversary*

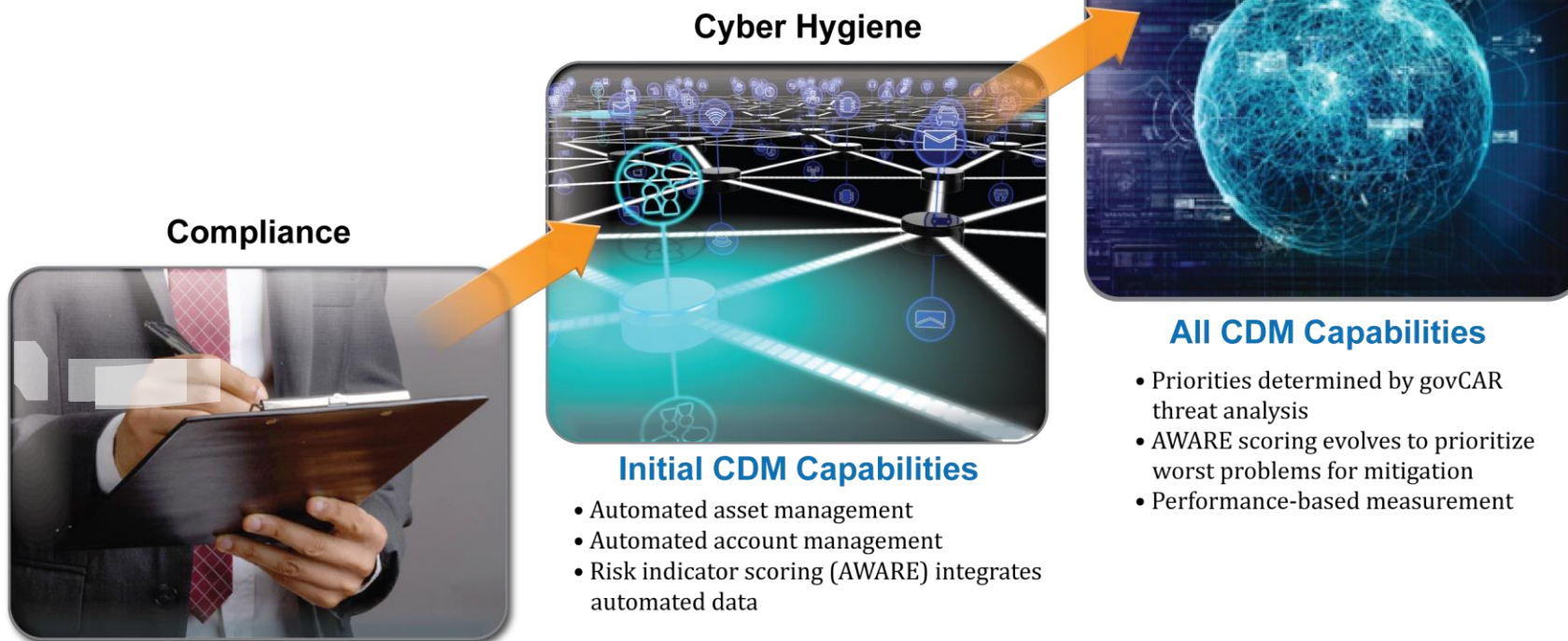


**CISA**  
CYBER+INFRASTRUCTURE



# Move to Stronger Risk Management

## From Compliance to Threat-Based Risk Management



### Pre-CDM

- Manual FISMA compliance
- Yes/no responses are simplistic
- Risk determination based on checklist

$$\text{Risk} = \text{Consequence} \times \text{Vulnerability} \times \text{Threat}$$



**CISA**  
CYBER+INFRASTRUCTURE



# About

- .govCAR methodology provides threat-based assessment of cyber capabilities
- looks at the problem of cyber security the way an adversary does
- directly identifies where mitigations can be applied for the best defense against all phases of a cyber-attack.
- designed to enhance cybersecurity by analyzing capabilities against the current cyber threats to highlight gaps, and identify and prioritize areas for future investments.
- parallels DoD project known as DoDCAR (previously NSCSAR), which introduced the concept of a threat-based, end-to-end analysis of large, enterprise cybersecurity architectures and is used to provide direction and justification for cybersecurity





# Why .govCAR?

- Evaluate architectures of architectures (layered architecture)
- Are my current cyber security capabilities protecting me against threats? If not, where are the gaps?
- Support investment direction and decisions especially at the portfolio level. Am I investing my cyber security budget wisely? What should my next investment be?
- Is there unwanted duplication of security functionality?
- Can evaluate people, policy and process capabilities, but has been primarily used for technology (materiel) evaluation





