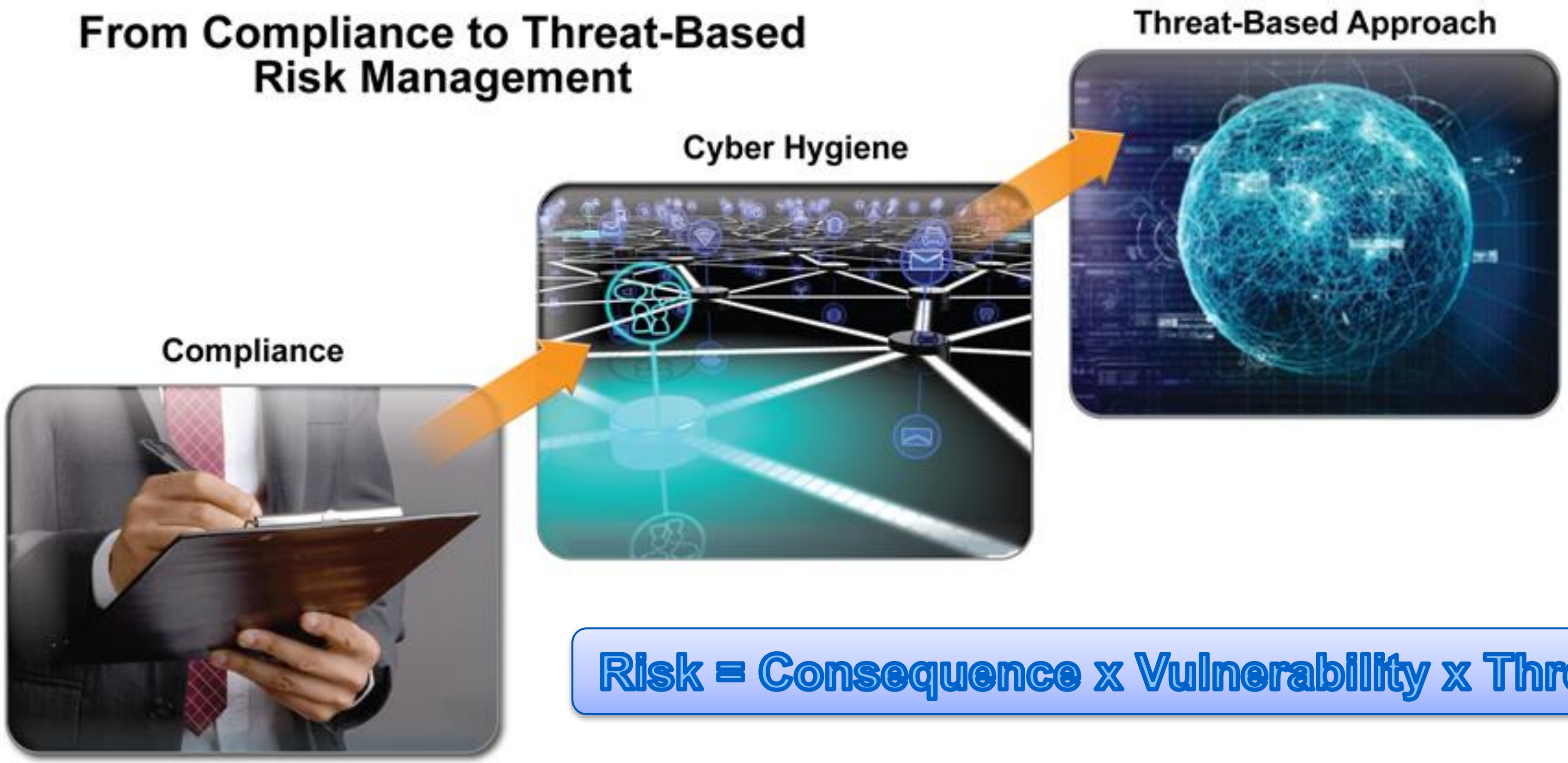
# .govCAR

*think like the adversary*

Branko Bokan, November 19, 2019

# Move to Stronger Risk Management



**Risk = Consequence x Vulnerability x Threat**

CISA
CYBER+INFRASTRUCTURE

Branko Bokan, November 19, 2019

# About .govCAR

- .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

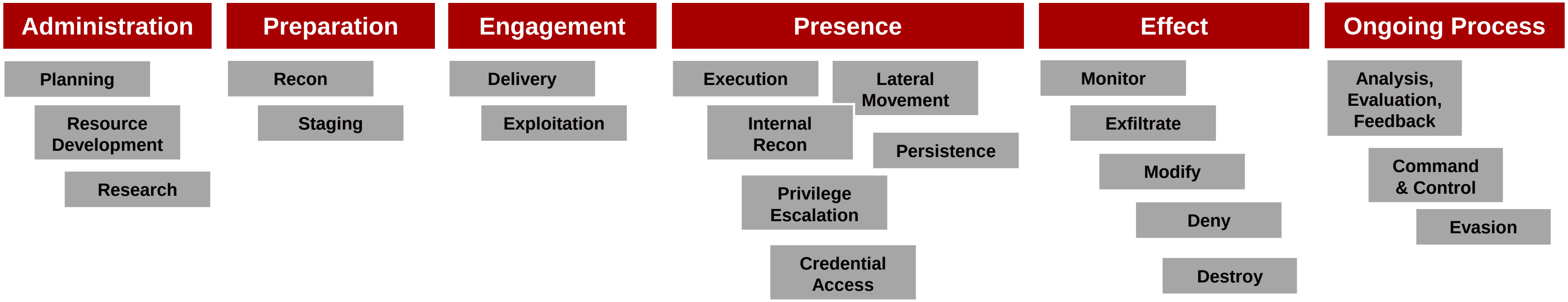
# Why .govCAR?

- 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

# Stages and Objectives



**Administration**

- Planning
- Resource Development
- Research

**Preparation**

- Recon
- Staging

**Engagement**

- Delivery
- Exploitation

**Presence**

- Execution
- Lateral Movement
- Internal Recon
- Persistence
- Privilege Escalation
- Credential Access

