# Continuous Diagnostics and Mitigation (CDM) and Mobile Security

*ATARC Federal Mobile Technology Summit*

*August 30, 2018*

# Moving to Stronger Risk Management

## Compliance

## Pre-CDM

Risk determination based on checklist

## Cyber Hygiene

## CDM Phases 1 & 2

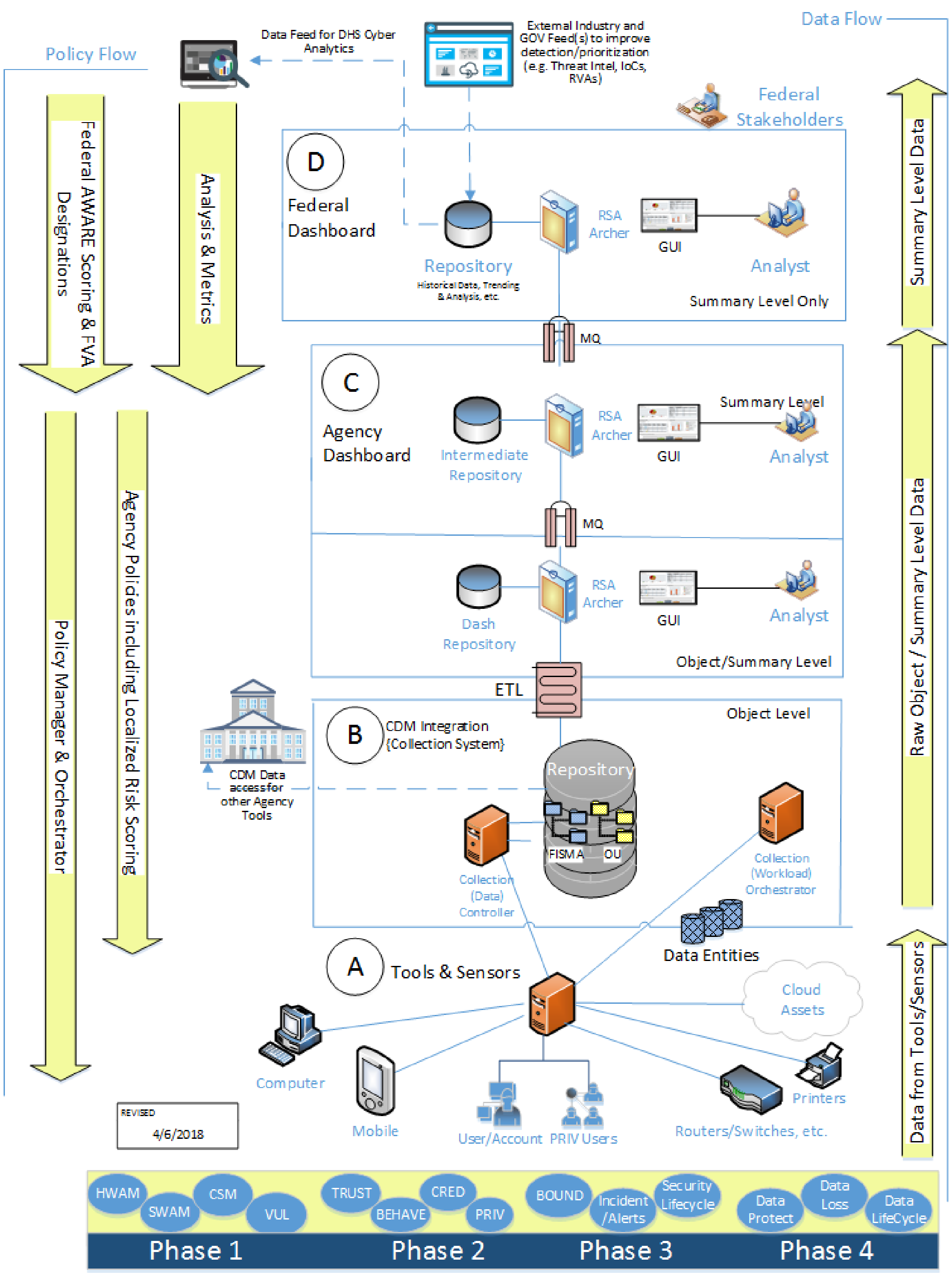
Risk determination based on automated management of assets and accounts