# Anatomy of a cyber attack

Administration

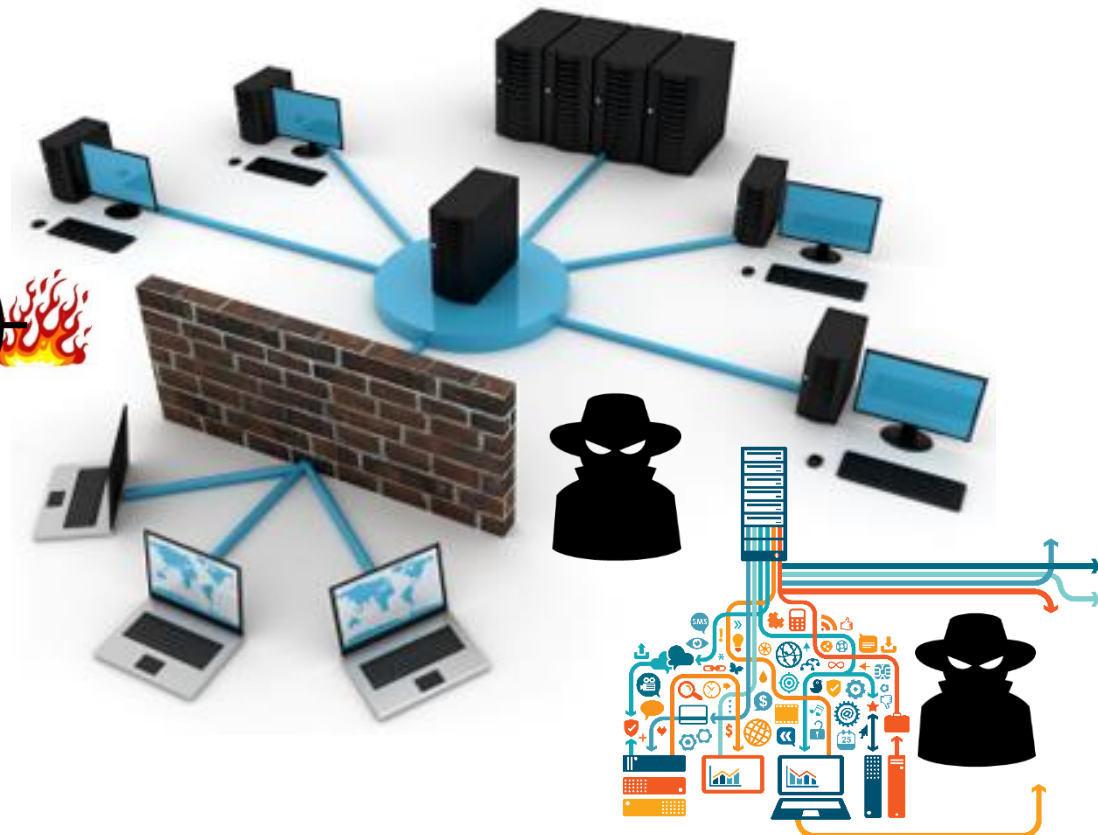
Preparation

Engagement

Presence

Effect

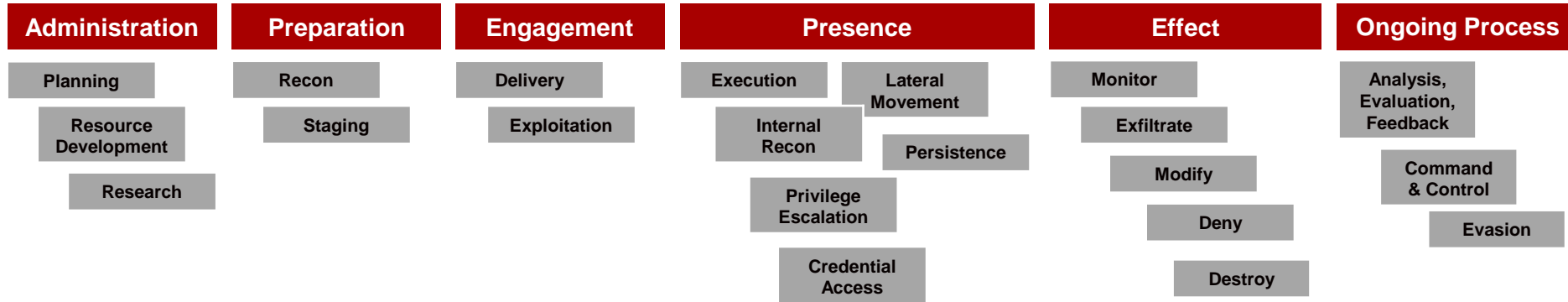
Ongoing Process



**CISA**  
CYBER+INFRASTRUCTURE



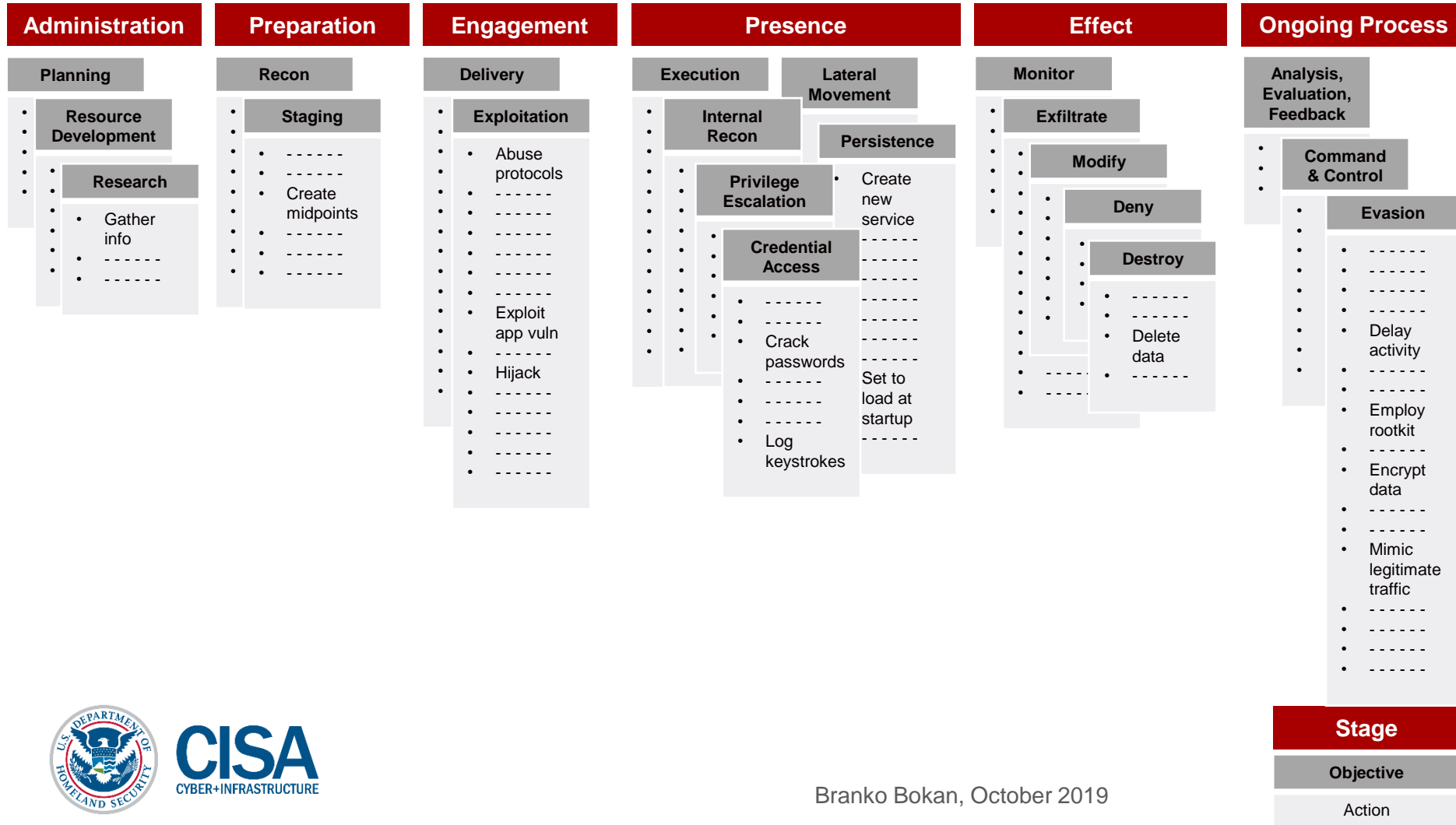
# Stages and Objectives



**CISA**  
CYBER+INFRASTRUCTURE



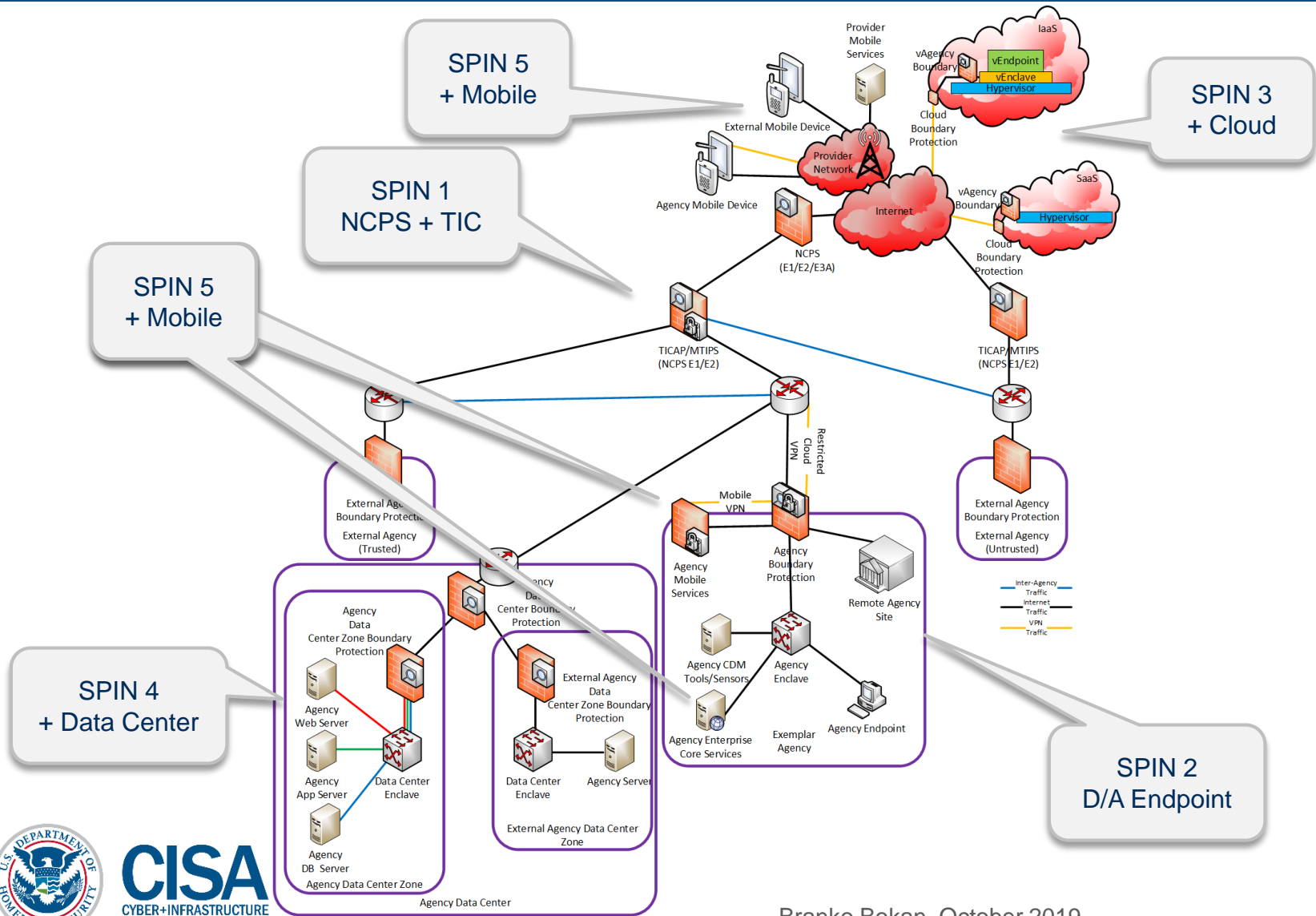
# Threat actions



**CISA**  
CYBER+INFRASTRUCTURE



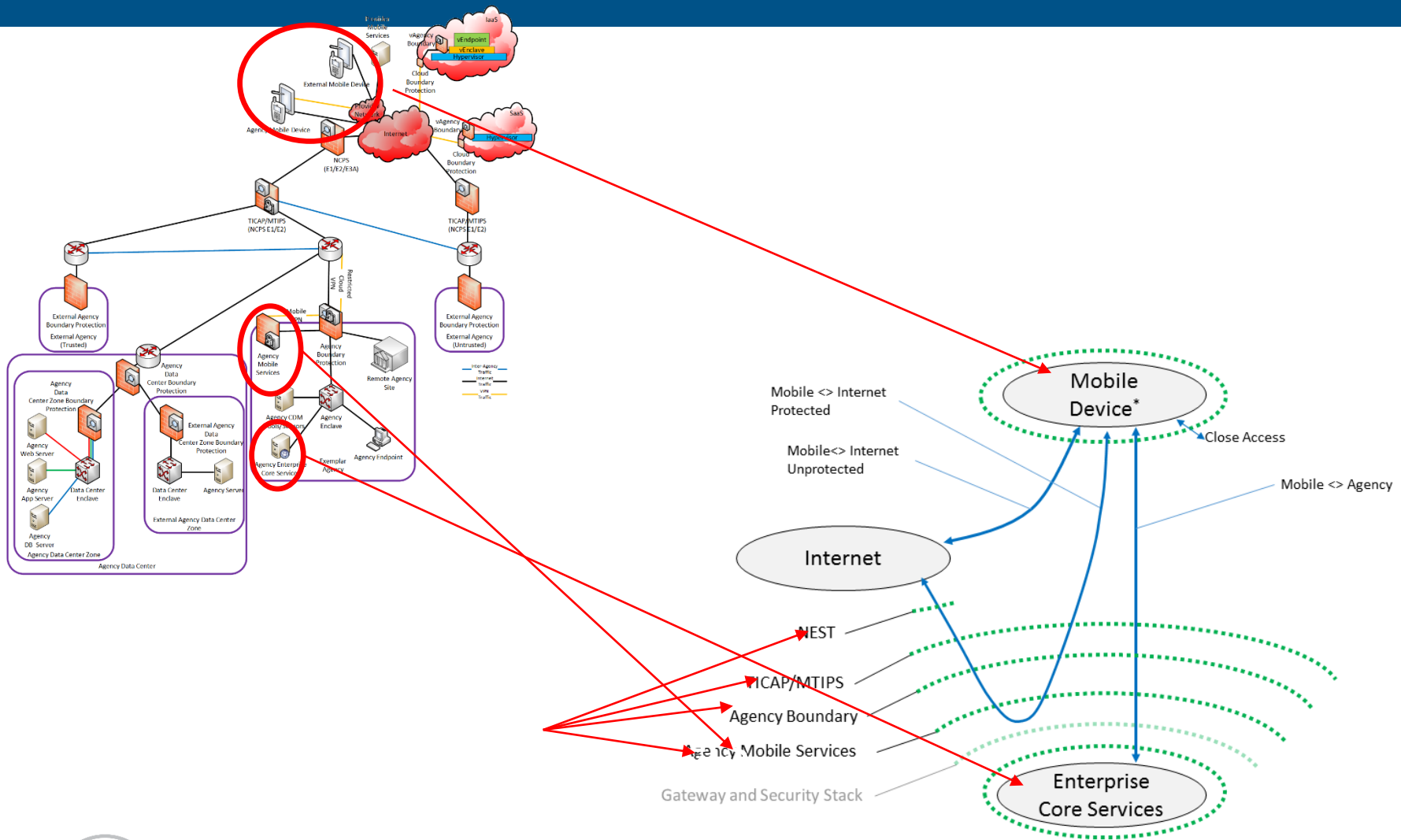
# Spin 1-5 Architecture View



**CISA**  
CYBER+INFRASTRUCTURE



# Architectures and Flows



**CISA**  
CYBER+INFRASTRUCTURE

\*Mobile Device includes Unmanaged and Managed Devices



# Scoring

govCAR Mitigation Draft Scoring Sheet				Stage					
				Objective					
				Threat Action Y			Threat Action		
				Protect	Detect	Respond	Protect	Detect	Respond
				Threat Action Description			Threat Action Description		
Capabilities	Detailed Capability Description	Enh	% Scores Done						
Layer1	To create new Capabilities, select the entire row of an	Is Enhanc	% Scoring Comple						
A	Description			M	M	S	None	None	L
Rationale				P/D has some allowed paths. All actions are logged			Threat action is permitted but logged. Logs only persist 1 week		
Layer2									
B	Description			N/A	N/A	N/A	L	L	L
Rationale			0%				only covers one possible vector		
B (Enhancement)	Description			N/A	N/A	N/A	M	M	M
Rationale			0%				coverage include additional but not all vectors		

