- BBFF
- IPMSCG Overview
- IPvMWG Overview
- IPvM CONOPS Development
- Biometric Equities

# Biometrics-enabled Business Function Framework (BBFF)

- The Biometrics-Enabled Business Functions Framework (BBFF) is intended to facilitate evaluation and integration of biometrics technologies into DoD business processes to increase effectiveness, efficiencies and accuracy while complying with DoD privacy, security, and information exchange policies/requirements.

- The BBFF has three critical perspectives:
  - **Strategic** – Authorities (Identity, Access Control & S&T)
  - **Operational** – Policy & Acquisition (implementing solutions)
  - **Technical** – biometrics technologies & biometrics solutions / systems

- The Friendly Biometrics BCF2011 Track has a focus on collecting community feedback to enable the development of the BBFF.

2011 DoD BIOMETRICS COLLABORATION FORUM

• 05 Oct 99, Public Law 106-65 - Congress directed <u>a Senior Coordinating Group for Smart Card Technology</u> w/ DoD CIO oversight

• 0 Nov 99, Deputy Secretary of Defense Memo, Smart Card Adoption & Implementation - <u>destablished the Smart Card Senior Steering Group and defined the Smart Card Senior Coordinating Group (SCSCG) and the Smart Card Configuration Management Control Board (SCCMCB)</u>

- **IPMSCG is the nexus for friendly forces Identity Protection & Management (IPM)**

•31 Aug 02, DoDD 8190.03, Smart Card Technology – <u>unified the role of the SCCMCB with the SCSCG</u>

•12 Jan 04, DoD CIO Memo established the Identity Management Senior Coordinating Group (IMSCG) in place of the SCSCG and <u>outlined the Biometric Management Office to provide executive secretariat</u> support along w/ CAC and PKI offices.

- **Biometrics is a recognized critical enabler for friendly forces IPM challenges**

•19 Jul 04, Certified Current 23 Apr 07, DoDD 1000.25 Personnel Identity Protection (PIP) Program <u>rename IMSCG as the Identity Protection Management Senior Coordinating Group (IPMSCG)</u> and establish Joint oversight between USD (P&R) and DoD CIO.

DoD Identity Management (IdM) Implementation Guidance

5
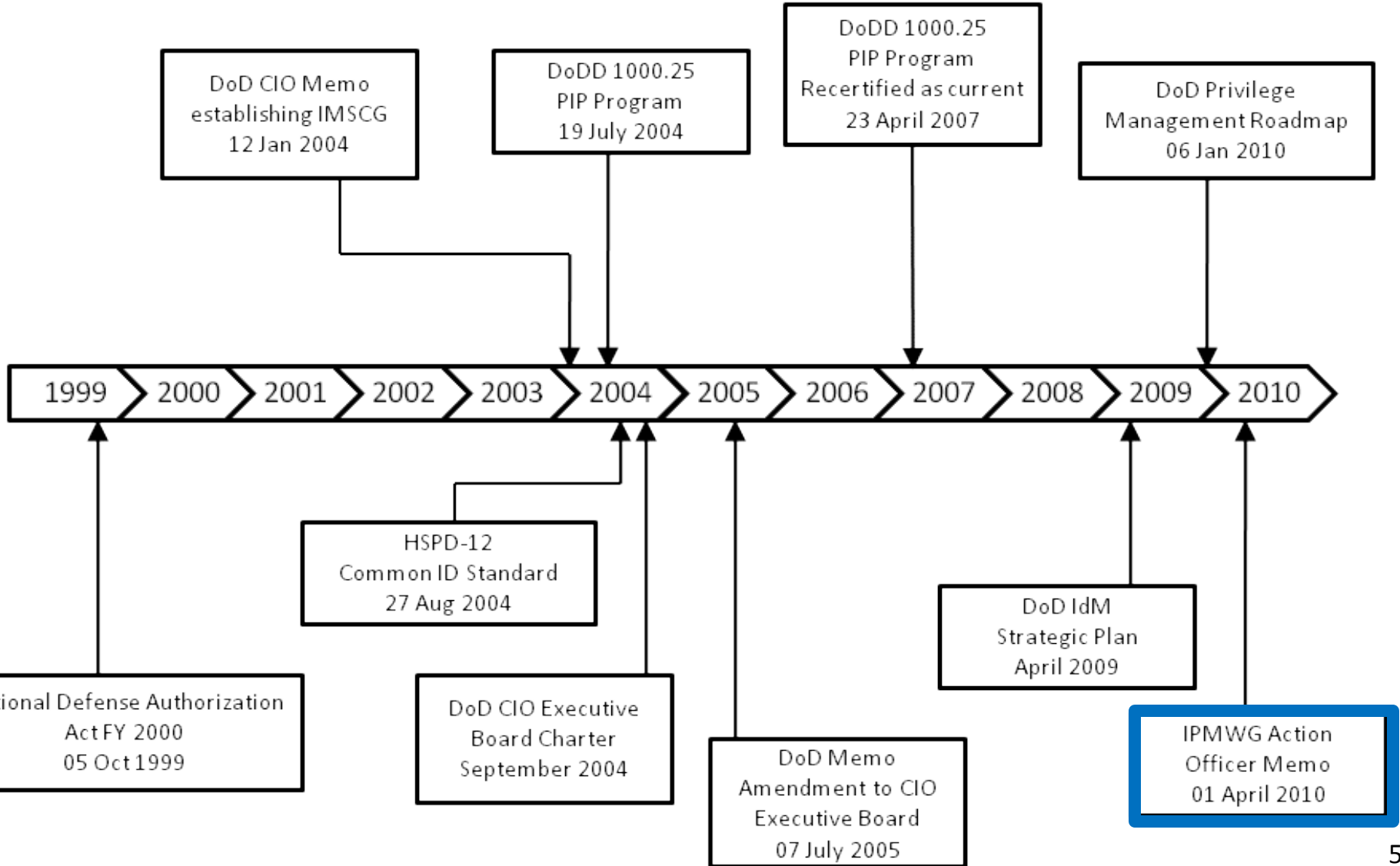
IPvMWG Responsibilities

- Lead the implementation of the DoD Identity Management Strategic Plan and DoD Privilege Management Roadmap

- Develop IPvM Roadmap & Milestones

- Transition IPMSCG approved Identity and Privilege Management (IPvM) recommendations into implementable activities

- Synchronize and coordinate IPvM efforts across the DoD and with federal partners

- Participants:
  - DoD Components
  - Military services
  - DoD Agencies

IPvMWG Progress Update

DoD IdM Strategic Plan
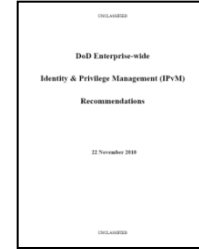
Signed by
DoD CIO
USD (P&R)
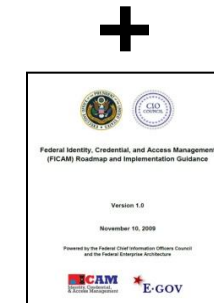USD (I)
USD (AT&L)
USD (P)
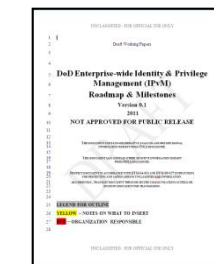**Apr 2009**