**Effect**

- Monitor
- Exfiltrate
- Modify
- Deny
- Destroy

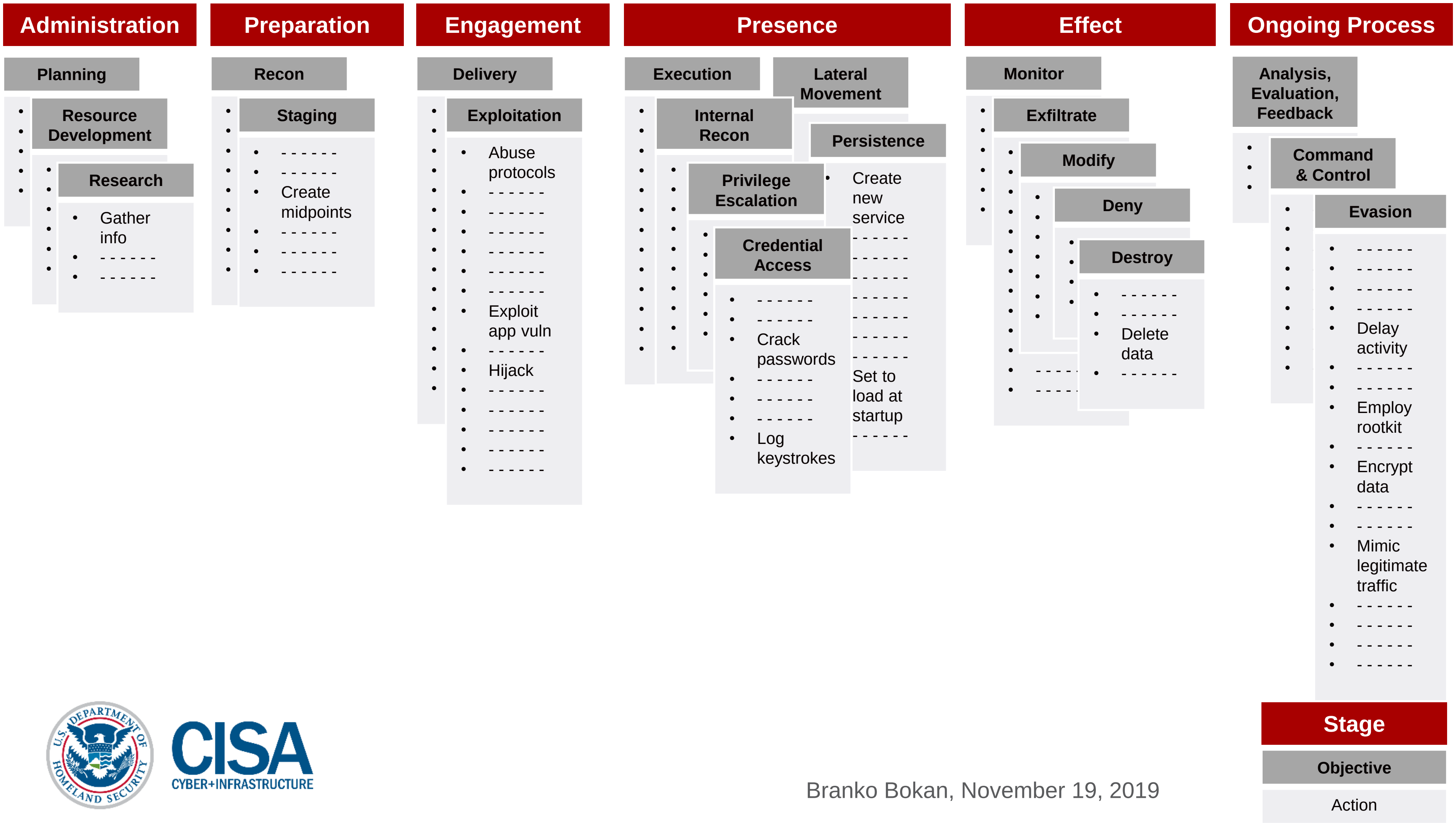
**Ongoing Process**

- Analysis, Evaluation, Feedback
- Command & Control
- Evasion

**Stage**

Objective

# Threat actions



**Administration**
- Planning
- Resource Development
- Research
  - Gather info
  - - - - - - -
  - - - - - - -

**Preparation**
- Recon
- Staging
  - - - - - - -
  - - - - - - -
  - Create midpoints
  - - - - - - -
  - - - - - - -
  - - - - - - -

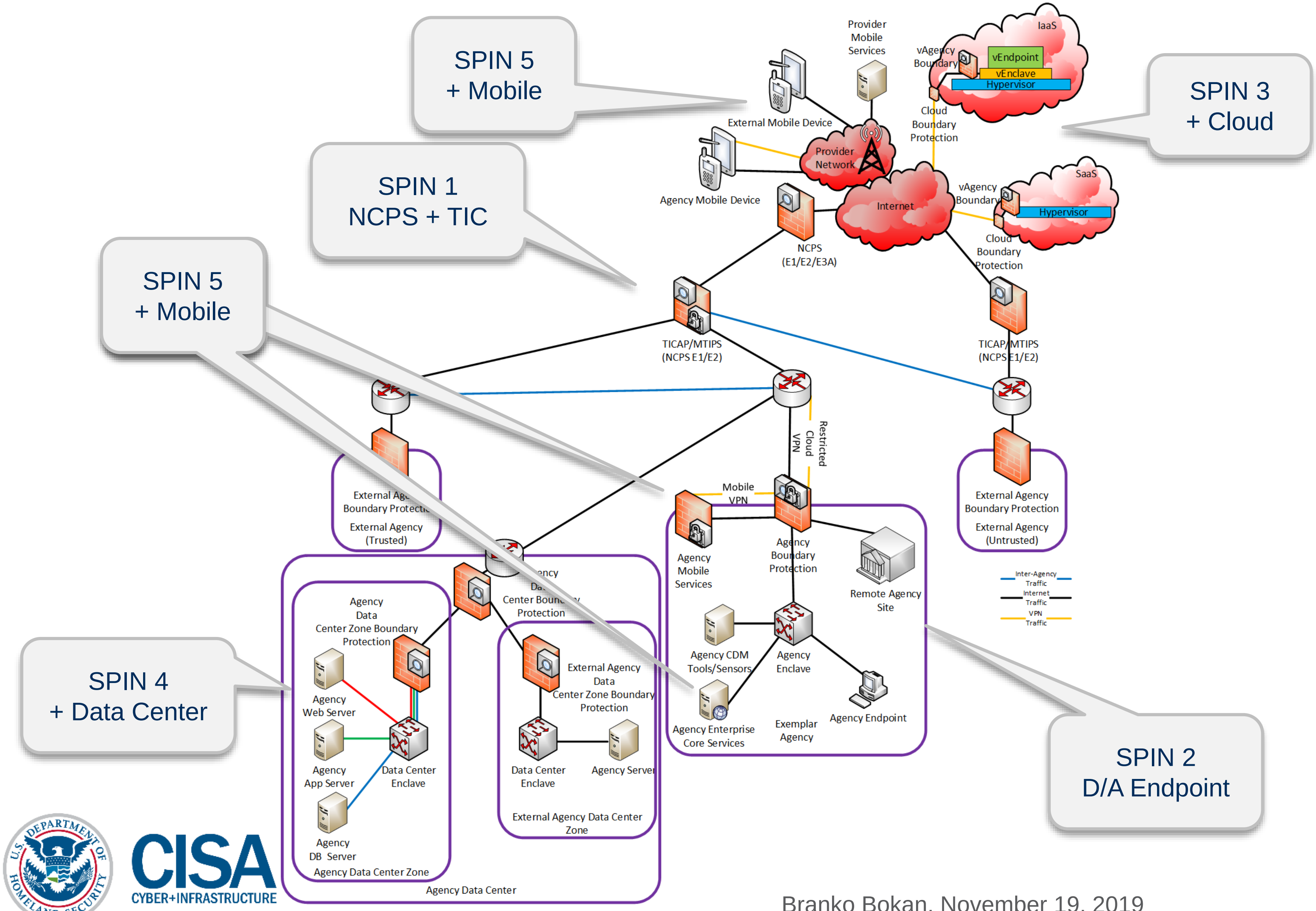
**Engagement**
- Delivery
- Exploitation
  - Abuse protocols
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - Exploit app vuln
  - - - - - - -
  - Hijack
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -

**Presence**
- Execution
- Lateral Movement
- Internal Recon
- Persistence
  - Create new service
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - Set to load at startup
  - - - - - - -
- Privilege Escalation
- Credential Access
  - - - - - - -
  - - - - - - -
  - Crack passwords
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - Log keystrokes

**Effect**
- Monitor
- Exfiltrate
- Modify
- Deny
- Destroy
  - - - - - - -
  - - - - - - -
  - Delete data
  - - - - - - -

**Ongoing Process**
- Analysis, Evaluation, Feedback
- Command & Control
- Evasion
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - Delay activity
  - - - - - - -
  - - - - - - -
  - Employ rootkit
  - - - - - - -
  - Encrypt data
  - - - - - - -
  - - - - - - -
  - Mimic legitimate traffic
  - - - - - - -
  - - - - - - -
  - - - - - - -
  - - - - - - -