Security Capabilities for as-implemented, as-funded, and as-recommended architecture configurations

Logical Groupings of Capabilities by Tier

Threat 'Actions' From the Framework

NIST CyberSecurity Framework Mitigation Functions

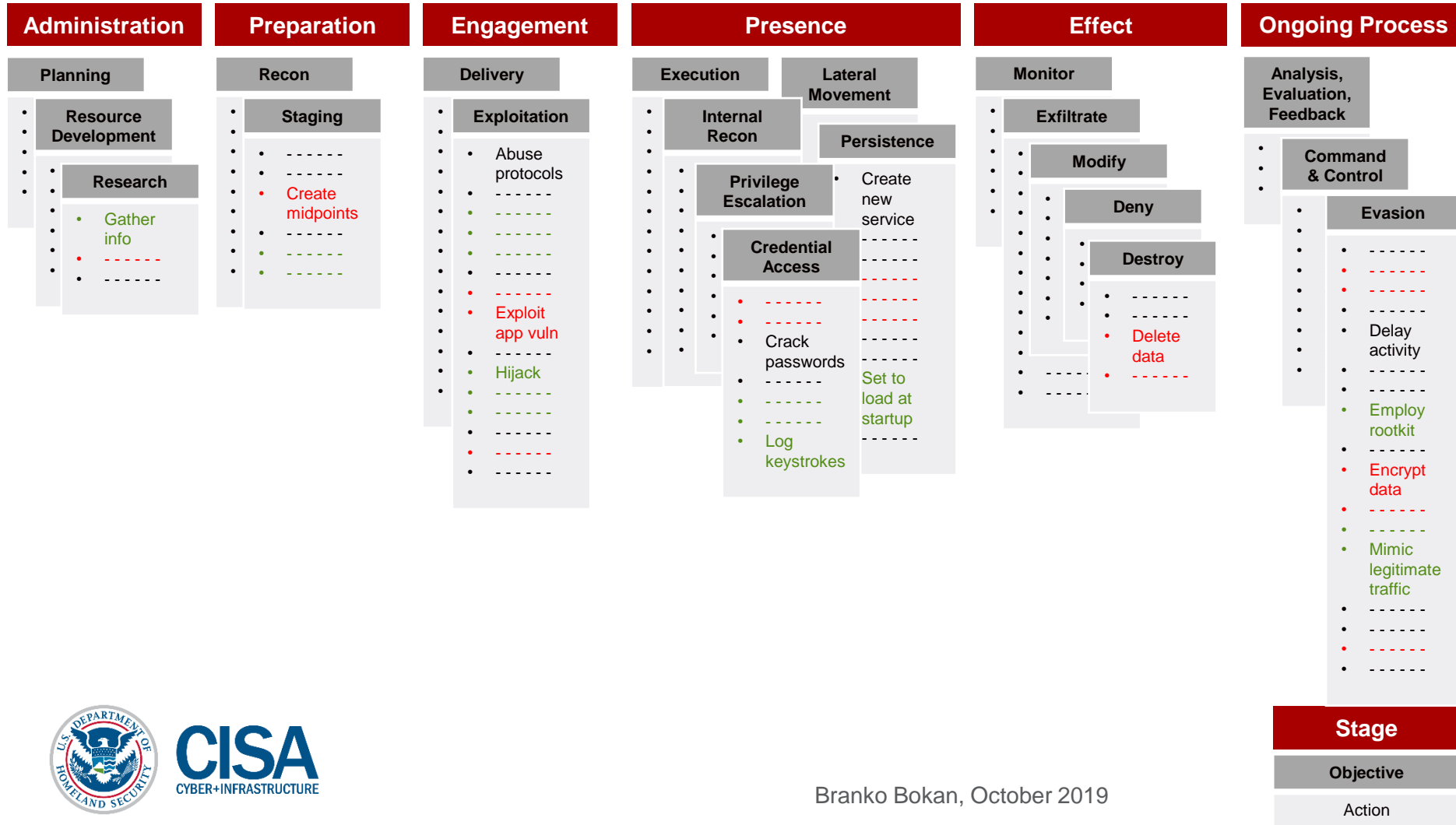
SME Scoring: Significant Moderate Limited



**CISA**  
CYBER+INFRASTRUCTURE



# Coverage mapping



**CISA**  
CYBER+INFRASTRUCTURE



# Threat heat mapping

Stay In			
Defense Evasion	Credential Access	Host Enumeration/Internal Reconnaissance	Lateral Movement
Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software
6.2	12.2	6.4	1.5
Binary Padding	Network Sniffing	File System Enumeration	Exploitation of Vulnerability
2.0	1.6	8.0	2.6
Disabling Security Tools	User Interaction	Group Permission Enumeration	Logon Scripts