## Threat-based Approach

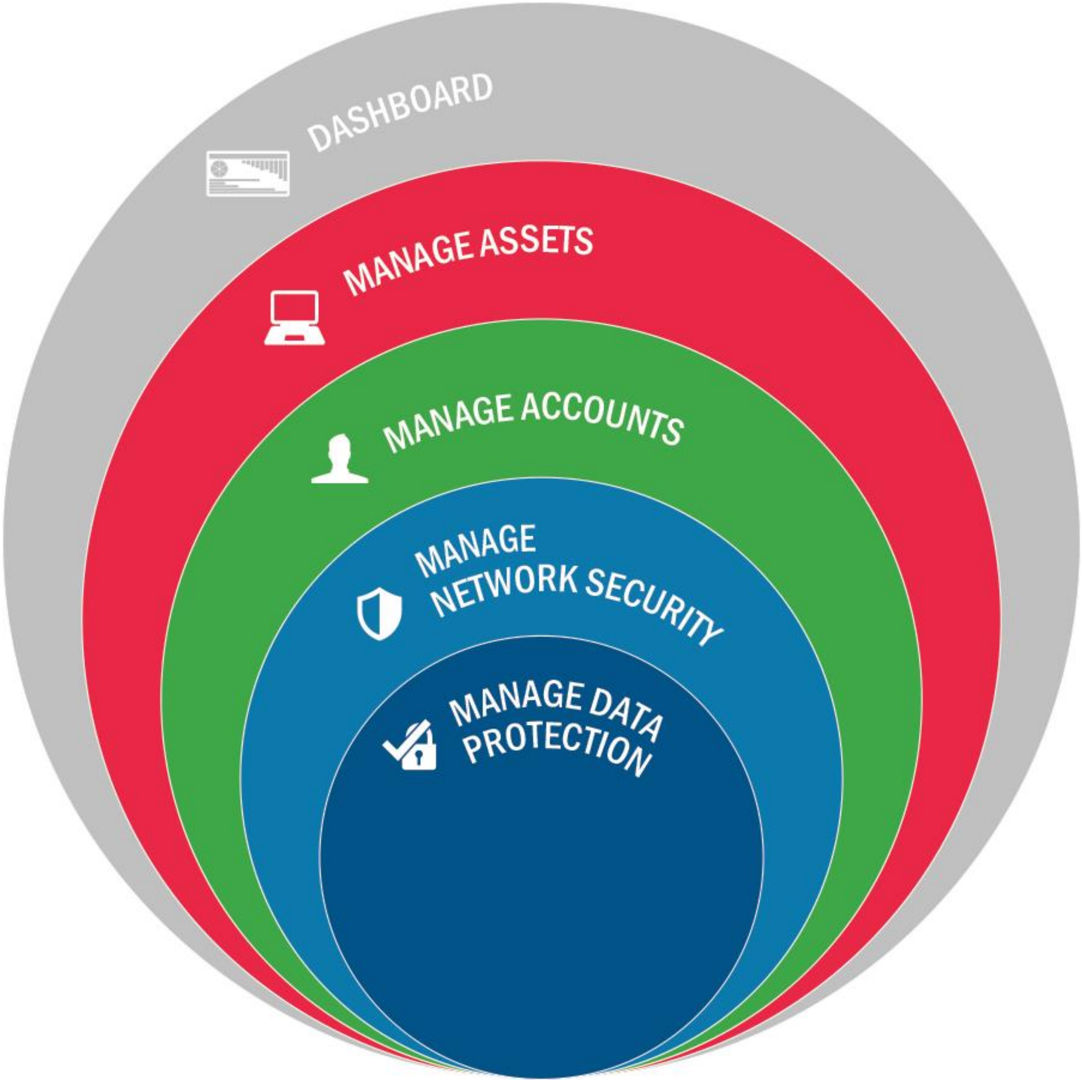
## CDM All Phases

Risk determination based on performance-based measures

# CDM ABCD Architecture



# CDM Capabilities



# Foundational CDM Information Records

MDR

**Master Device Record :** A set of attributes or assertions about a device.

Classes of Mobile devices

MUR

**Master User Record :** A set of attributes or assertions about a user.

Handling of Derived Credentials

MSR

**Master System Record :** A set of attributes or assertions about a system. The MSR is associated with the MDR.

Reporting on the Authorized Mobile System

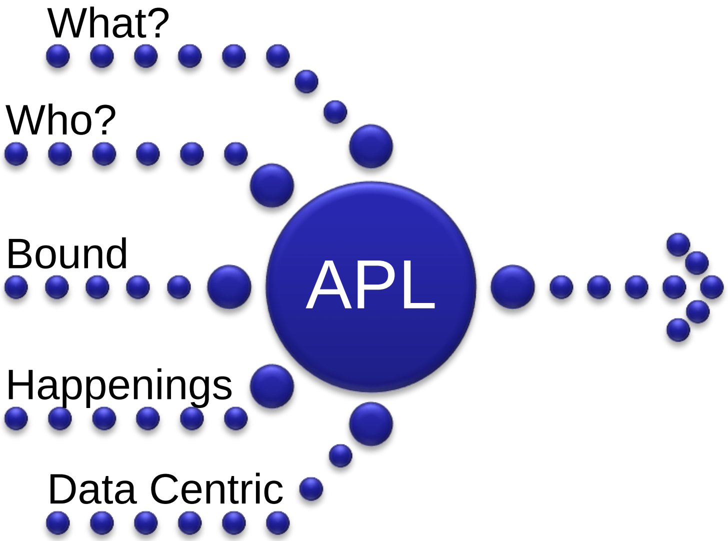
MIR

**Master Incident Record:** Represents activities associated with security controls that require an action when an event occurs.

Handling of “lost” devices

# CDM Acquisition Process

APL continuously updated by DHS to match the cyber security threat tempo

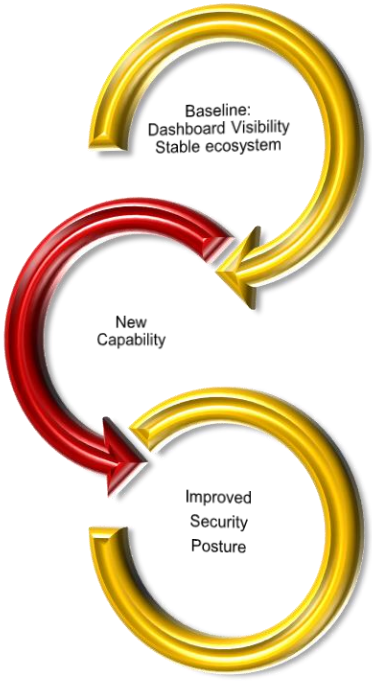


T
O
O
L
S

CDM-SIN Schedule 70 Approved Product List

## DEFEND Task Orders

Request
For Service
Process



# DEFEND Acquisition Strategy

- Dynamic and Evolving Federal Enterprise Network Defense
- Longer period of performances for the task orders (Base + 5 or 6 option years) utilizing Cost Plus Award Fee contract types.
- Advantageous cost and price discounts by continuing to group Agency requirements (Agency groupings will largely remain the same).