# Spin 1-5 Architecture View



SPIN 5
+ Mobile

SPIN 1
NCPS + TIC

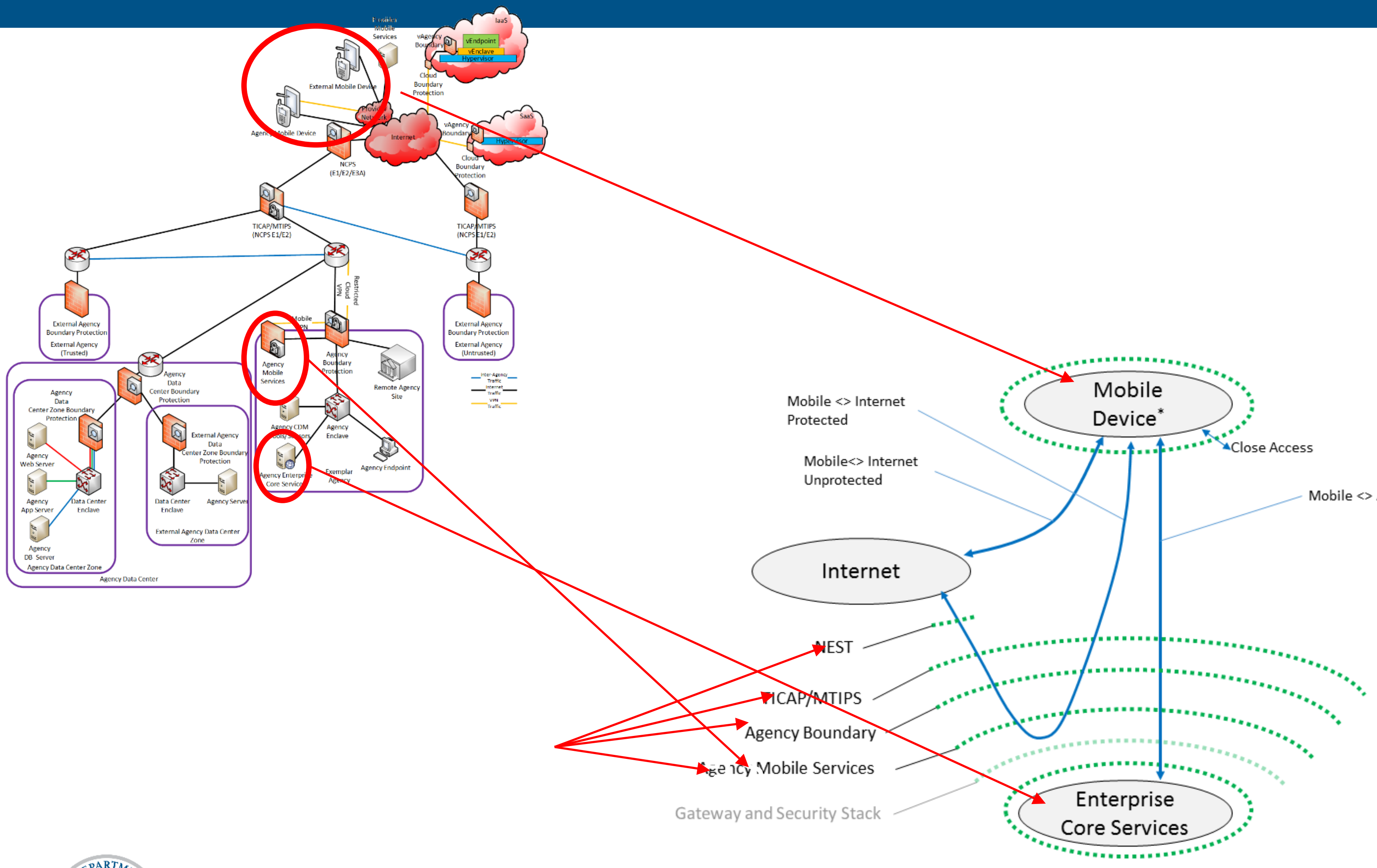
SPIN 3
+ Cloud

SPIN 5
+ Mobile

SPIN 4
+ Data Center

SPIN 2
D/A Endpoint

# Architectures and Flows



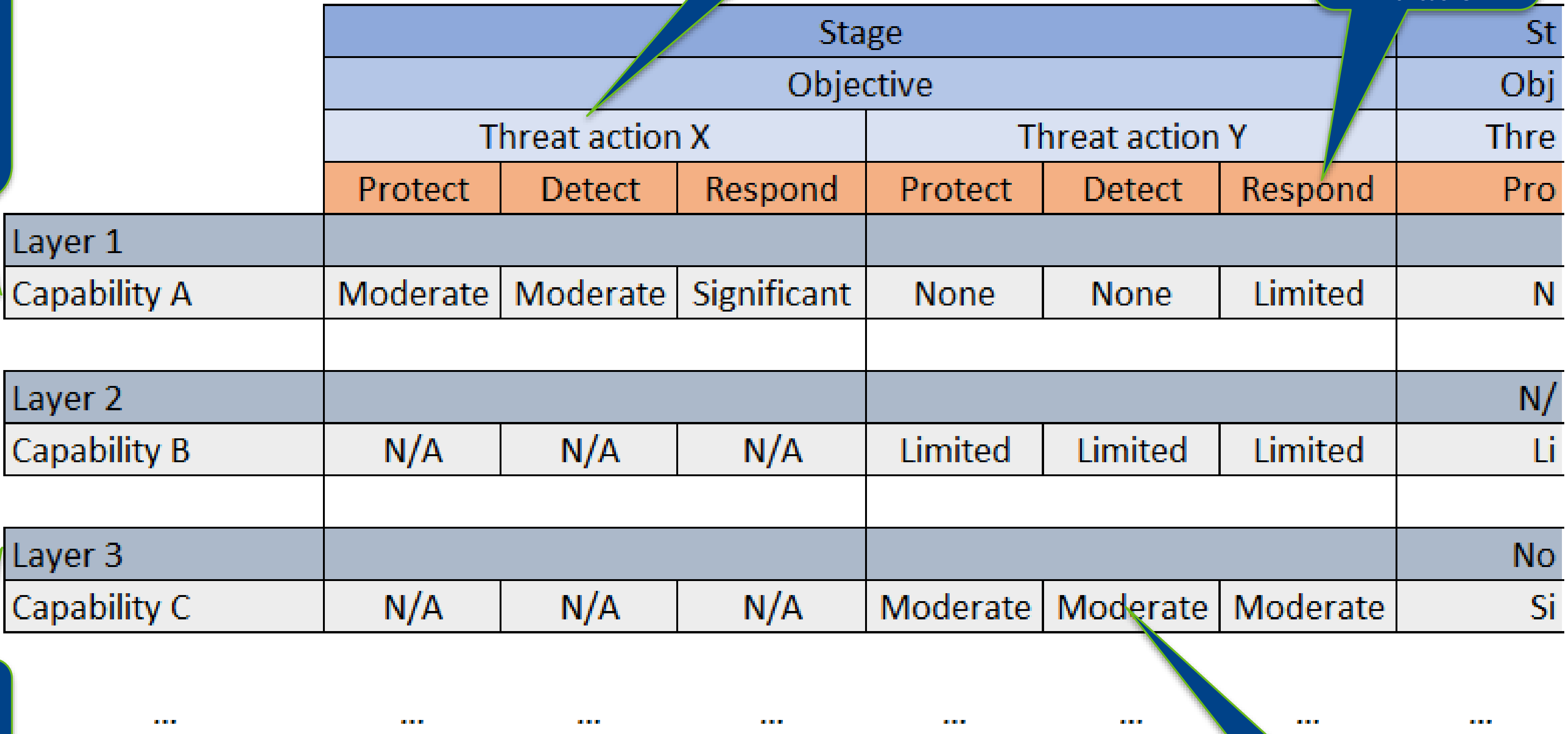
*Mobile Device includes Unmanaged and Agency Managed Devices