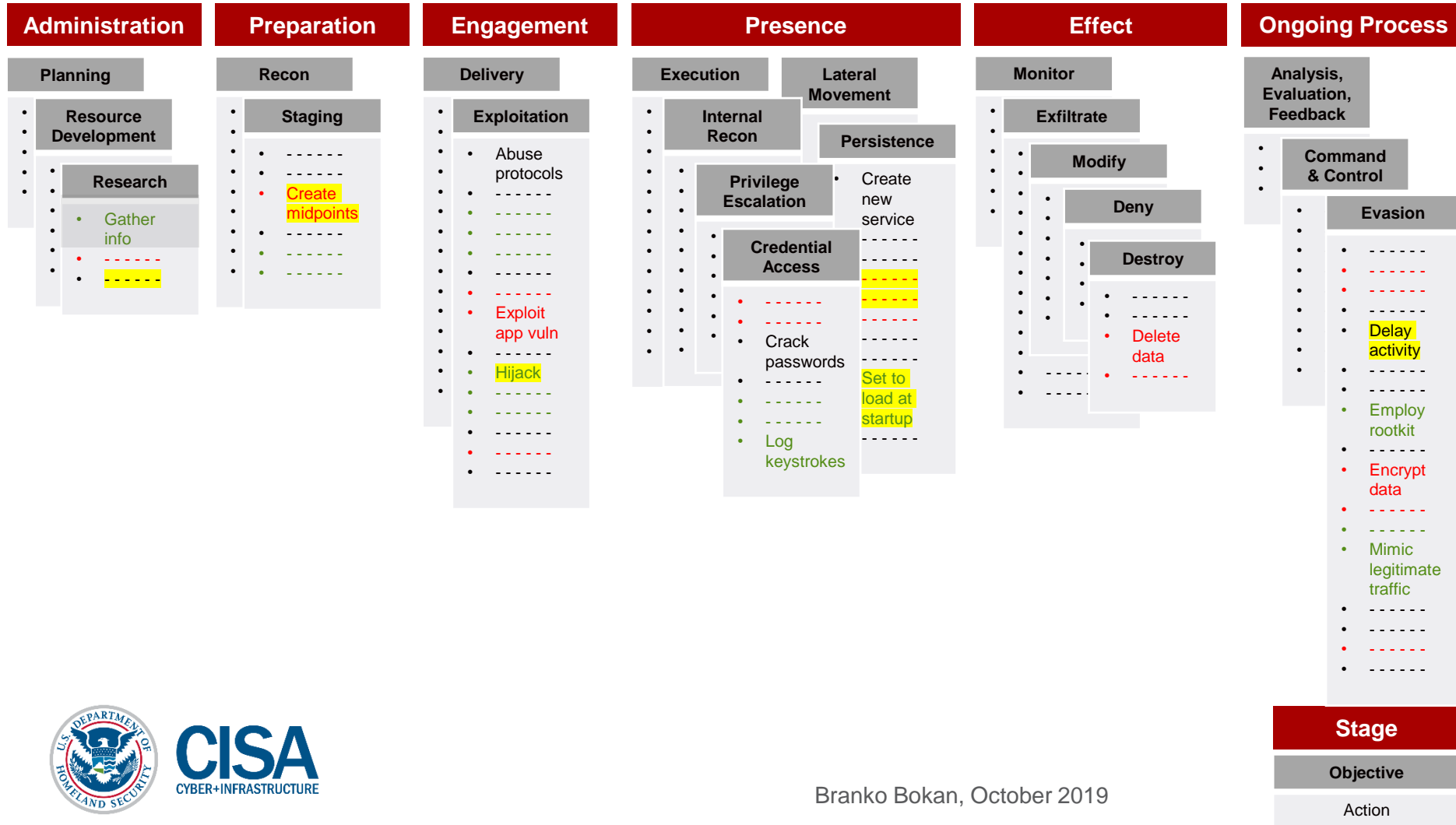
Threat Intelligence Map Analysis

Threat Actor	Objective	Threat Action	Heat Map
APT28	Credential Access	Credential Dumping	13.6
APT28	Credential Access	Password Recovery	9.0
APT28	Host Enumeration/ Internal Reconnaissance	File System Enumeration	8.9
APT28	Command & Control (C2)	Commonly used port	8.5
APT28	Host Enumeration/ Internal Reconnaissance	Process Enumeration	8.4
APT28	Installation	Writing to Disk	7.7
APT28	Host Enumeration/ Internal Reconnaissance	Account Enumeration	7.3
APT28	Initial Compromise/ Exploitation	Targets Application Vulnerability	7.3
APT28	Defense Evasion	Masquerading	7.2
APT28	Weaponization	Add Exploits to Application Data Files	7.0
APT28	Command & Control (C2)	Standard app layer protocol	7.0
APT28	Execution	Command Line	6.9

Objective	Threat Action	Heat Map
Credential Access	Credential Dumping	13.6
Credential Access	Password Recovery	9.0
Host Enumeration/ Internal Reconnaissance	File System Enumeration	8.9
Command & Control (C2)	Commonly used port	8.5
Host Enumeration/ Internal Reconnaissance	Process Enumeration	8.4
Installation	Writing to Disk	7.7
Host Enumeration/ Internal Reconnaissance	Account Enumeration	7.3
Initial Compromise/ Exploitation	Targets Application Vulnerability	7.3
Defense Evasion	Masquerading	7.2
Weaponization	Add Exploits to Application Data Files	7.0
Command & Control (C2)	Standard app layer protocol	7.0
Execution	Command Line	6.9



# Threat heat mapping

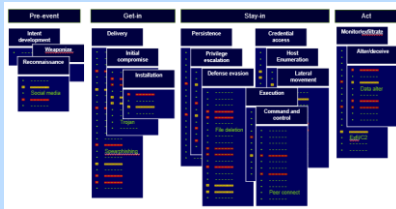


**CISA**  
CYBER+INFRASTRUCTURE

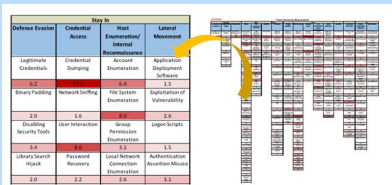


# Methodology - recap

## Threat Focus Framework



## Heat\_Map



## Scoring

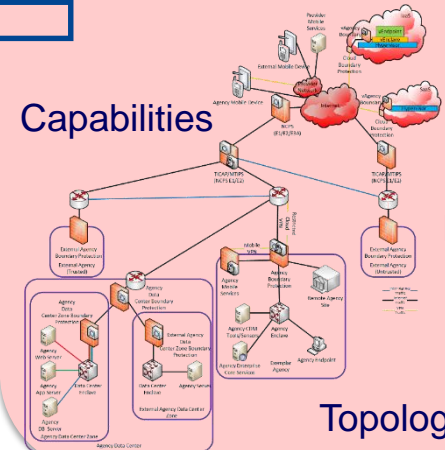


## Analysis



## Architecture Focus

### Capabilities



### Flows

### Topologies

Recommendations  
Affirmations  
Observations



**CISA**  
CYBER+INFRASTRUCTURE



# Notes

- Capabilities are deployed and used as intended. Scores do not reflect the impact of partial, incomplete, or incorrect deployment of a capability.
- A generic architecture is used for scoring and analysis; current results do not represent a particular agency.
- Threat actions are not linear.
- Vendor agnostic
- Does not provide impact analysis
- Does not delineate detailed implementation tradeoffs



# Analysis to date

**SPIN 1** - Score DHS provided cybersecurity services in the context of a typical large agency environment (CDM (Phase I - IV), Einstein, and TIC).