DoD PvM Roadmap

Signed by Dep CIO
Jan 2010

DoD Enterprise-wide IPvM Recommendations

Approved by
IPMSCG chair
September 2010

Develop the Strategy

Stage **1** ✔

Identity Management Strategic Plan (2009)

Privilege Management Roadmap (2010)

Stage **2** ✔

Translate the Strategy

FICAM Roadmap & Implementation Guide (draft) November, 2009

Enterprise-wide Identity and Privilege Management (IPvM) Recommendations (2010)

Stage **5**

Test and Adapt the Strategy
- Conduct profitability analysis
- Conduct strategy validation and testing (data from strategy map and BSC)
- Examine emerging strategies

Strategic Plan
- Objective alignment with Challenges

results

Stage **4**

Monitor and Learn
- Hold strategy reviews
- Hold operational reviews

Implementation Plan

Implementation Activities

Enterprise-wide IPvM Roadmap & Milestones (2011)

Stage **3**

In Progress

DoD IPvM Roadmap (draft)

Implements to Support

DOD IT CONSOLIDATION ROADMAP

DoD IT Consolidation Roadmap (draft)

Execute Implementation Guidance
- Execute Processes and Initiatives (Pilot)
- Community wide implementation

UNCLASSIFIED

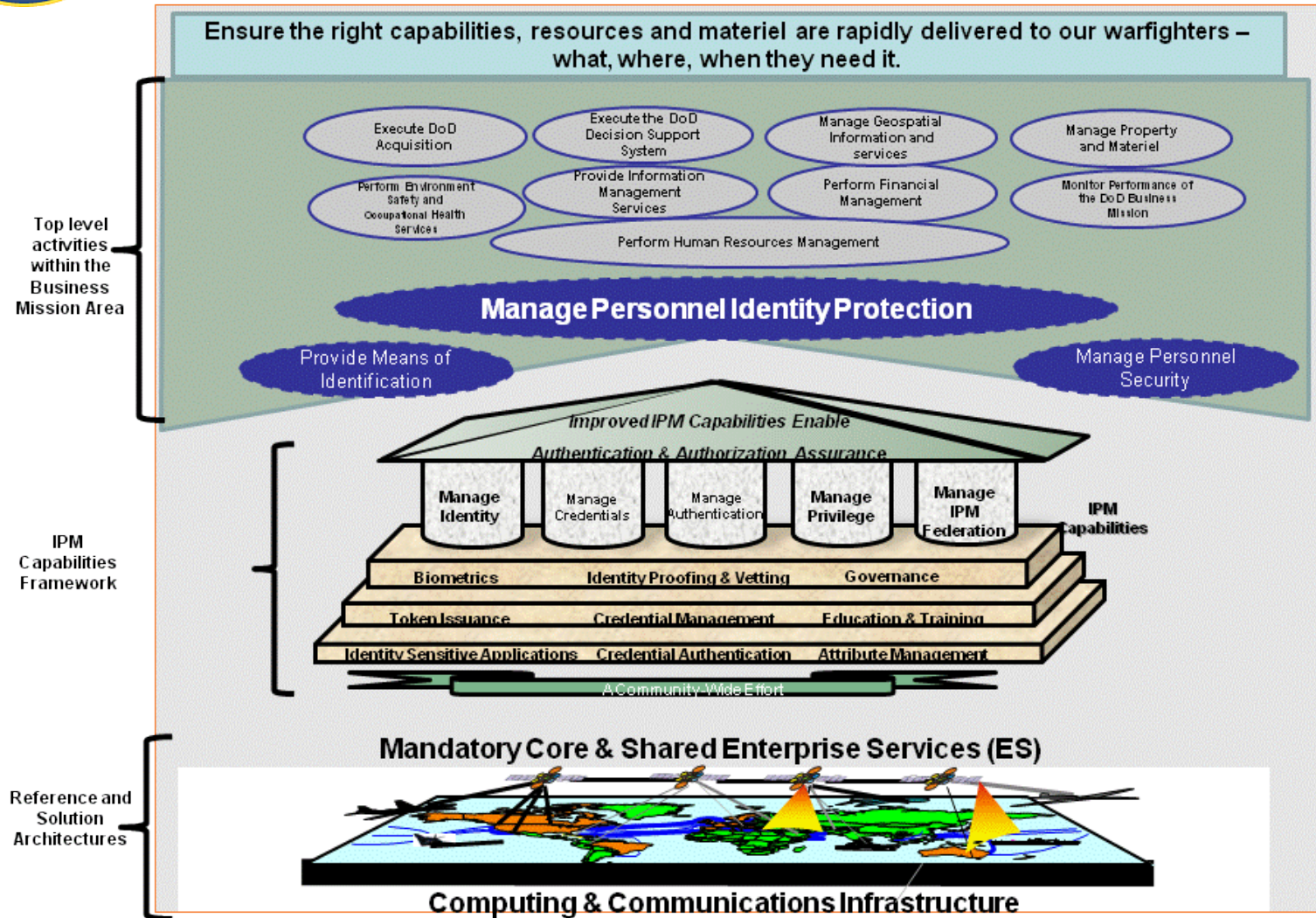# IPvM Strategic Plan Goals

- Goal 1: Unity of Purpose for Effective Governance and Employment of IPvM

- Goal 2: Institutionalize the DoD IPvM capability and culture across the Department

- Goal 3: Build, deploy, operate and maintain a reliable, interoperable and secure IPvM capability

Identity & Privilege Management (IPvM) in the Business Enterprise Architecture (BEA)

IPvM "Cornerstone" Recommendations

1. **Execute IPvM performance management**
   – Develop an IPvM Roadmap & Plan of Action & Milestones (POA&M) and measure progress of the integration of interoperable IPvM capabilities across DoD Mission Areas
   – Utilize existing governance structures (IPMSCG, DAWG, etc.)

2. **IPvM Outreach to Functionals across DoD and beyond:**
   – Work with functional area architectures advocating priorities important to IPvM to institutionalize integrated & interoperable IPvM IT Investment Review Board decision-making across the DoD Business Enterprise
   – Promote the interdependencies between mission areas regarding IPvM capabilities
   – Coordinate and synchronize activities with ICAMSC and AASC
   – Enhance cyber security through DoD Enterprise-wide Identity & Privilege Management

3. **Organize, update, amplify existing architectures and embrace federated architectures**
   – Integrate IPvM capabilities into DoD Mission Areas (BMA,WMA,IMA)
   – Force IPvM compliance through funding constraints
     • Insert IPvM criteria into the USD P&R Human Resources Management (HRM) Enterprise Architecture (EA) and ultimately into the Business Enterprise Architecture (BEA)

Authority: IPMSCG Chair approved the cornerstone recommendations and assigned the IPvMWG to execute the development of the Roadmap & Milestones