# Scoring

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

Threat 'Actions' From the Framework

NIST CyberSecurity Framework Mitigation Functions

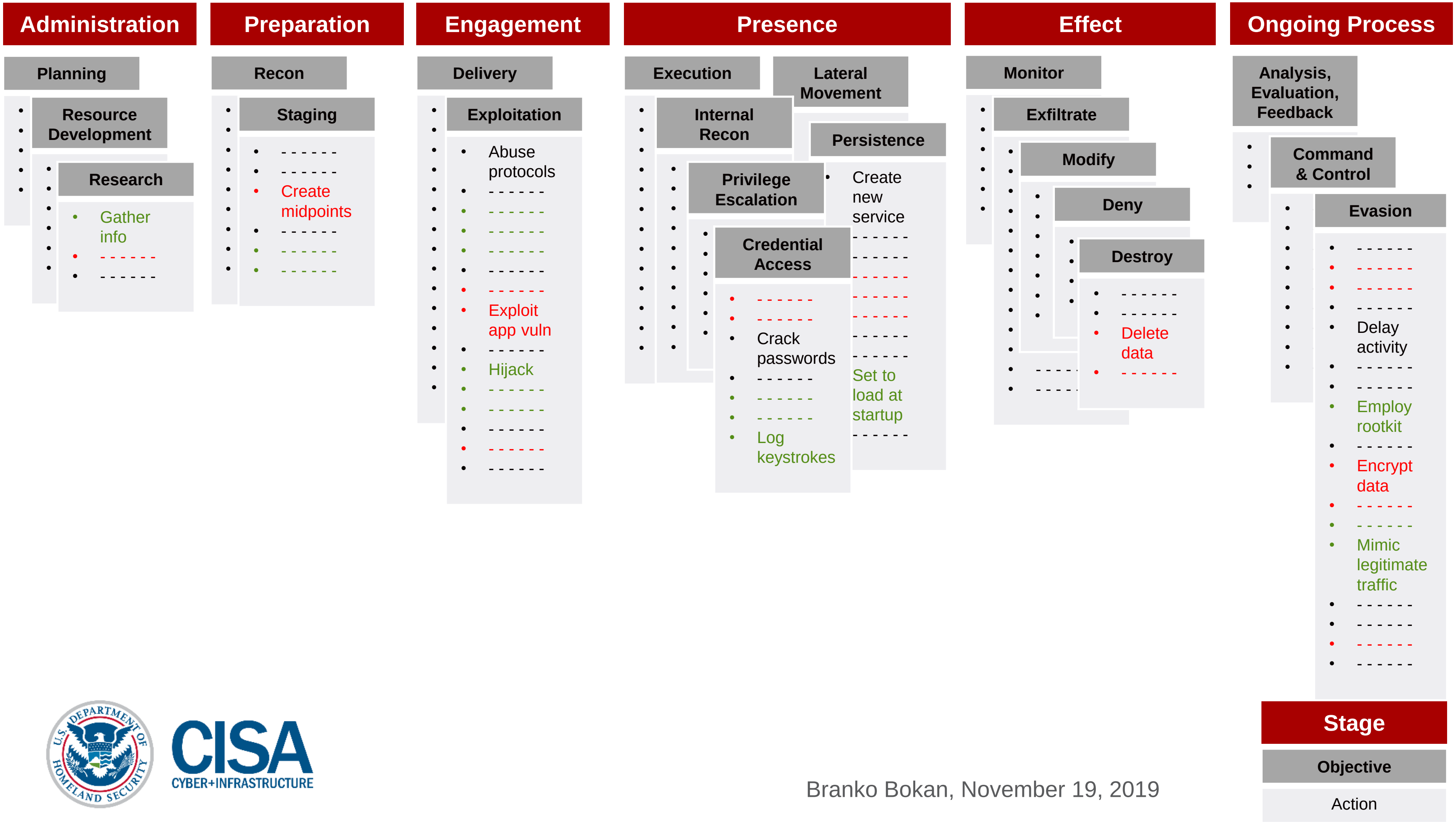


| | Stage | | | | | | St |
|---|---|---|---|---|---|---|---|
| | Objective | | | | | | Obj |
| | Threat action X | | | Threat action Y | | | Thre |
| | Protect | Detect | Respond | Protect | Detect | Respond | Pro |
| Layer 1 | | | | | | | |
| Capability A | Moderate | Moderate | Significant | None | None | Limited | N |
| | | | | | | | |
| Layer 2 | | | | | | | N/ |
| Capability B | N/A | N/A | N/A | Limited | Limited | Limited | Li |
| | | | | | | | |
| Layer 3 | | | | | | | No |
| Capability C | N/A | N/A | N/A | Moderate | Moderate | Moderate | Si |
| … | … | … | … | … | … | … | … |

Logical Groupings of Capabilities by Tier

SME Scoring:
Significant
Moderate
Limited

# Coverage mapping



**Administration**

Planning

Resource Development

Research
- Gather info
- - - - - - -
- - - - - - -

**Preparation**

Recon

Staging
- - - - - - -
- - - - - - -
- Create midpoints
- - - - - - -
- - - - - - -
- - - - - - -

**Engagement**

Delivery

Exploitation
- Abuse protocols
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- Exploit app vuln
- - - - - - -
- Hijack
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -

**Presence**

Execution

Lateral Movement

Internal Recon

Persistence
- Create new service
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- Set to load at startup
- - - - - - -

Privilege Escalation

Credential Access
- - - - - - -
- - - - - - -
- Crack passwords
- - - - - - -
- - - - - - -
- - - - - - -
- Log keystrokes

**Effect**

Monitor

Exfiltrate
- - - - - -
- - - - - -

Modify

Deny

Destroy
- - - - - - -
- - - - - - -
- Delete data
- - - - - - -

**Ongoing Process**

Analysis, Evaluation, Feedback

Command & Control

Evasion
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- Delay activity
- - - - - - -
- - - - - - -
- Employ rootkit
- - - - - - -
- Encrypt data
- - - - - - -
- - - - - - -
- Mimic legitimate traffic
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -