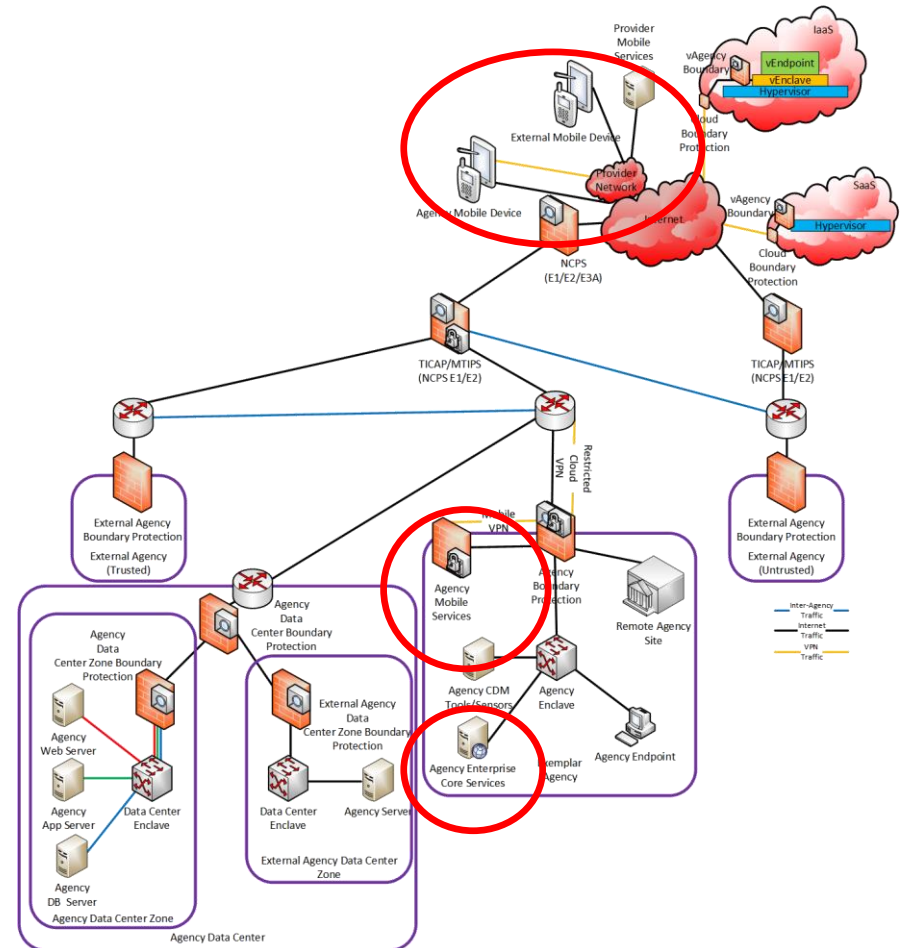
**SPIN 2** - Exemplar agency protections at boundary and endpoint

**SPIN 3** – Cloud basic structures exemplar D/A protections for virtual data center (IaaS and SaaS)

**SPIN 4** – Exemplar Agency Data Center

**SPIN 5** – Mobile architecture (EMM, MDM, MAM, MAV, MIM, MTD, ...)

**SPIN 6** – Next generation network technologies (Private .gov, w/ VDI browser, SDP, ABAC –E, Deception Technologies, SOAR)



**CISA**  
CYBER+INFRASTRUCTURE



# Worked Example - Mobile EE

Materiel

N/A
None
Limited
Moderate
Significant

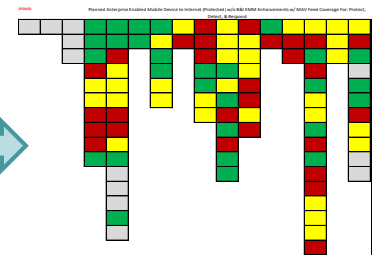
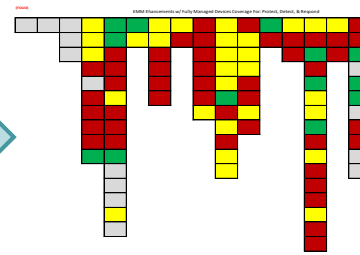
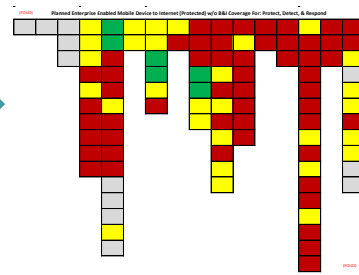
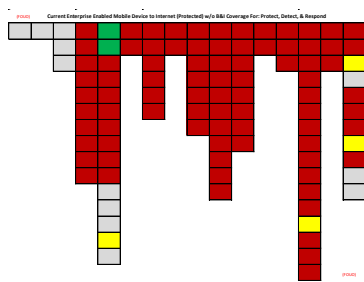
## Part 2

Current EE

Planned EE

Planned EE Fully Managed

Planned EE w/ Integrated MAV



### Configuration Control from EMM Provides Limited Mitigation

- MDM
- MAM with application blacklist
- MIM

### Controlling apps via Enterprise App Store improves posture

- MDM
- MAM Enhancements with application blacklist
- MIM
- MAV
- MTD
- MDSE

### Supervising device improves quality of Configuration Control

- MDM
- MAM Enhancements with application whitelist
- MIM / MAV/ MTD
- Fully Managed device

### Tight integration with MAV improves quality of App Whitelisting Mitigations

- MDM
- MAM Enhancements with application whitelist
- MIM
- MAV integrated with EMM



**CISA**  
CYBER+INFRASTRUCTURE



# Worked example – FedRAMP IaaS

Functional

Current Agency/Internet to IaaS UCloud/RCloud CSP-Provided IaaS Only Coverage For: Protect, Detect, & Respond

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)	Monitor (Observation)/Exfiltration	After/Decide...		
	Crawling/Internet Websites	Add Exploits to Application Data Files	Spamming/Emails w/ Attachments	Targets Application Vulnerability	Writing to Disk	Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Account Enumeration	Application Deployment Software	Command Line	Commonly used port	Automated or Scripted Exfiltration	Distributed Denial of Service (DDoS)		
	Network Mapping (e.g. NMAP)		Spamming/Emails w/Malicious Link	Targets Operating System Vulnerability	In Memory Malware	Accessibility Features	Accessibility Features	Binary Padding	Virtualization Attacks	File System Enumeration	Virtualization Attacks	File Access	Common through removable media	Virtualization Attacks	Partial Disk/OS Deletion (Corruption)		
	Social Media		Websites	Targets Application Vulnerability	Scripted Scripts	Automatic Loading at Startup	Automatic Loading at Startup	Disabling Security Tools	Network Sniffing	Group Permission Enumeration	Exploitation of Vulnerability	Scripted Scripts	Custom Application Layer Protocol	Data Compressed	Full Disk/OS Deletion (Bricking)		
	Ad-ware		Removable Media (i.e. USB)	Targets Web Application Vulnerabilities	Replace Legitimate Binary with Malicious	Library Search Hijack	Library Search Hijack	Library Search Hijack	User Interaction	Local Network Connection Enumeration	Logon Scripts	Process Injection	Communications Encrypted	Data Size Limits	Data Alteration		
	Vulnerability Scan		Credential Phishing	Trojan		New Service	New Service	File System Logical Effects	Password Recovery	Local Networking Enumeration	Authentication Assertion Misuse	Configuration Modification to Facilitate Launch	Data Obfuscation	Data Staged	Data Encrypted and Unavailable (Crypto Locked)		
			SQL Injection	Social Engineering		Path Interception	Path Interception	File Deletion	Credential Manipulation	Operating System Enumeration	Remote Services	Use of Trusted Process to Execute	Failback Channels	Soft over C2 channel	Data Deletion (Partial)		
			Devising Exploit using Advertising	Legitimate Access		Scheduled Task	Scheduled Task	Indicator Blocking on Host	Hijack Active Credentials	Domain/User Enumeration	Peer Connections	Scheduled Task	Multiband comm.	Soft over Alternate Channel to a C2 Network	Data Deletion (Full)		
			DDoS/Cashe Poisoning	Delegated Encryption		Service File Permission Weakness	Service File Permission Weakness	Indicator Removal from Tools	Credentials in File	Process Enumeration	Remote Interactive Logon	Service Manipulation	Multitask encryption	Exfiltration Over other Network Medium	Denial of Service		
			Vulnerability Attacks	Exploit Weak Access Controls		Link Modification	Link Modification	Indicator Removal from Host		Security Software Enumeration	Remote Management Services	Word Pasting Software	Peer Connections	Exfiltration via Local System	Cause Physical Effects		
			Connection of Rogue Network Devices			Edit Default File Handlers	Manipulate Trusted Process	Manipulate Trusted Process		Service Enumeration	Replication through Removable Media	Remote Management Services	Standard app layer protocol	Soft over network resources			
			Trusted Website							Window Enumeration	Shared Windows	APIs to Facilitate Launch	Standard non-app layer protocol	Scheduled Transfer			
			Legitimate Remote Access								Taint Shared Content		Standard Encryption Cipher	Data Encrypted			
			CrossTalk (Data Enumeration)								Remote File Shares		Uncommonly Used Port	Soft over Virtual Medium			
			Service Mapping (Cross Domain Violation)										Custom encryption cipher	Soft over Physical Medium			
			Exploit Cross-Domain or Multi-Level Solution Misconfiguration										Multiple Protocols Combined	CrossTalk (Data Enumeration)			
			Physical Network Bridge														
			Data Encoded														
			Automatically Transported Scripted Services														
			Cross Domain or Multi-Level Solution Traversal														
			Supply Chain / Trusted Source Compromise HW														
			Supply Chain / Trusted Source Compromise SW														
			Auto Delivery via Cloud Service														
			Insider Threat/Close Access														
			Compromise Customer Network Infrastructure														