- Access to qualified vendors that understand CDM.
- Flexibility and large ceilings on individual orders that can account for:
  - Dynamic cyber environment
  - Varying priorities and timelines
  - DHS/CDM and Agency funding sources
- Flexibility achieved by the Request for Service (RFS) process

# Why is Mobile Different:  CDM Phase 1 Challenges

| | | |
|---|---|---|
| Well established CVE progress | VUL | New classes of VUL/Attacks identified |
| Agency Defined Benchmarks defined from USG mature standards | CSM | Multi-Party selected SRGs, consumer control dominated |
| Agency controlled Library of approved, deployed SW | SWAM | Consumer Selected SW (Appstores/Marketplace Model) |
| Assets:  Full enterprise management, more consistent (i.e., “Wintel”) | HWAM | Assets:  Highly diverse, often tailored by Service Provider |

**Different Threat Profile[1]:**

- ***Mobile Applications***: Malware and vulnerabilities in mobile apps and systems.
- ***Networks***: Rogue cellular base stations and Wi-Fi access points; Man-in-the-Middle attacks on communications.
- ***Mobile Device Technology Stack***: Delays in security updates and zero-day exploits against software and firmware, particularly the baseband.
- ***Devices***: Loss or theft of a mobile device.
- ***Devices and Applications***: Exfiltration of data without user awareness or consent.
- ***User***:  Phishing, SMSishing, or spoofing.

