CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) PROGRAM

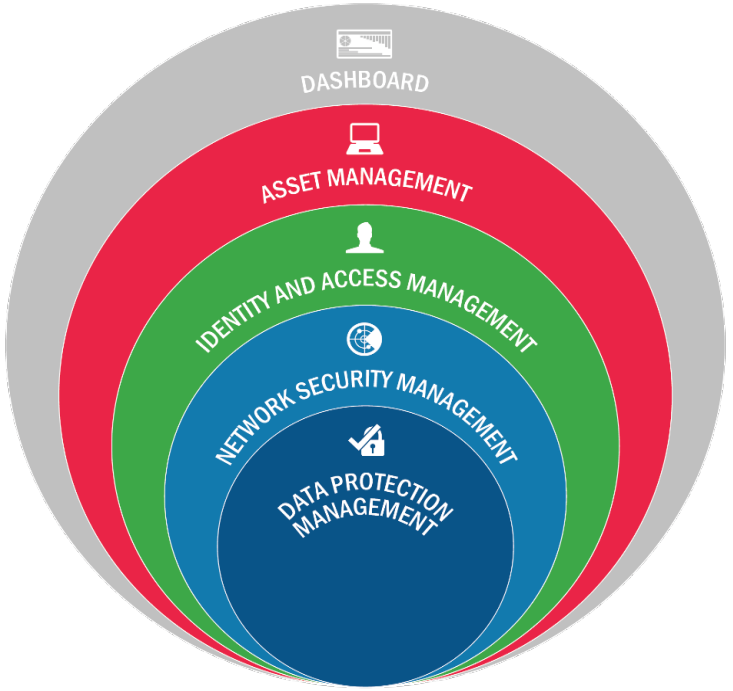
CDM AND FICAM CONVERGENCE

CISA
CYBER+INFRASTRUCTURE

Ross Foard (CDM PMO) & Cathy Hall (Sila Solutions Group)
December 4, 2019

Continuous Diagnostics and Mitigation (CDM) Program

- Established in 2012, CDM provides a consistent approach for cyber security continuous monitoring and mitigation of Information Technology (IT) assets at federal civilian agencies.
- Agency and Federal Dashboards
  - Provide risk information
- Asset Management
  - Hardware, software, vulnerabilities, and configurations
- Identity and Access Management (IAM)
  - User accounts and associated vetting and privileges
- Network Security Management
  - Incident response, ongoing assessments and authorization, boundary protections, and building in security
- Data Protection Management