Color Code Legend
N/A
FedRAMP Control



# Best from Spins 1-4

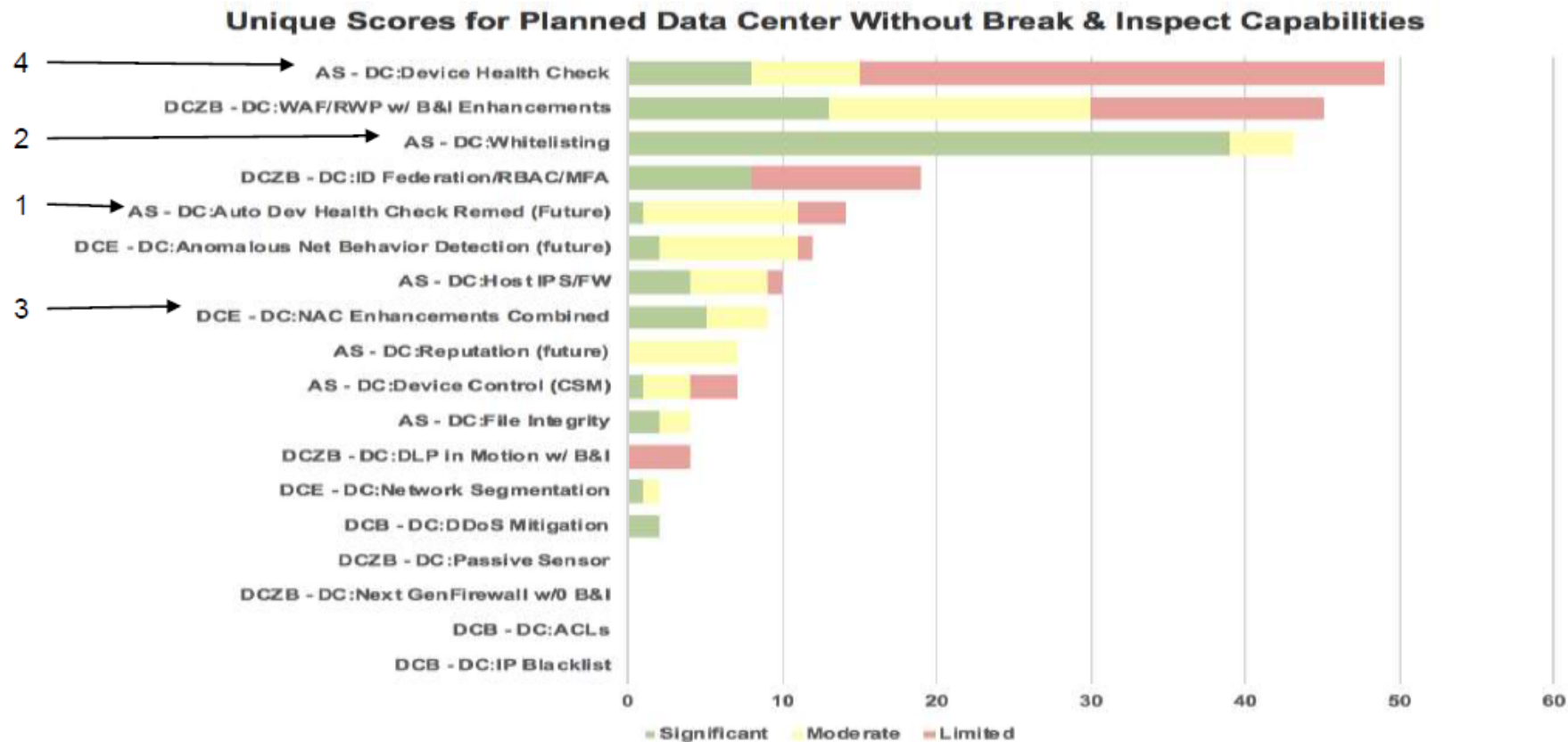
A value weighted by the strength and breadth of the capability with the threat importance is created. These individual values are combined across threat actions. Capabilities with the highest weighted value are considered best.

	<b>Current</b>	<b>Future</b>
1	Device Health Check Remediation	Auto Device Health Check Remediation
2	Application Whitelisting	Application Whitelisting
3	Device Health Check	NAC Enhancements
4	WAF/RWP w/ B&I	Device Health Check





# Best from Spins 1-4



Best Capabilities are also unique in the threat actions that they cover



# .govCAR goals


- Inform DHS's approach to assisting Agencies with insight and knowledge to make prioritized cybersecurity investment decisions across the .gov environment
  - Create a threat-based security architecture review that provides an end-to-end holistic assessment that is composed of capabilities provided by DHS or the individual Departments and Agencies.
  - Create a common framework to discuss and assess cybersecurity architectural choices:
    - For a shared Federal IT Infrastructure
    - To inform DHS's approach for its capabilities
    - To enable Agencies to make threat-based risk decisions
- Be transparent and traceable





# .govCAR Recommendations



**CISA**  
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

## .govCAR Recommendations: MOBILE CYBERSECURITY

The Cybersecurity and Infrastructure Security Agency (CISA) developed .govCAR—Cybersecurity Architecture Review of the .gov domain—to take a threat-based approach to cybersecurity risk management. Traditional risk management focuses on consequence and vulnerability (i.e., compliance and cyber hygiene), while a threat-based approach looks at cybersecurity capabilities from an adversary's standpoint. This next-generation approach directly identifies areas where mitigations should be applied for best defense.