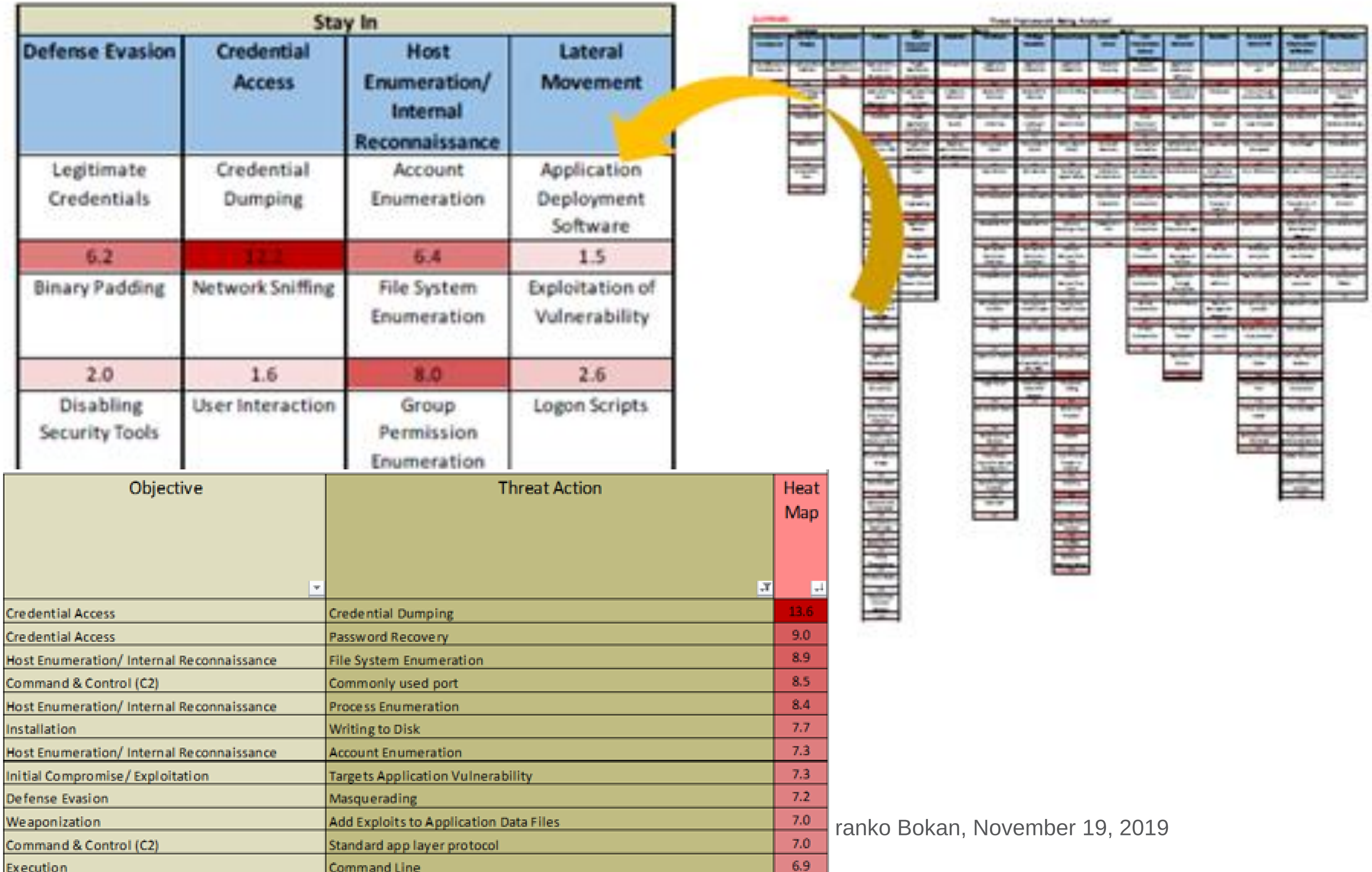
**Stage**

Objective

Action

Branko Bokan, November 19, 2019

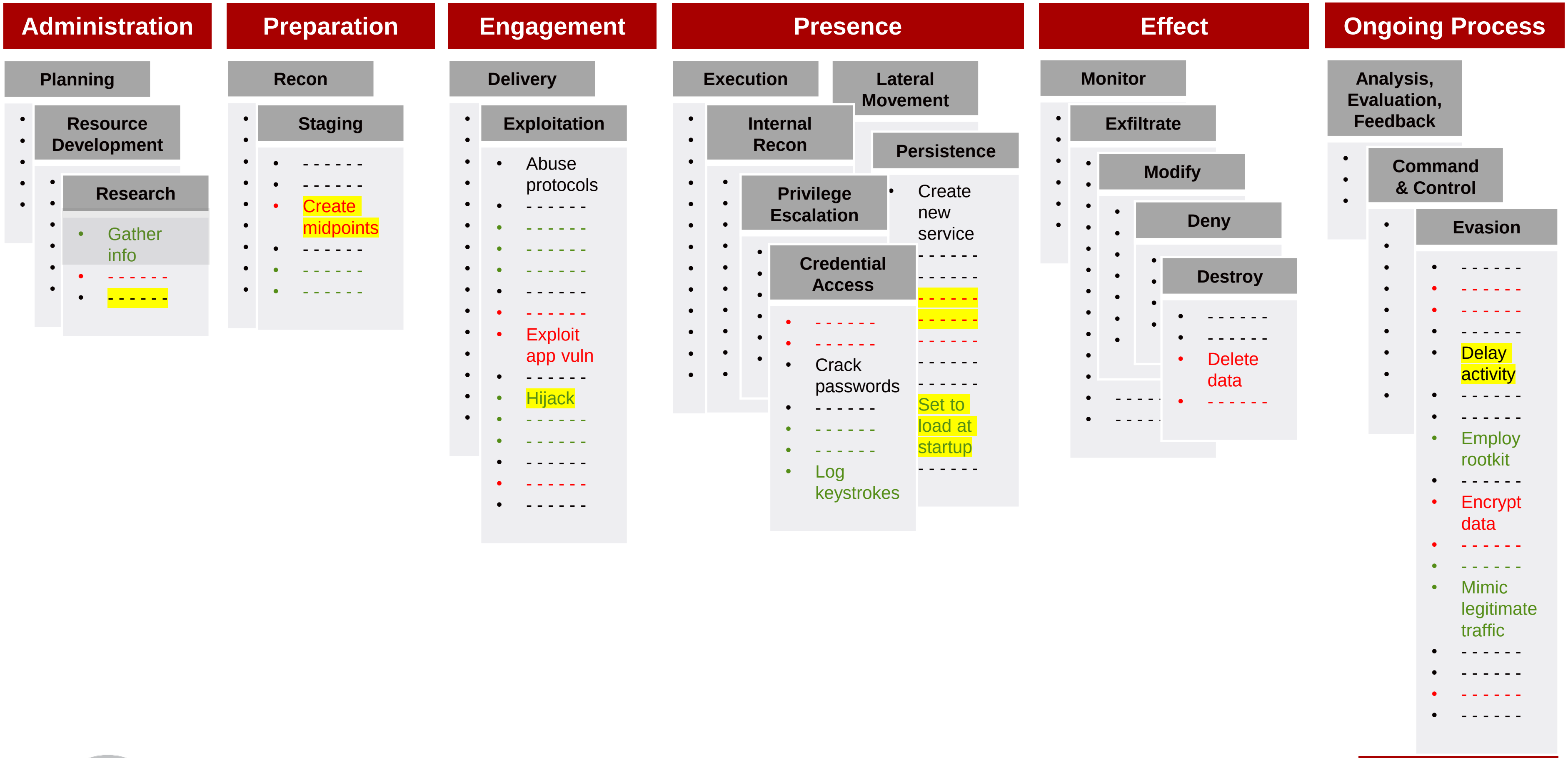
# Threat heat mapping



| 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 |

| 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



## Administration

### Planning

### Resource Development

### Research

- Gather info
- - - - - - -
- - - - - - -

## Preparation

### Recon

### Staging

- - - - - - -
- - - - - - -
- Create midpoints
- - - - - - -
- - - - - - -
- - - - - - -

## Engagement

### Delivery

### Exploitation

- Abuse protocols
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- Exploit app vuln
- - - - - - -
- Hijack
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -

## Presence

### Execution

### Lateral Movement

### Internal Recon

### Persistence

- Create new service

- - - - - -
- - - - - -
- - - - - -
- - - - - -
- - - - - -
- - - - - -
- - - - - -

Set to load at startup

- - - - - -

### Privilege Escalation

### Credential Access

- - - - - - -
- - - - - - -
- Crack passwords
- - - - - - -
- - - - - - -
- - - - - - -
- Log keystrokes

## Effect

### Monitor

### Exfiltrate

- - - - - -
- - - - - -

### Modify

### Deny

### Destroy

- - - - - - -
- - - - - - -
- Delete data
- - - - - - -

## Ongoing Process

### Analysis, Evaluation, Feedback

### Command & Control

### Evasion

- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -
- Delay activity
- - - - - - -
- - - - - - -
- Employ rootkit
- - - - - - -
- Encrypt data
- - - - - - -
- - - - - - -
- Mimic legitimate traffic
- - - - - - -
- - - - - - -
- - - - - - -
- - - - - - -

**Stage**

**Objective**

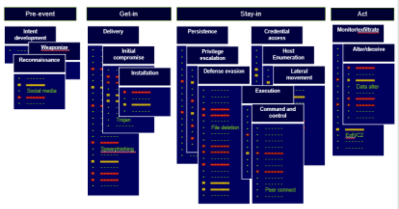
Action

Branko Bokan, November 19, 2019

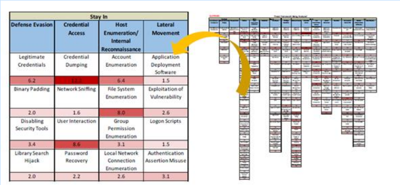
# Methodology - recap

## Threat Focus

Framework

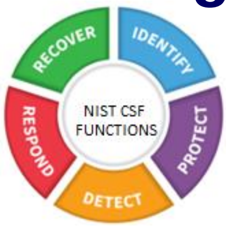


Heat_Map



| 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 |
| 3.4 | 8.6 | 3.1 | 1.5 |
| Library Search Hijack | Password Recovery | Local Network Connection Enumeration | Authentication Assertion Misuse |
| 2.0 | 2.2 | 2.6 | 3.1 |