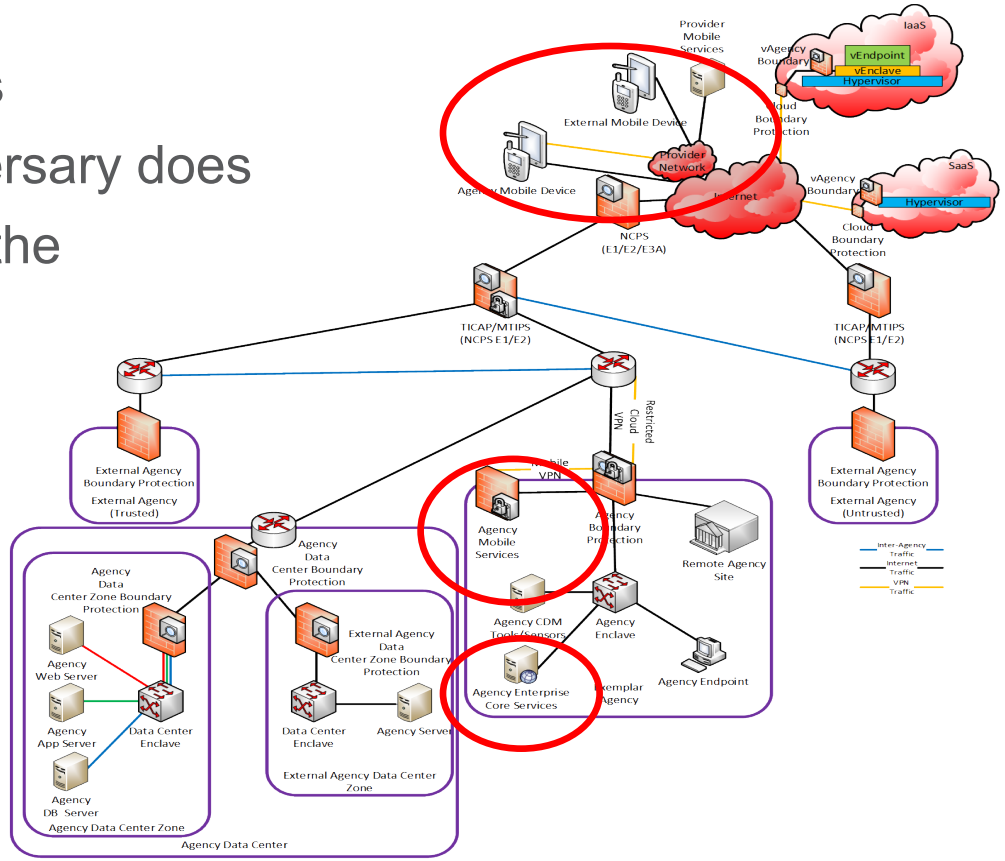


CISA
CYBER+INFRASTRUCTURE

.gov Cybersecurity Architecture Review (.govCAR)

Achieving the Largest Return on Investment Possible: Covering the Basics

- 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
- Highlights gaps and identifies and prioritizes areas for future investments. Also identifies capability overlaps.
- Parallels DoD project known as DoDCAR (previously NSCSAR)

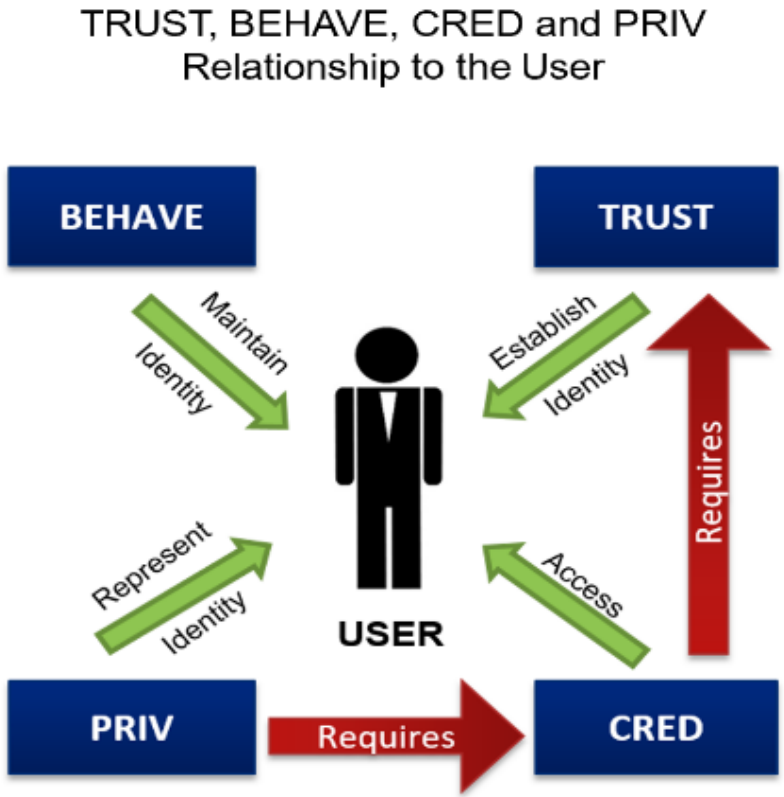


CDM Capabilities are Critical for Cybersecurity Posture

- .govCAR provides operational recommendations for CDM Program requirements:
  - Hardware and Software Asset Management
  - Vulnerability Management
  - Configuration Settings
  - Identity and Access Management
  - Future Capabilities
- CDM Program uses .govCAR analysis in support of a threat-based mitigation approach
- .govCAR analysis identifies areas in Cyber architecture where improvements provide greatest benefit, including Federal Identity, Credential, and Access Management (FICAM) capabilities

CDM View of the Master User Record (MUR)

- The Master User Record is the heart of FICAM for CDM
- It is the basis of the Identity, Credential, and Access Management (ICAM) reporting in Agency Dashboards
- TRUST, CRED, BEHAVE AND PRIV are the capabilities measured



USER is a generic term that applies to any entity (including non-person entities) that access any resource, physical or logical, in an organization.

TRUST is used to validate a person's identity and the degree to which they have been vetted.

CRED is a digital representation of a user and binds a type of credential or authentication mechanism to an identity established in TRUST with a level of assurance and is used to grant access (physical and logical).