UNCLASSIFIED

Tentative IPvM Roadmap Timeline

2011											
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

IPvM CONOPs
- Develop
- Staff

IPvM Activities & Milestones
- Develop

IPvM Roadmap
- Draft

Staff IPvM Roadmap
- IPvMWG
- IPMSCG

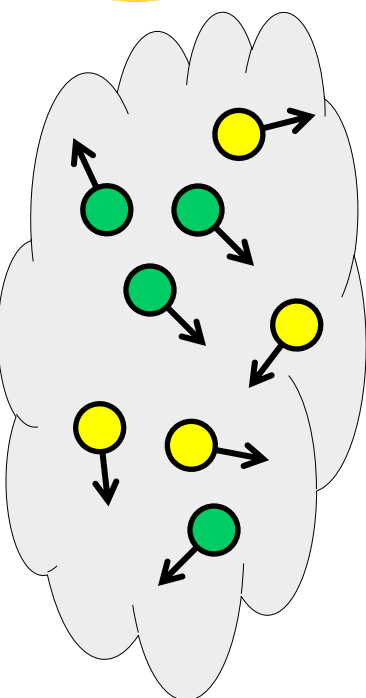DoD CIO Signature

DAWG
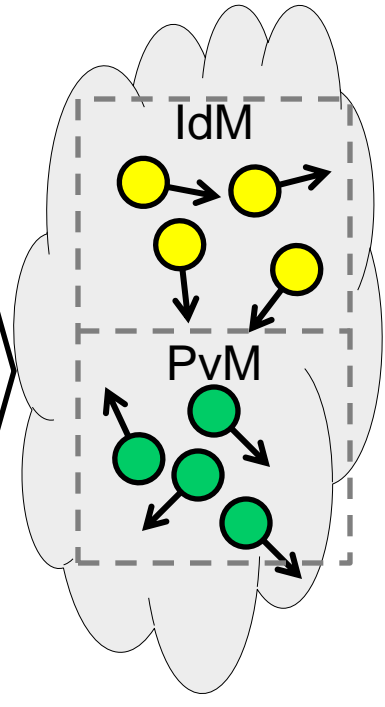- Staff

DAWG Approval

UNCLASSIFIED
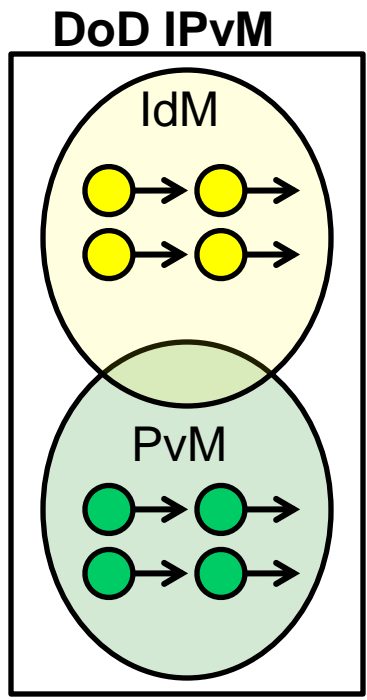
11

Stages of IPvM CONOPS Development

IPvM Scenarios

• help define scope of IPvM activities
• help define what we consider IdM
• help define what we consider PvM

IPvM CONOPS

• defines scope of IPvM activities
• defines IdM at a high-level
• defines PvM at a high-level
• defines IdM to PvM Transition
• defines IPvM key terminology

DoD IPvM

IdM

PvM

Current State – IPvM is not a recognized, managed attribute across the DoD Enterprise

IPvM Scenario Development will help define scope of DoD Enterprise IPvM Road Map impacts and what are existing attributes of Identity Management (IdM) & Privilege Management (PvM).

IPvM CONOPS clearly defines the agreed upon and desired end-state of the IPvM Roadmap & Milestones to focus sub-working group activities.

UNCLASSIFIED

12

Steps towards IPvM CONOPS

- Submit Stakeholder Scenarios
- Validate Identities of Interest
- Develop Conceptual Model / Cartoon
- Identify potential IPvM Use Cases
- Identify notional integration of IPvM Management & Technical Frameworks
- Identify IPvM National Security / Joint War fighting Capability Objectives
- Distinguish between Enterprise and Local IPvM Services

IPvM Identities of Interest

DoD IdM Strategic Plan identities:

- Individuals and Non-Person Entities (NPEs)
  - **Blue / Friendly Forces** - e.g., DoD Civilian, Military, Contractors, Dependents, Vendors, Federal, State, Local, Tribal
  - **Red / Adversary** - e.g., Nation State, Asymmetric
  - **Gray / Neutral** - e.g., US Citizen, Coalition, Not-Adversary but Foreign, Industry, NGOs

These are the IPvM identities of interest to be covered in the Roadmap.

Draft IPvM Scenario Themes

Draft IPvM Scenario Themes
Hiring
Physical Access
Logical Access
Retirement
Financial Transactions
Forensics (red)
Raid (capture/kill)
Media Exploitation
Boarding at Sea
Humanitarian Assistance/Disaster Relief (HADR)

UNCLASSIFIED

Draft IPvM Conceptual "Cartoon" DoD Military and Civilian

Identity Life-Cycle

Establish DoD Identity

- Manage DoD Career Development
- Manage DoD Benefits/Compensation
- Manage DoD Manpower and Health Services
- Unknown

Retire DoD Identity

Transition to VA (Military)

Establish Suitability & Trustworthiness

Manage Trustworthiness via Periodic Reviews

DoD Enterprise

"Local" (Component, Agency, Installation & Facility)

Establish Local Physical Access — Establish Local Logical Access — NETWORK — Execute Mission (Job)

PCS

Establish Local Physical Access — Establish Local Logical Access — NETWORK — Execute Mission (Job)

PCS

Establish Local Physical Access — Establish Local Logical Access — NETWORK — Execute Mission (Job)

USD Personnel & Readiness (P&R)
USD Intelligence (I)
Local commander/resource owner
Veterans Affairs (VA)

Terminology purposely abstracted up to very generic language & Concepts
IPvMWG will mature this "Cartoon" to a Model