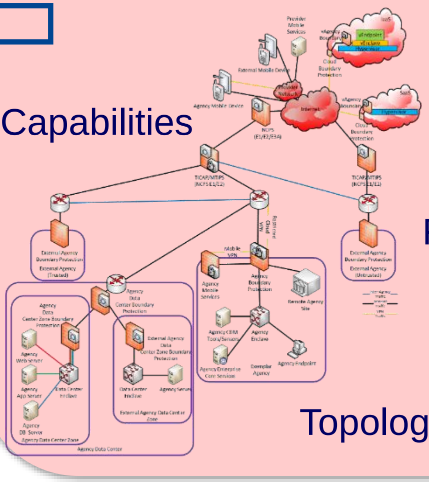
## Scoring



## Analysis

Recommendations
Affirmations
Observations

## Architecture Focus



Capabilities

Flows

Topologies

CISA
CYBER+INFRASTRUCTURE

Branko Bokan, November 19, 2019

# 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).

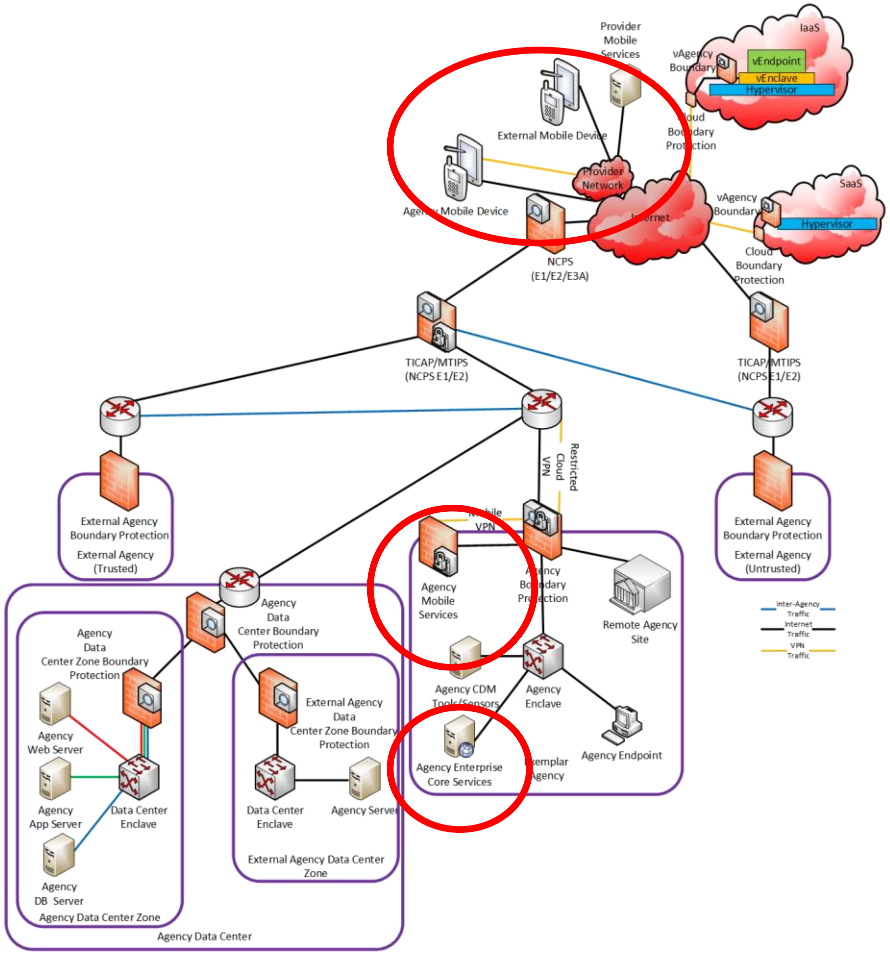
**SPIN 2** - Exemplar agency protections at boundary and endpoint