PRIV establishes the privileges associated with the credential and in turn the individual or service

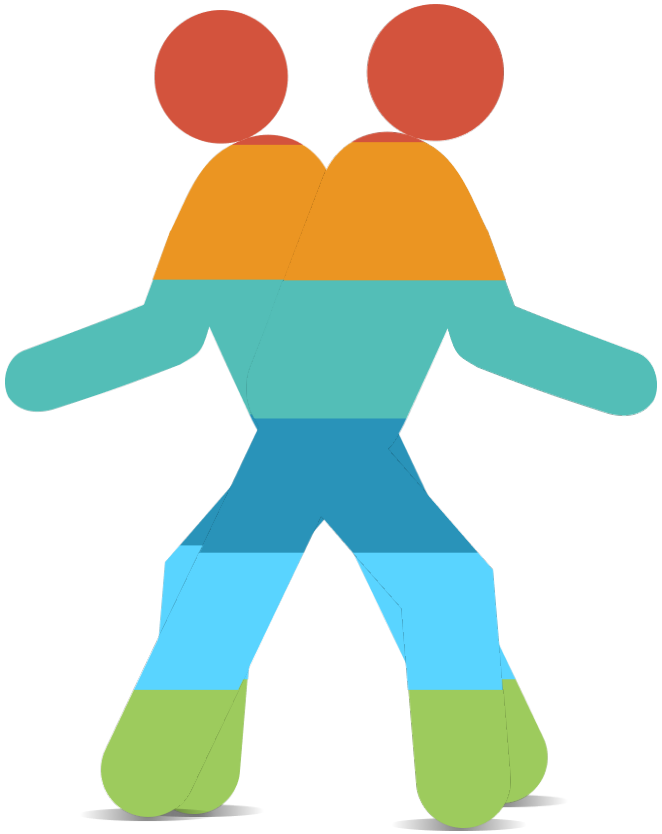
BEHAVE identifies that the individual has the proper knowledge and training for the roles they are assigned and that they remain up to date.

CISA
CYBER+INFRASTRUCTURE

OMB M-19-17 – Modernizing ICAM

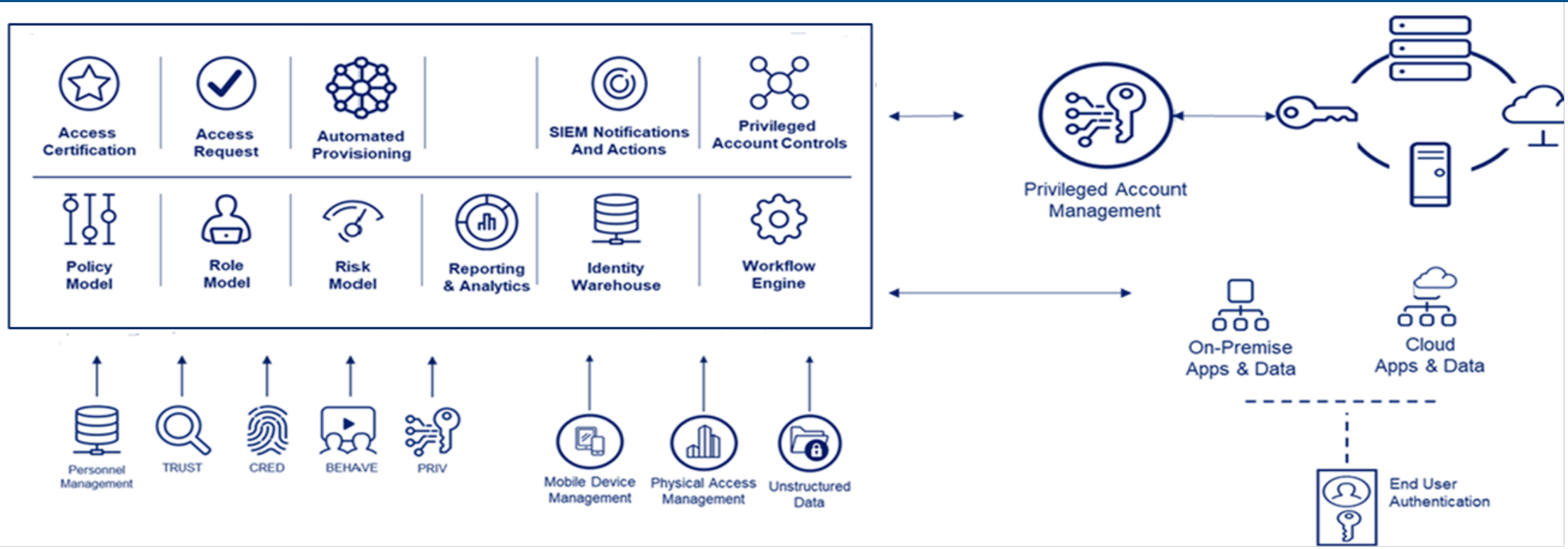
- Move from “lifecycle of credential” to “lifecycle of identity”
- Move from NIST LOA to 800-63 IAL, AAL, and FAL
- Incorporate digital identity risk management
- Evaluate and adopt more options in authenticators
- Enable federation – between agencies and with citizens
- Governance at the highest levels and across agencies
- Share identity proofing data to reduce collection of personally identifiable information (PII)

Identity Lifecycle Management (ILM) with Privileged Access Management (PAM)



- PRIVMGMT and CREDMGMT were first task orders and gapfills are occurring now
- ILM is foundational to managing access control
  - Managing users in context – the lifecycle of the user
  - Sometimes expressed as joiner-mover-leaver
  - In the federal government, we align the joiner event with the issuance of the Personal Identity Verification (PIV) card
  - Entitlements as one changes jobs or leaves the government are important to manage properly

CDM IAM with PAM integration Architecture



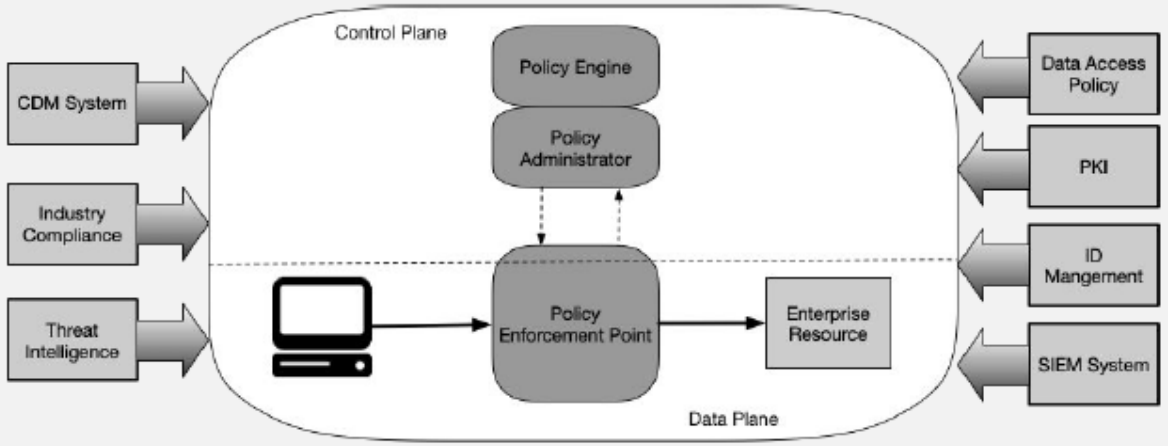
- TRUST, CRED, BEHAVE and PRIV capabilities are reported from the MUR
- The next set of CDM IAM services will focus on managing risk, especially of privileged users, through additional tools and capabilities such as provision/de-provision and role management

Tenants of Zero Trust

- All enterprise systems are considered resources
- The enterprise ensures all owned systems are in their most secure state possible
- All communication is done in a secure manner regardless of network location
- Access to individual enterprise resources is granted on a per-connection basis
- User authentication is dynamic and strictly enforced before access
- Access to resources is determined by policy, including the observable state of user, system, and environment

CDM, FICAM, and Zero Trust Architecture

ZTA Logical Architecture



Two separate network planes:

- Control Plane: used by ZT components to set up and manage network
- Data Plane: used by applications for business processes

- Both FICAM and CDM play a key role in the NIST Zero Trust Architecture
- PDPs and PEPs are fundamental elements in both FICAM and CDM
- Risks regarding user and device identity are key to ZTA

Zero Trust Security – Steps to Achieve

- Establish strong identity governance strategy that includes strong authentication methods
- Establish centralized privileged access management strategy
- Application access is centralized and governed – includes access policies and re-certifications
- Analytics provide rich context to access control decisions, enforcement of policies

Protecting High Value Assets (HVA)

- CISA Binding Operational Directive 18-02 - Securing HVAs: https://cyber.dhs.gov/bod/18-02/
- As part of Agency strategic, enterprise-wide view of cyber risk that unifies the effort to protect HVAs against evolving cyber threats FICAM and CDM can support that effort by:
  - Accelerating CDM capabilities to focus on the HVA
  - Provide additional capabilities beyond those tools that are in the CDM pipeline
  - Taking a risk-based approach to protecting HVAs

CISA

CYBER+INFRASTRUCTURE