16

Human Resource Management (HRM) High-Level Operational Concept Graphic (OV-1)
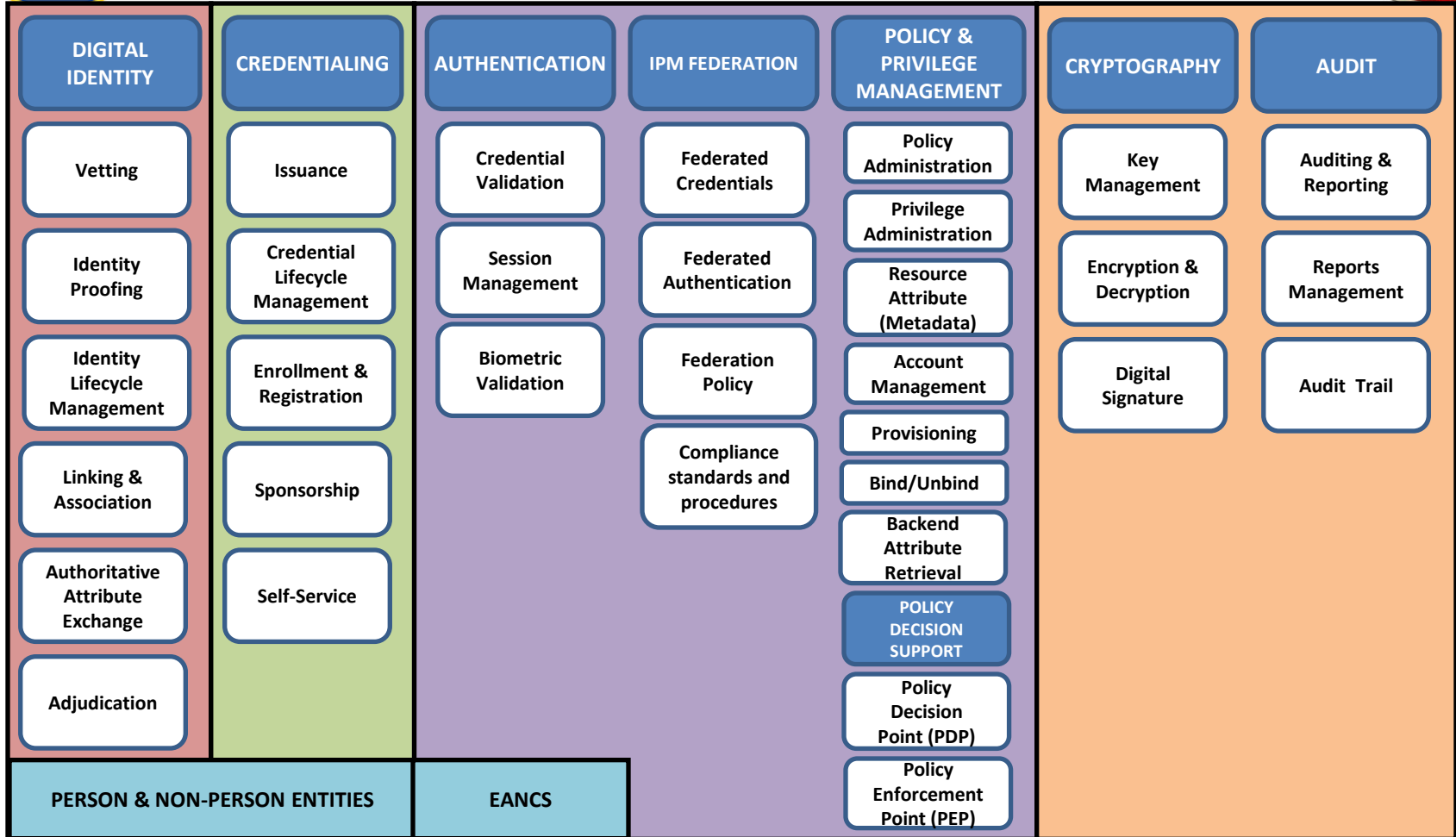

IPvM operational concepts are primarily within the HR Information Security Line of Business (LoB)

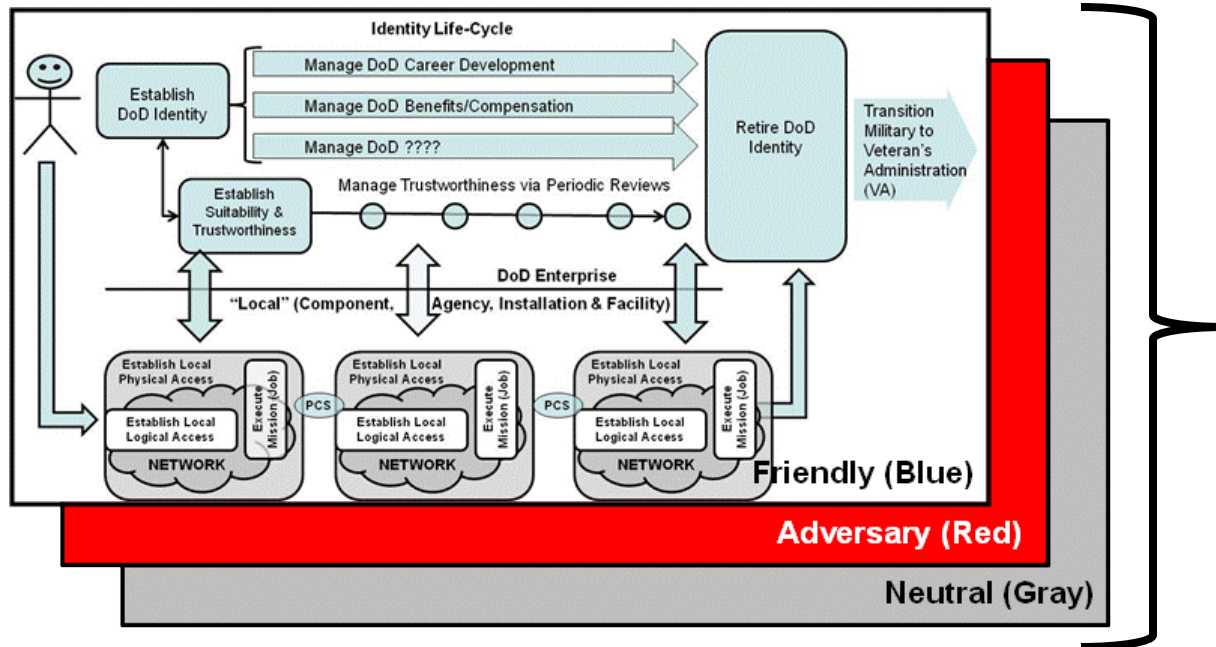Identity and Privilege information will flow in/out of other LoBs (e.g., Retirement, Assignment)

Policy — Customer Service

Records Management

Change Management

Position Management

Military Health Services Management

Human Resources Information Security

Assignment/ Placement/ Transfer

Travel Management

Quality of Life/MWR Management

Personnel/Pay Management

Personnel Development

Legal Affairs

Interagency Support

Recruiting and Accessions

Retirement/ Separation

Law Enforcement

Benefits Management

Managing careers

Maintaining HR Infrastructure Ensuring readiness Providing quality of life

Changing the way HR serves you

Continuous Process Improvement

UNCLASSIFIED

Friendly / Blue : Draft DoD ICAM Framework

DIGITAL IDENTITY	CREDENTIALING	AUTHENTICATION	IPM FEDERATION	POLICY & PRIVILEGE MANAGEMENT	CRYPTOGRAPHY	AUDIT
Vetting	Issuance	Credential Validation	Federated Credentials	Policy Administration	Key Management	Auditing & Reporting
Identity Proofing	Credential Lifecycle Management	Session Management	Federated Authentication	Privilege Administration	Encryption & Decryption	Reports Management
Identity Lifecycle Management	Enrollment & Registration	Biometric Validation	Federation Policy	Resource Attribute (Metadata)	Digital Signature	Audit Trail
Linking & Association	Sponsorship		Compliance standards and procedures	Account Management		
Authoritative Attribute Exchange	Self-Service			Provisioning		
Adjudication				Bind/Unbind		
				Backend Attribute Retrieval		
				POLICY DECISION SUPPORT		
				Policy Decision Point (PDP)		
				Policy Enforcement Point (PEP)		

PERSON & NON-PERSON ENTITIES	EANCS

FICAM Service Area

Notional Integrated IPvM Operational Capabilities

Each major Identity Population have a distinct Management & Technical Services Framework