### OVERVIEW

The recommendations below provide organizations with actionable guidance on—and justifications for future investments in—mobile cybersecurity capabilities. CISA based these recommendations on a .govCAR analysis that identified how—in an exemplar enterprise mobile environment at a typical organization—mobile devices and organizational sensitive data on those devices are protected.

### KEY TAKEAWAYS

The .govCAR analysis identified a range of capabilities that can be deployed to increase threat mitigation coverage. The major finding indicates that to provide maximum coverage against mobile threat actions, organizations must deploy Enterprise Mobility Management (EMM), Mobile Threat Defense (MTD), and Mobile App Vetting (MAV) capabilities together as an *integrated solution*, and not as a series of standalone products. **Note:** although integration and interoperability of these three capabilities are key, this solution does not require organizations to source each of the capabilities from a single vendor.

### MOBILE CYBERSECURITY ARCHITECTURE

A typical mobile cybersecurity architecture is made of capabilities and protections for an organization's mobile environment. The .govCAR analysis addressed two mobile use cases, which represent the predominant deployment models across the Federal Government:

- **Corporate-Owned, Personally Enabled** devices (known as COPE devices) are corporate-owned and centrally managed mobile devices capable of remotely accessing enterprise resources. COPE devices allow for personal use as they have fewer restrictions than EEA devices (see below) on non-enterprise applications and data.
- **Enterprise-Enabled, Owned by the Agency** devices (known as EEA devices) are also corporate-owned and centrally managed mobile devices capable of remotely accessing enterprise resources. However, EEA devices restrict (or strictly limit) personal use. Tradeoffs between security and functional usability in this model are made at the discretion of the organization's leadership.

Both COPE and EEA devices and their associated data belong to the enterprise.

2019-09-06



**CISA**  
CYBER+INFRASTRUCTURE



# OMB Max Repository

.govCAR Home

(permalink <https://community.max.gov/x/FqVIY> )

Technical Annex Documents - Restricted Access

(permalink [https://community.max.gov/x/\\_9n7YQ](https://community.max.gov/x/_9n7YQ) )

**-govCAR**  
*think like the adversary*



**CISA**  
CYBER+INFRASTRUCTURE





**CISA**  
CYBER+INFRASTRUCTURE



Review of agency specific architectures (e.g. Census, EPA, USDA)

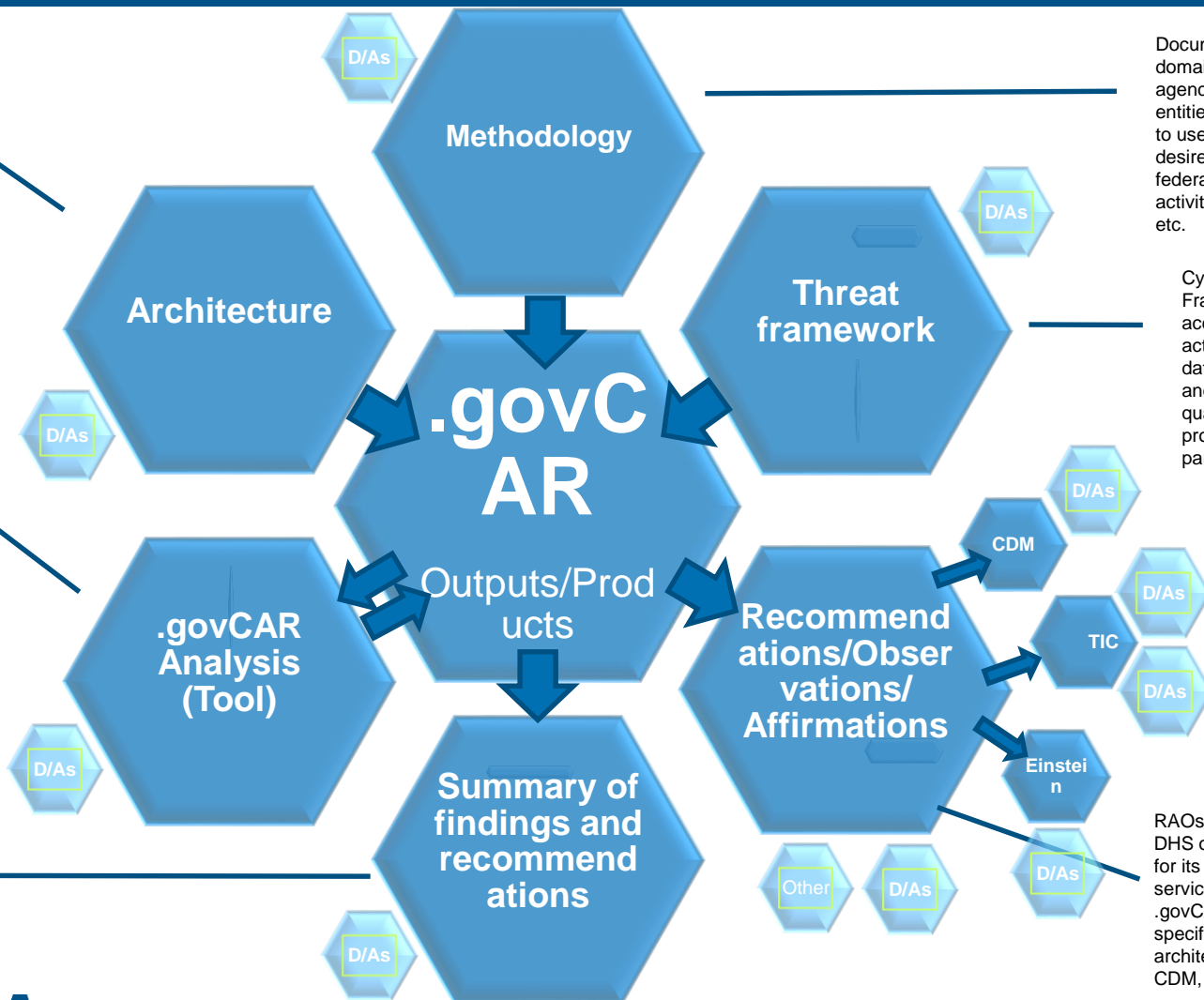
A tool, currently under development, that includes cybersecurity threat framework (including up-to-date threat activities and heat maps), architectures, scoring results, and other supporting data available to federal agencies (and possibly others) that allows them to easily perform their own what-if and gap analyses using the data produced by .govCAR team.

The tool will also allow agencies to input their own architectures (not already evaluated by the .govCAR team).

RAOs resulting from .govCAR analysis activities conducted by DHS generally applicable to all federal agencies (and possibly outside of .gov) in form of fact sheets, potentially BOD, and other types of communications



**CISA**  
CYBER+INFRASTRUCTURE



Documentation in public domain available to agencies and other entities (e.g. commercial) to use however they desire, independently of federal government activities, feeds, results, etc.

Cybersecurity Threat Framework (including accompanying threat actions and heat mapping data) maintained by DHS and updated quarterly(ish) a side product but an integral part of .govCAR

RAOs that directly inform DHS on the future course for its products and services (results of .govCAR analyses of specific DHS architectures - e.g. TIC, CDM, Einstein, etc.)

Rev 10/19/2018