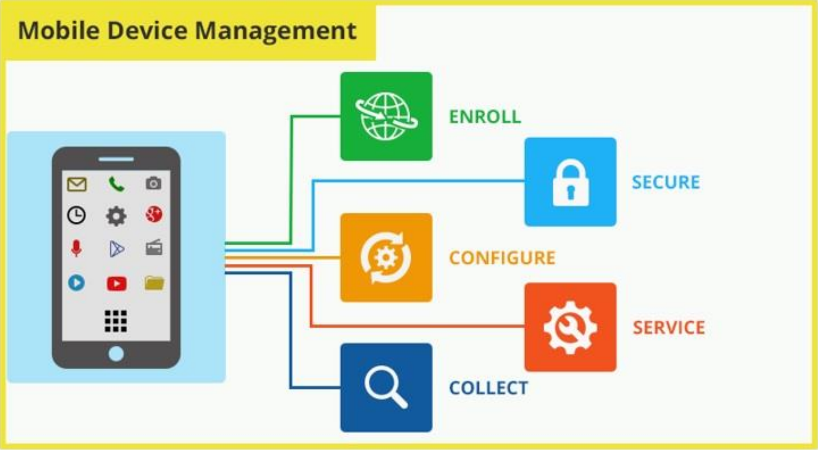
[1] *Study on Mobile Device Security.  DHS Science and Technology.  2017*

# Integration of Mobile into CDM

- "Low drag", new DEFEND contracts allow CDM to provide more surgical help to agencies in the mobile space with minimal contractual overhead (ability to scale from 100s to 100k devices if needed)
- With specialized RFS the program can execute along a pragmatic path:
  - Survey / Develop / Deploy
- Current strategy: to the maximum extent possible, bring "CDM Parity" to mobile devices when compared to other CDM endpoint type devices

# Survey the Current State

- Leverage agency “on-prem” engagements and contracted resources under DEFEND to determine the state of mobile management in the “.gov” space
  - What is being done well, what technologies are being used?
  - What are the gaps/needs?
  - How can CDM help?



- Solicit industry for “best of breed” tools to satisfy the realized mission needs, mitigate the priority threats (e.g., marry lost devices with remote wipe capabilities)