- **Friendly Goals –** enabled trusted hiring, identity proofing & vetting for access control
- **Adversary Goals** – Find, Fix (Identity), Track & Act against Known or Suspected Threats to US National Security
- **Neutral Goals** – Identity proofing & vetting / Fix, track, other
- **Operational (aggregate) Goals** – Identity "superiority" capabilities that require integration of all of the above to achieve, e.g. *Force Protection; Cyber security; Personnel Recovery; other*

"Hiring" Use Case Process Flow Diagram

Establishing a DoD Identity (Military & Civilian)
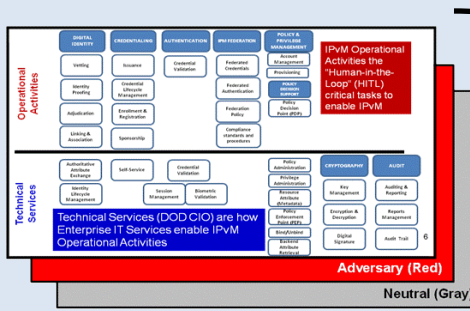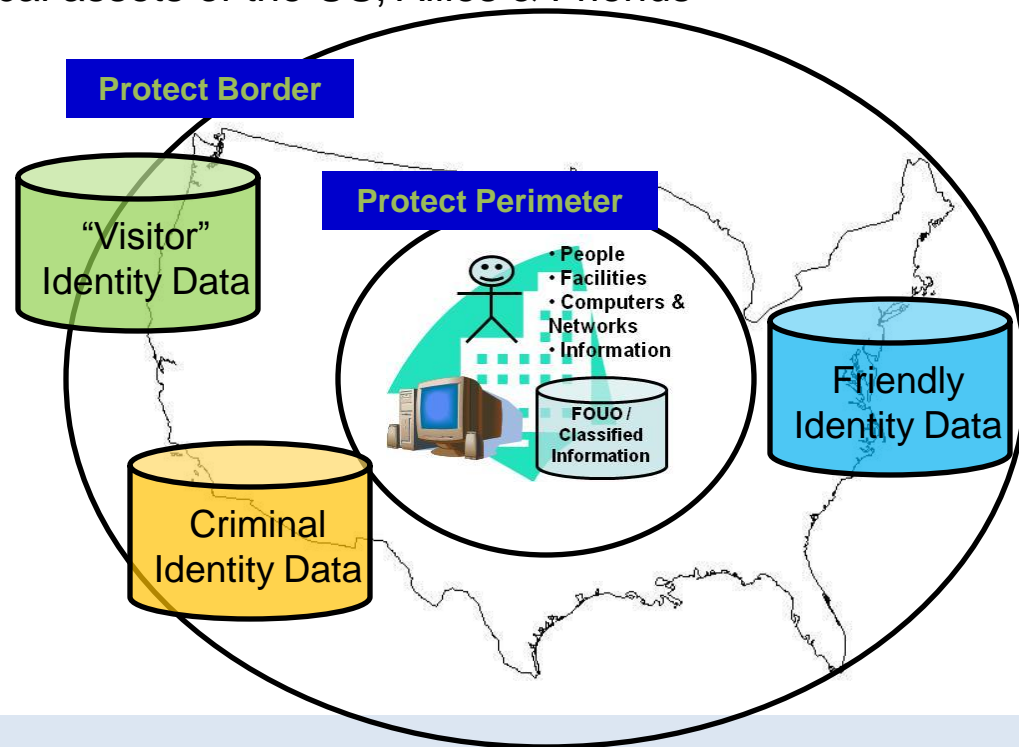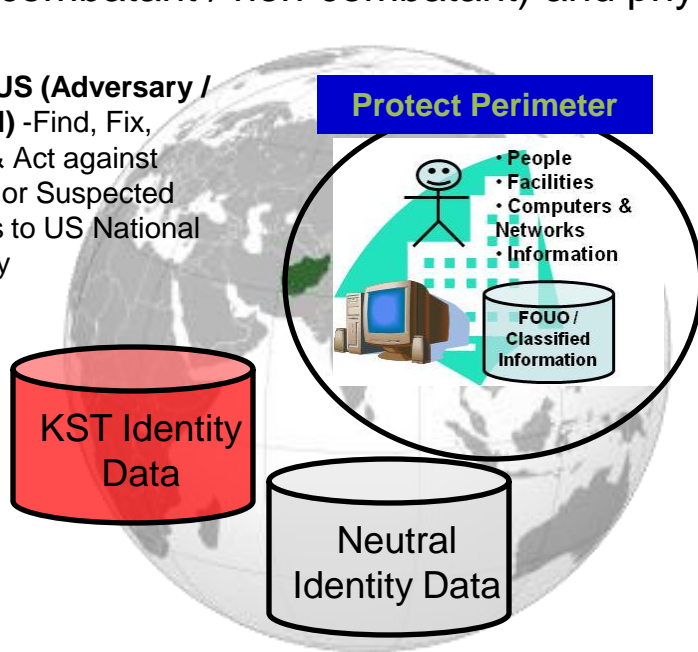
UNCLASSIFIED
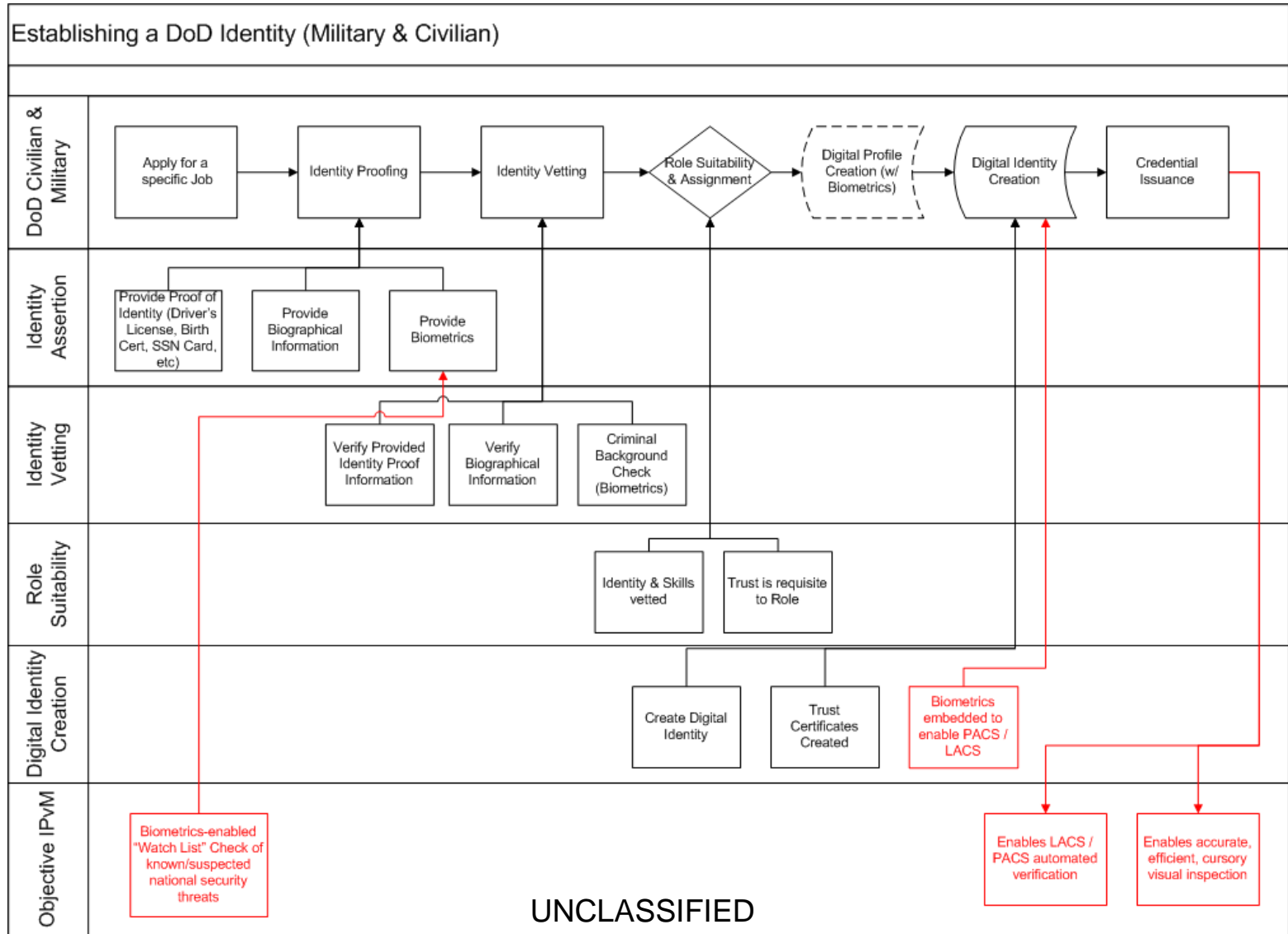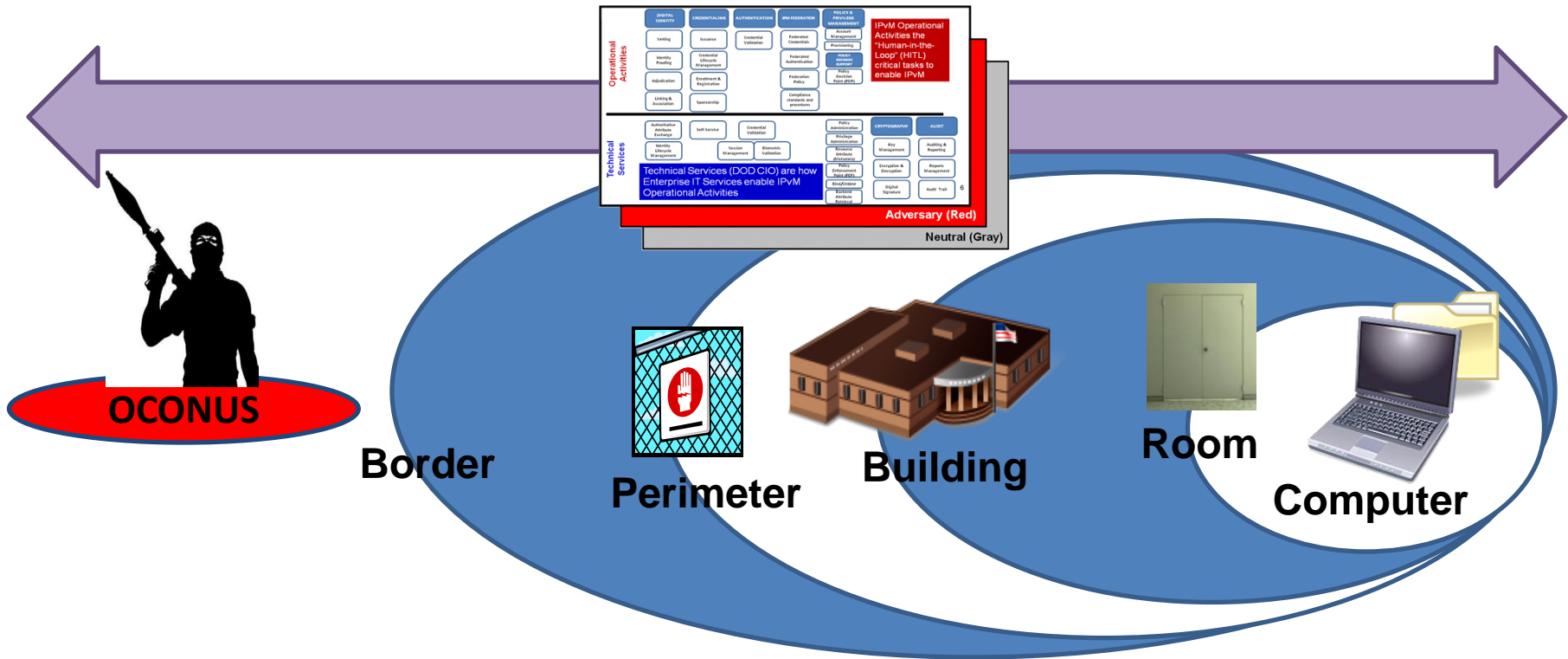
Systems of System (or integrated) IPvM Framework allows for assessing security requirements respective to risk to allow for more streamlined access control policies and processes "deeper" in the secure IPvM enclave.

Force Protection- The ability to prevent/mitigate adverse effects of attacks on personnel (combatant / non-combatant) and physical assets of the US, Allies & Friends

OCONUS (Adversary / Neutral) -Find, Fix, Track & Act against Known or Suspected Threats to US National Security

Protect Perimeter
- People
- Facilities
- Computers & Networks
- Information

FOUO / Classified Information

KST Identity Data

Neutral Identity Data

Protect Border

"Visitor" Identity Data

Protect Perimeter
- People
- Facilities
- Computers & Networks
- Information

FOUO / Classified Information

Friendly Identity Data

Criminal Identity Data

- <u>Manage Identity</u> – across the full spectrum of IPvM Frameworks
- <u>Manage Credentials</u> – to align trusted roles to authorized access
- <u>Manage Authentication</u> – to ensure only authorized access
- <u>Manage Privilege</u> – manage life-cycle of aligned trusted roles & authorized access
- <u>Manage IPvM Federation</u> – Federate to enable IPvM Operational Goals and allow DoD business efficiencies

23

Privacy Compliance - more Systems Engineering than Policy Constraint

Friendly Biometric Systems require Privacy Impact Assessment:

- Collection
  - Signed Consent
  - Disclosure legal authority, handling (collect, store, share), purpose, etc.
- Storage & Share
  - System of Records Notice (SORN)
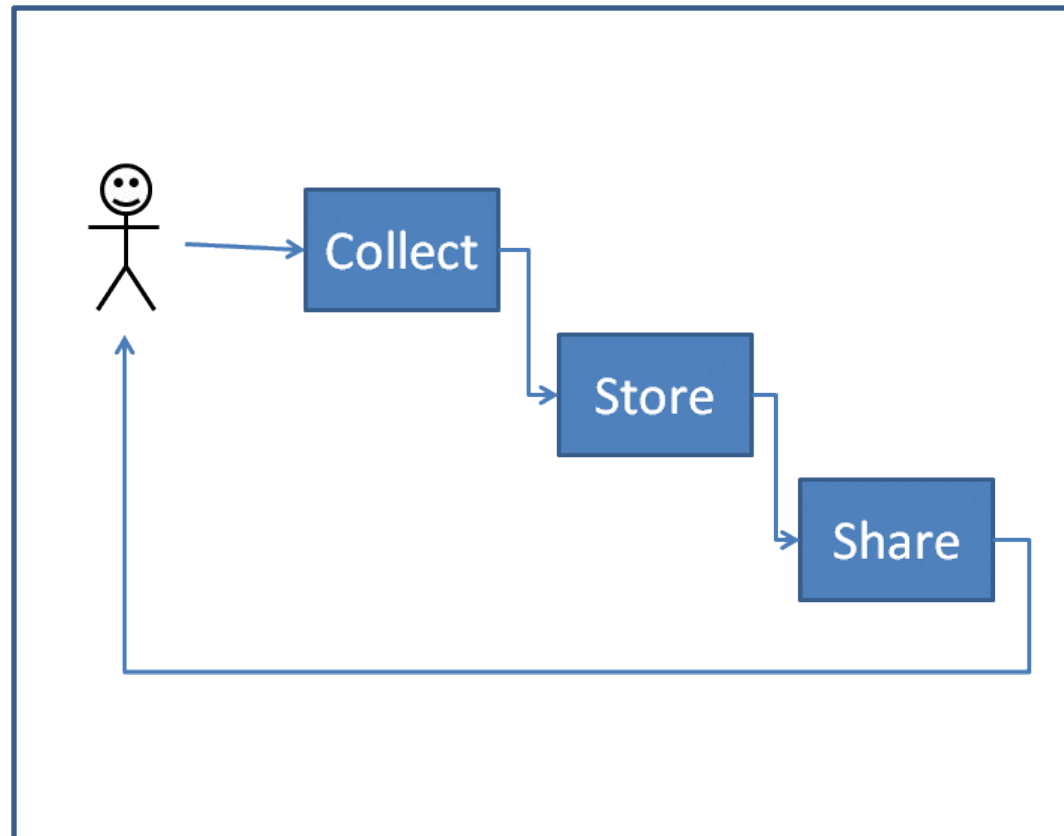
* The Privacy Act of 1974, E-Government Act of 2002 , other…

UNCLASSIFIED

- IPvM Policy & Guidance development & drafting
- **Identity proofing & vetting**
  - New hire
    - New – biometrics-enabled vetting against "Watch List" of known or suspected national security threats, i.e., checks that would result in actions, e.g., detain, deny access, etc.
  - Life-Cycle
- **Create *Digital Profile* to enable Human Resource Management (HRM)**
  - Digital Profile (Draft Definition) – electronic record with biographical, contextual & biometric information that describes a DoD Identity utilized to enable administrative management.
- **Create Digital Identity to enable Access Management**
  - Digital Identity – electronic representation of an individuals identity *to enable granting of privileges*
  - *Does this actually happen locally, is a certificate is all that is created at the enterprise level?*
- **Credential Issuance & Life-Cycle Management**

Note: DoD Services enable privilege management, the provisioning / deprovisioning of privileges and resulting management occurs "locally"
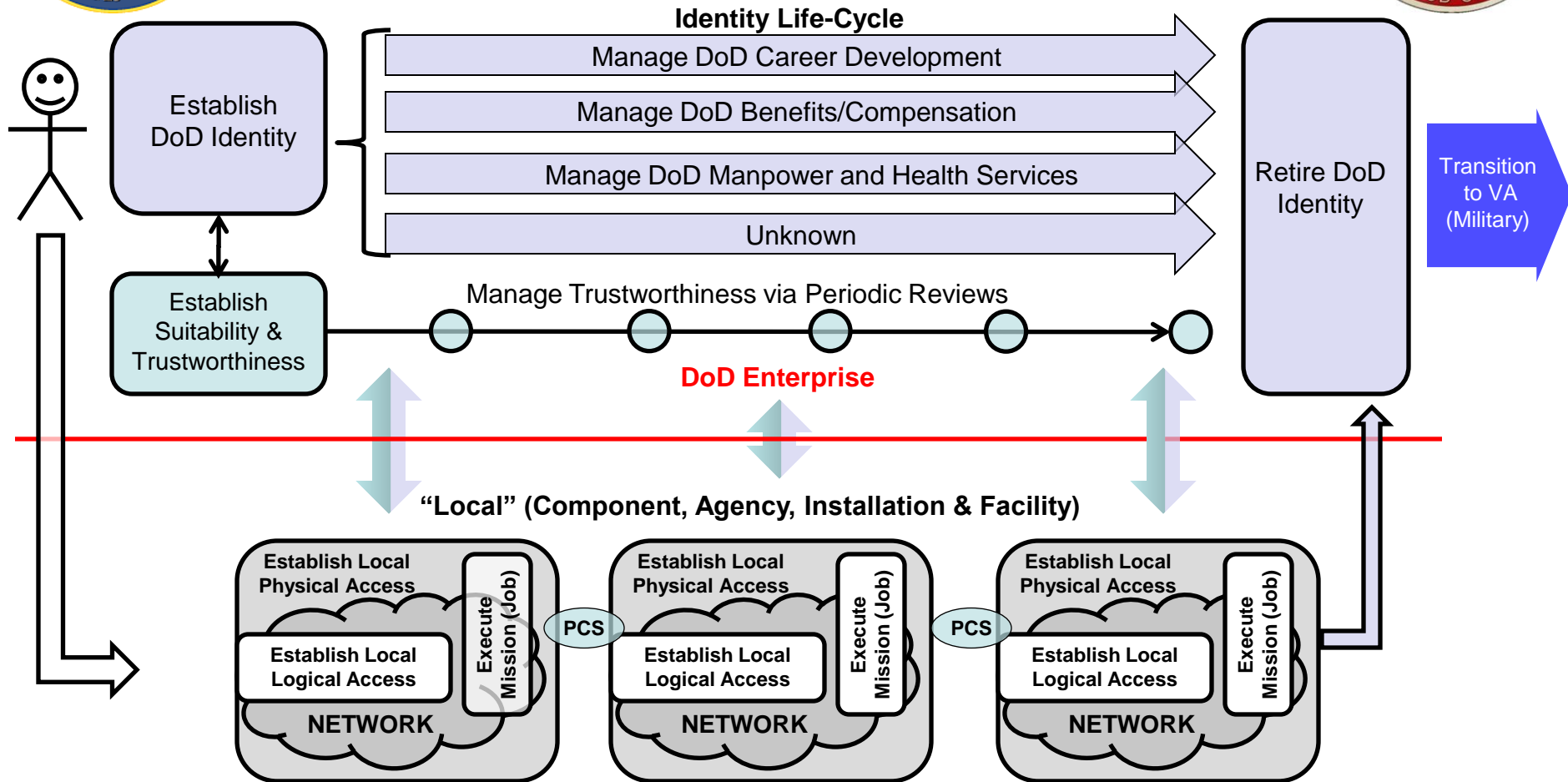
- IPvM Policy & Guidance compliance & refinement
- Identity proofing & vetting
    - Visitors (short-term, limited access requirements) & tenants (TDY or PCS'd personnel and Contractors)
    - "Local Life-Cycle" – ensure access is granted for specific purpose and duration of need/requirement.
    - Really need to understand the policy driven use cases here…
- Leverage *Digital Profile* to enable Human Resource Management (HRM)
    - What are the policy/regulatory use case of PCS or TDY inprocessing????
- Leverage DoD Credential to Create Digital Identity to enable Access Management
    - Verify Trust
    - *Provision Access*
    - *Deprovision Access*
- Credential Issuance & Life-Cycle Management
    - Only applicable for "local" Credential requirements