**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)



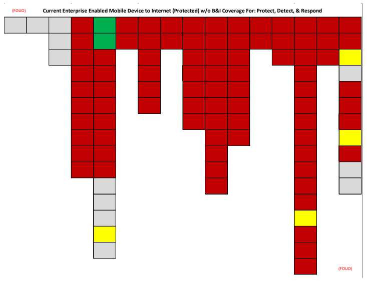
# Worked Example - Mobile EE

Materiel

N/A
None
Limited
Moderate
Significant

## Part 2

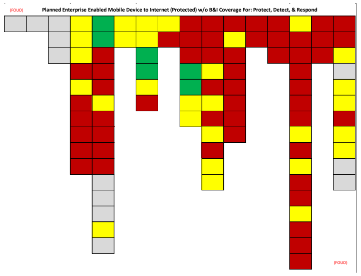
### Current EE



**Configuration Control from EMM Provides Limited Mitigation**

- MDM
- MAM with application blacklist
- MIM

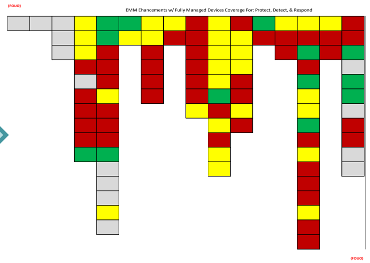
### Planned EE



**Controlling apps via Enterprise App Store improves posture**

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

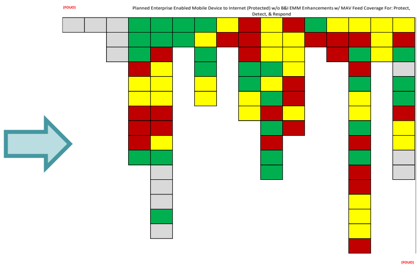
### Planned EE Fully Managed



**Supervising device improves quality of Configuration Control**

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

### Planned EE w/ Integrated MAV



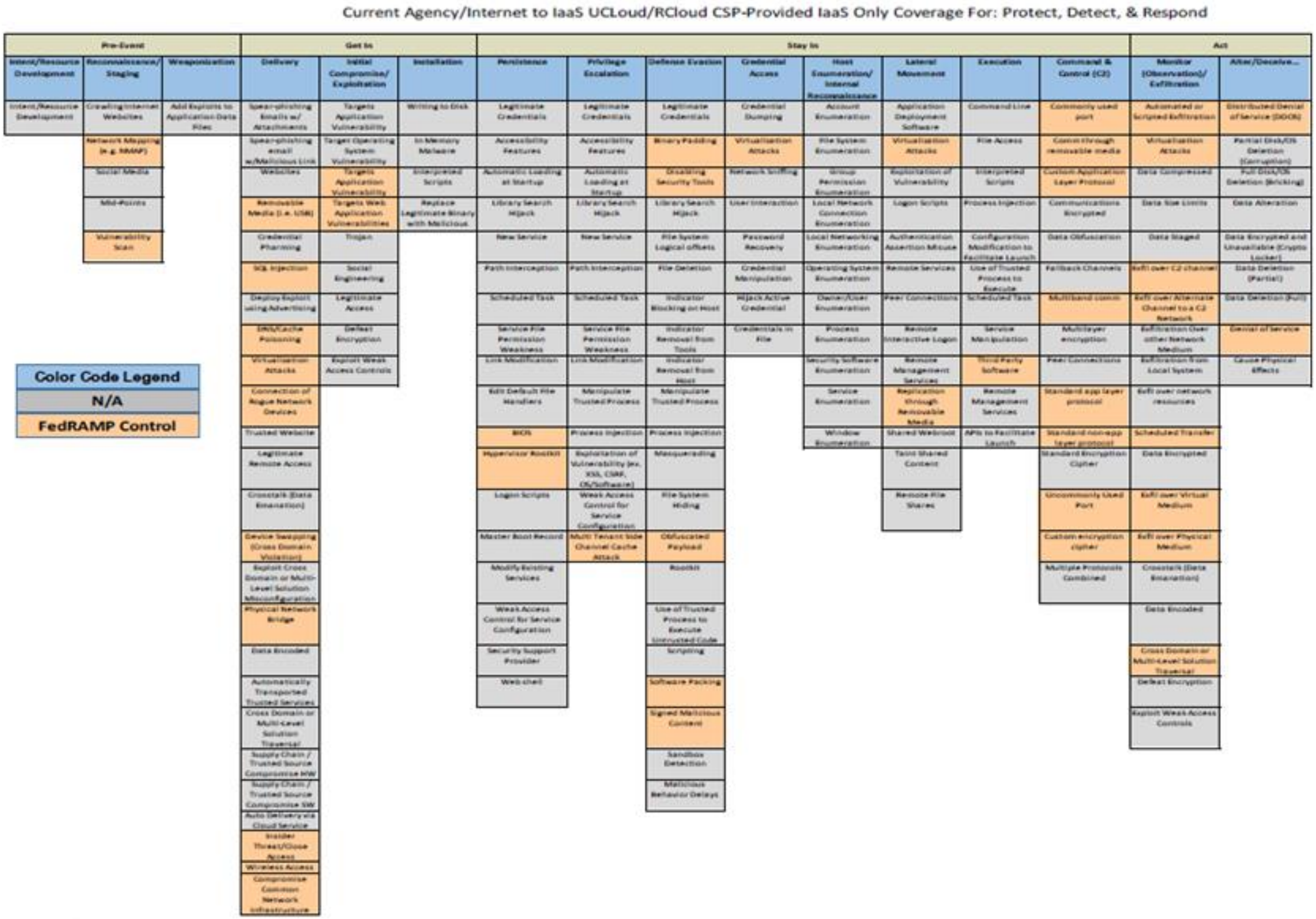
**Tight integration with MAV improves quality of App Whitelisting Mitigations**

- 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 | Alter/Deceive... |
| Intent/Resource Development | Crawling Internet Websites | Add Exploits to Application Data Files | Spear-phishing 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) | | Spear-phishing email w/Malicious Link | Target Operating System Vulnerability | In Memory Malware | Accessibility Features | Accessibility Features | Binary Padding | Virtualization Attacks | File System Enumeration | Virtualization Attacks | File Access | Comm through removable media | Virtualization Attacks | Partial Disk/OS Deletion (Corruption) |
| | Social Media | | Websites | Targets Application Vulnerability | Interpreted Scripts | Automatic Loading at Startup | Automatic Loading at Startup | Disabling Security Tools | Network Sniffing | Group Permission Enumeration | Exploitation of Vulnerability | Interpreted Scripts | Custom Application Layer Protocol | Data Compressed | Full Disk/OS Deletion (Bricking) |
| | Mid-Points | | 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 Pharming | Trojan | | New Service | New Service | File System Logical offsets | Password Recovery | Local Networking Enumeration | Authentication Assertion Misuse | Configuration Modification to Facilitate Launch | Data Obfuscation | Data Staged | Data Encrypted and Unavailable (Crypto Locker) |
| | | | SQL Injection | Social Engineering | | Path Interception | Path Interception | File Deletion | Credential Manipulation | Operating System Enumeration | Remote Services | Use of Trusted Process to Execute | Fallback Channels | Exfil over C2 channel | Data Deletion (Partial) |
| | | | Deploy Exploit using Advertising | Legitimate Access | | Scheduled Task | Scheduled Task | Indicator Blocking on Host | Hijack Active Credential | Owner/User Enumeration | Peer Connections | Scheduled Task | Multiband comm | Exfil over Alternate Channel to a C2 Network | Data Deletion (Full) |
| | | | DNS/Cache Poisoning | Defeat Encryption | | Service File Permission Weakness | Service File Permission Weakness | Indicator Removal from Tools | Credentials in File | Process Enumeration | Remote Interactive Logon | Service Manipulation | Multilayer encryption | Exfiltration Over other Network Medium | Denial of Service |
| | | | Virtualization Attacks | Exploit Weak Access Controls | | Link Modification | Link Modification | Indicator Removal from Host | | Security Software Enumeration | Remote Management Services | Third Party Software | Peer Connections | Exfiltration from 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 | Exfil over network resources | |
| | | | Trusted Website | | | BIOS | Process Injection | Process Injection | | Window Enumeration | Shared Webroot | APIs to Facilitate Launch | Standard non-app layer protocol | Scheduled Transfer | |
| | | | Legitimate Remote Access | | | Hypervisor Rootkit | Exploitation of Vulnerability (ex. XSS, CSRF, OS/Software) | Masquerading | | | Taint Shared Content | | Standard Encryption Cipher | Data Encrypted | |
| | | | Crosstalk (Data Emanation) | | | Logon Scripts | Weak Access Control for Service Configuration | File System Hiding | | | Remote File Shares | | Uncommonly Used Port | Exfil over Virtual Medium | |
| | | | Device Swapping (Cross Domain Violation) | | | Master Boot Record | Multi Tenant Side Channel Cache Attack | Obfuscated Payload | | | | | Custom encryption cipher | Exfil over Physical Medium | |
| | | | Exploit Cross Domain or Multi-Level Solution Misconfiguration | | | Modify Existing Services | | Rootkit | | | | | Multiple Protocols Combined | Crosstalk (Data Emanation) | |
| | | | Physical Network Bridge | | | Weak Access Control for Service Configuration | | Use of Trusted Process to Execute Untrusted Code | | | | | | Data Encoded | |
| | | | Data Encoded | | | Security Support Provider | | Scripting | | | | | | Cross Domain or Multi-Level Solution Traversal | |
| | | | Automatically Transported Trusted Services | | | Web shell | | Software Packing | | | | | | Defeat Encryption | |
| | | | Cross Domain or Multi-Level Solution Traversal | | | | | Signed Malicious Content | | | | | | Exploit Weak Access Controls | |
| | | | Supply Chain / Trusted Source Compromise HW | | | | | Sandbox Detection | | | | | | | |
| | | | Supply Chain / Trusted Source Compromise SW | | | | | Malicious Behavior Delays | | | | | | | |
| | | | Auto Delivery via Cloud Service | | | | | | | | | | | | |
| | | | Insider Threat/Close Access | | | | | | | | | | | | |
| | | | Wireless Access | | | | | | | | | | | | |
| | | | Compromise Common Network Infrastructure | | | | | | | | | | | | |