# Develop effective integration approaches

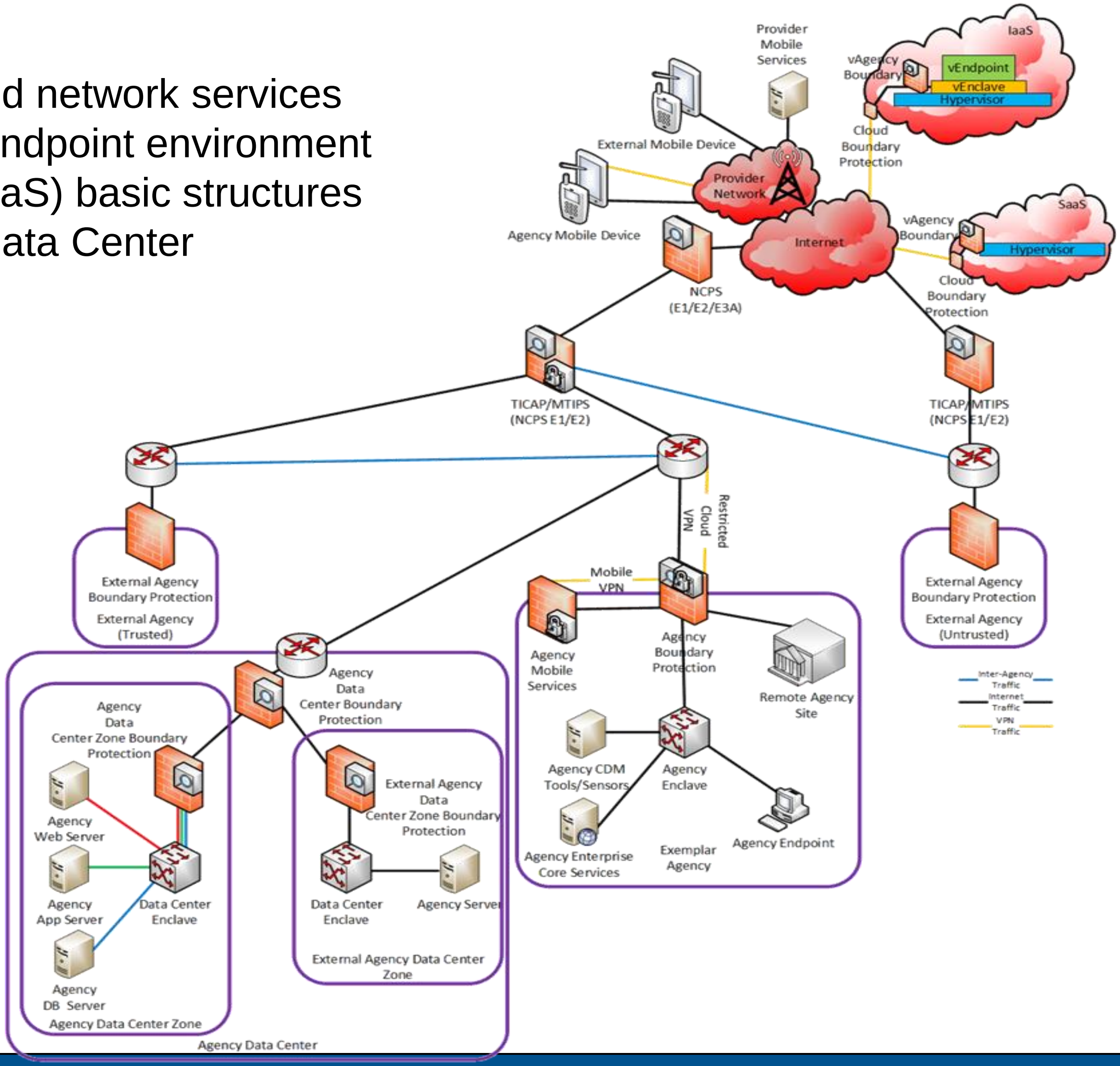
- Align and Refine CDM common architecture to mobile "idiosyncrasies"
  - Not all "MDR"s are created equal!
    - Different data attributes pertaining to differences in mobile (e.g., Cellular Provider related information, IMEI, etc.)
    - Different policy and technical control capabilities depending on tools employed (environmental risks posed by cellular networks are not under the primacy of the Government)
    - CDM Architecture will necessitate a centralized management approach: Data will be centrally collected/reported, individualized mobile assets will not be "chased" for their information
  - Create synergy with existing CDM data constructs (FISMA containers, MUR, etc.)
    - For example:  Mobile opens the door for derived credentials, which can help enumerate new MUR possibilities (Credentials, associated PRIV, etc.)

# Integrate .govCAR findings to CDM priorities

- **.govCAR is a standardized threat-informed approach,**
  - Adopting MTTT Mobile Threat Framework and
  - mobile specific architectural elements
    - using Mobile Security Reference Architecture (MSRA)
    - Also provides basis of use for CDM
- **"scores" the cyber security framework on the effectiveness for Protect, Detect, Respond of**
  - Mobile Threat Actions against
  - Mobile Capabilities (EMM, MTD, etc.)
- **Results in:**
  - Summary of Findings
  - Priority of actions based on responding to Threats

# .govCAR Architecture with Mobile

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**



Provider Mobile Services
IaaS
vAgency Boundary
vEndpoint
vEnclave
Hypervisor
Cloud Boundary Protection
External Mobile Device
Provider Network
Agency Mobile Device
Internet
SaaS
vAgency Boundary
Hypervisor
NCPS (E1/E2/E3A)
Cloud Boundary Protection
TICAP/MTIPS (NCPS E1/E2)
TICAP/MTIPS (NCPS E1/E2)
VPN
Restricted Cloud
External Agency Boundary Protection
External Agency (Trusted)
Mobile VPN
External Agency Boundary Protection
External Agency (Untrusted)
Agency Mobile Services
Agency Boundary Protection
Remote Agency Site
Agency Data Center Boundary Protection
Agency Data Center Zone Boundary Protection
Inter-Agency Traffic
Internet Traffic
VPN Traffic
Agency CDM Tools/Sensors
Agency Enclave
Agency Web Server
External Agency Data Center Zone Boundary Protection
Agency Enterprise Core Services
Exemplar Agency
Agency Endpoint
Agency App Server
Data Center Enclave
Data Center Enclave
Agency Server
External Agency Data Center Zone
Agency DB Server
Agency Data Center Zone
Agency Data Center