Note: Local IPvM encompasses role assumption, perimeter access, facilities access, logical access and all associated "Local Life-Cycle" management requirements

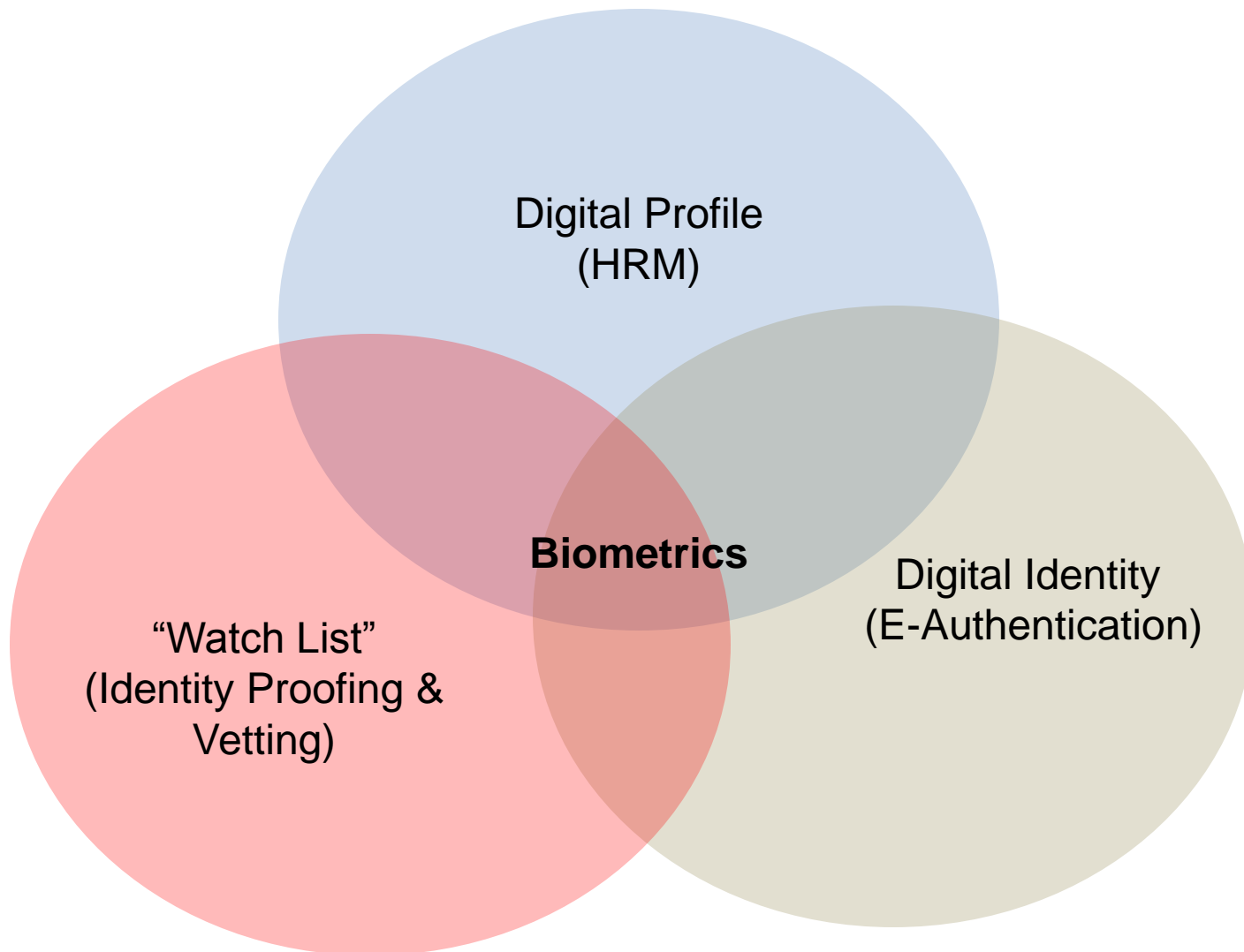# Draft IPvM Conceptual "Cartoon" DoD Military and Civilian

Identity Life-Cycle

Establish DoD Identity

- Manage DoD Career Development
- Manage DoD Benefits/Compensation
- Manage DoD Manpower and Health Services
- Unknown

Retire DoD Identity

Transition to VA (Military)

Establish Suitability & Trustworthiness

Manage Trustworthiness via Periodic Reviews

DoD Enterprise

"Local" (Component, Agency, Installation & Facility)

Establish Local Physical Access

Execute Mission (Job)

Establish Local Logical Access

NETWORK

PCS

Establish Local Physical Access

Execute Mission (Job)

Establish Local Logical Access

NETWORK

PCS

Establish Local Physical Access

Execute Mission (Job)

Establish Local Logical Access

NETWORK

USD Personnel & Readiness (P&R)
USD Intelligence (I)
Local commander/resource owner
Veterans Affairs (VA)

Terminology purposely abstracted up to very generic language & Concepts
IPvMWG will mature this "Cartoon" to a Model

UNCLASSIFIED

27

Notional Friendly Force IPvM Biometric Enterprise Equities

- **Hiring**
  - Identity Proofing & Vetting
  - Credential Issuance (Digital Profile)

- **Biometrics-enabled Physical & Logical Access Control**
  - Identity Proofing & Vetting

- **Biometrics-enabled "Watch List"**
  - Hiring - Identity Proofing & Vetting
  - Identity Fixing
  - Identity Tracking
  - Authoritative Repository(s)

- **Personnel Recovery**

- Second Order Effects, i.e., if we can support all of the above, then we can
  - Humanitarian Assistance / Disaster Response
  - Personnel Accountability

2011 DoD
BIOMETRICS
COLLABORA
TIONFORUM

Digital Profile
(HRM)

Biometrics

"Watch List"
(Identity Proofing &
Vetting)

Digital Identity
(E-Authentication)

UNCLASSIFIED

IPvMWG Contact Information

Co-Chairs, IPvMWG

Tim Fong
Deputy Director,
Identity Assurance & PKI Directorate
OASD (NII) / DASD, CI&IA

timothy.fong@osd.mil

703-604-3156

Arthur R. Friedman
Senior Strategist for Privilege
Management

OASD (NII) / DASD, CI&IA

arfried@nsa.gov

240-373-1968

IPvMWG support:

    Cynthia Odom (cynthia.odom.ctr@osd.mil) 703-604-3155
    Peter Joukov (peter.joukov.ctr@osd.mil) 703-604-3154
    Bruce Groskreutz (bagrosk@nsa.gov) 240-373-4303

IPvMWG Websites:

    https://www.us.army.mil/suite/grouppage/103390
    https://www.intelink.gov/sites/dodipmwg/default.aspx
    Email peter.joukov.ctr@osd.mil to request access