Color Code Legend

N/A

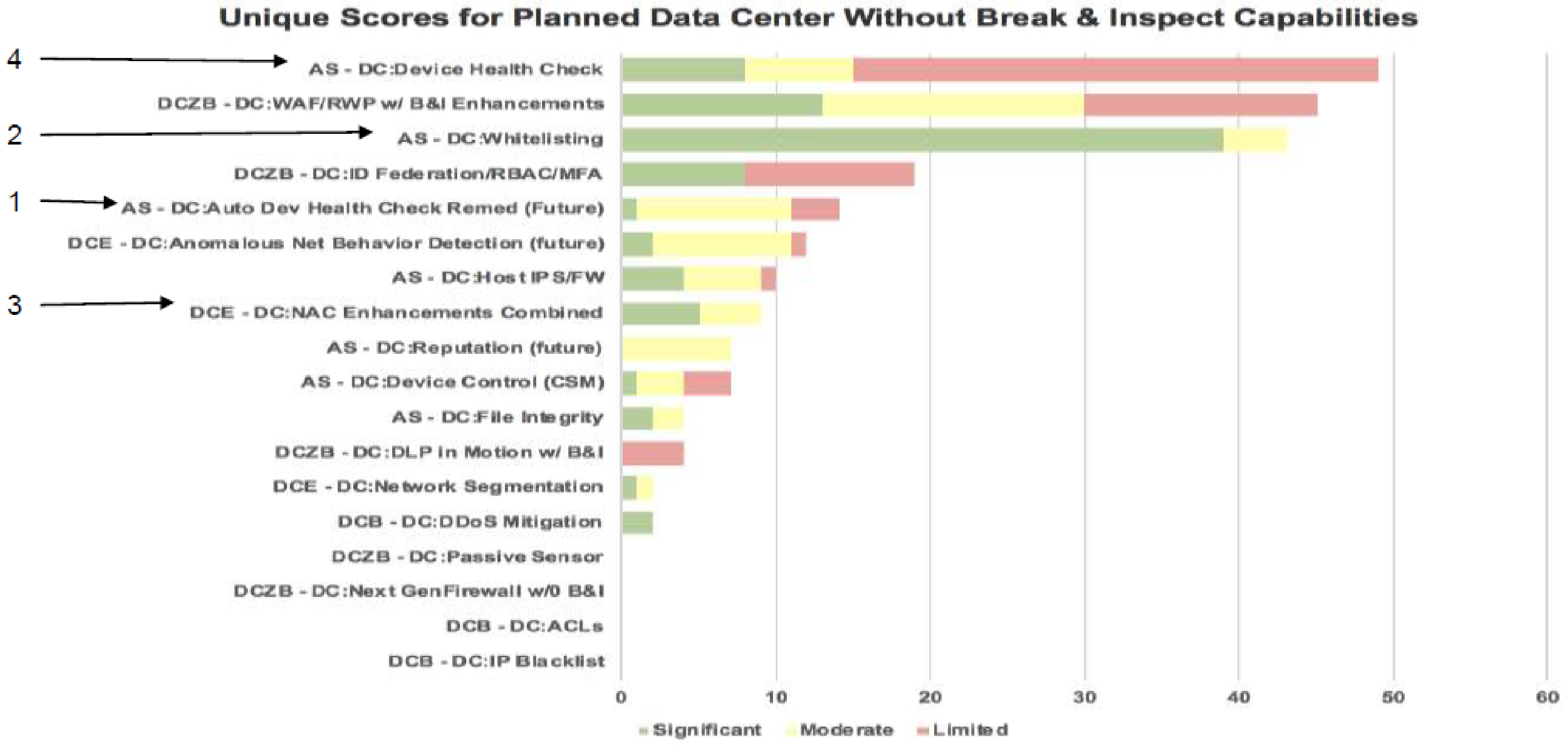
FedRAMP Control

# 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.

| | Current | Future |
|---|---|---|
| 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

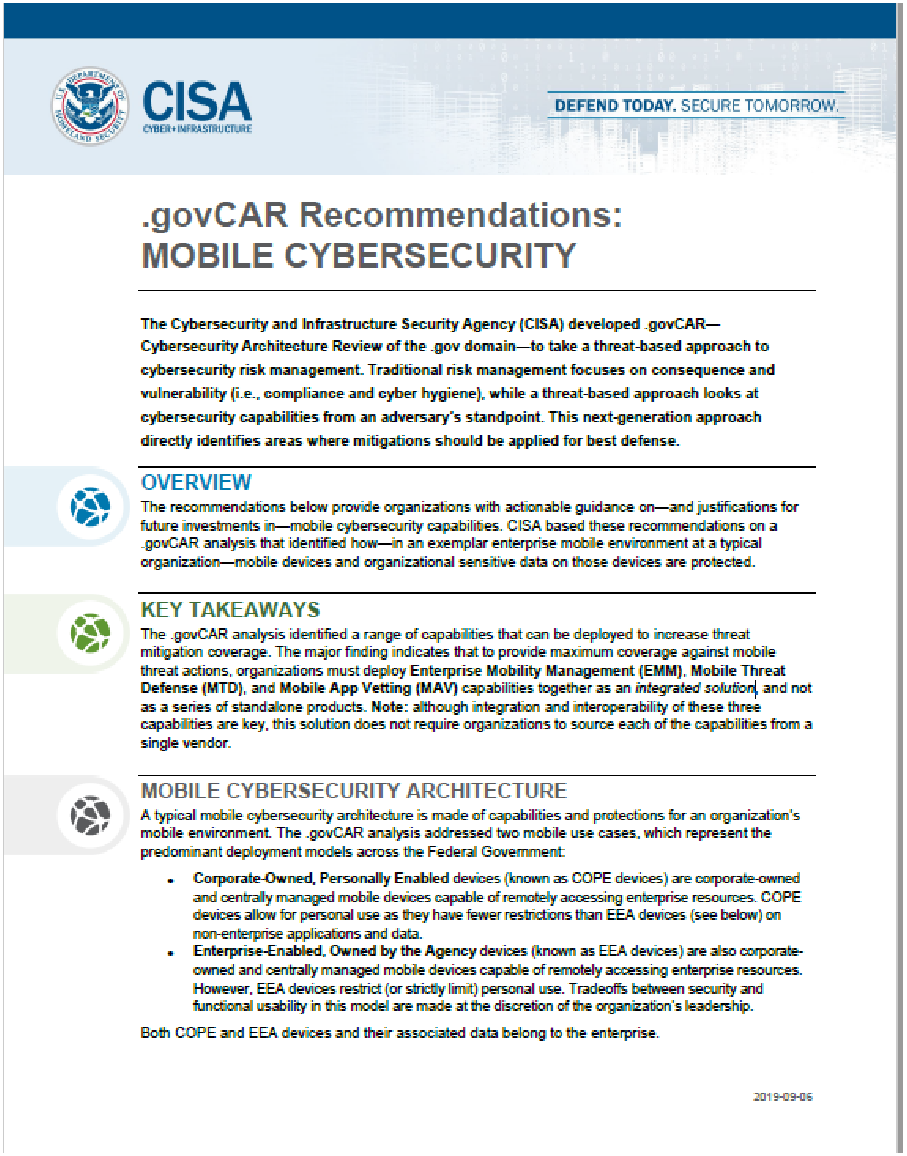


Best Capabilities are also unique in the threat actions that they cover

# .govCAR goals

- Inform DHS's approach to assisting Departments and 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 Departments and 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

# .govCAR Mobile Recommendations

**KEY TAKEAWAYS**

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.

**MOBILE CYBERSECURITY ARCHITECTURE**

.govCAR analysis addressed two mobile use cases **Corporate-Owned, Personally Enabled (COPE)** and **Enterprise-Enabled, Owned by the Agency (EEA)** devices. Tradeoffs between security and functional usability in this model are made at the discretion of the organization's leadership.

**MOBILE CYBERSECURITY CAPABILITIES**

.govCAR analysis revealed that —when **used together in an integrated solution** – EMM, MTD, and MAV capabilities - provide maximum coverage against mobile threat actions.

**MOBILE DEVICE SECURITY**

Although there are no current regulatory requirements that mandate the responsible selection of mobile devices for the Federal Civilian Executive Branch, agencies should **consider supply chain risks** and maintain their own **approved product lists (APLs)** or use those developed by organizations such as the National Information Assurance Partnership, which maintains the Protection Profile for Mobile Device Fundamentals (PP_MD).

**RECOMMENDATIONS**

The results of .govCAR analysis strongly suggest that organizations consider all three dimensions of risk and use the following lifecycle model:

**Stage One – Device Selection**

**Stage Two – Deployment Model Selection**

**Final Stage – Mobile Cybersecurity Capabilities Integration**: invest in and deploy EMM, MTD, and MAV capabilities together, as an integrated solution.

# OMB Max Repository

.govCAR Home
(permalink https://community.max.gov/x/FqVIY )

Technical Annex Documents - Restricted Access
(permalink https://community.max.gov/x/_9n7YQ )

.govCAR
think like the adversary

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE