

Interagency Advisory Board

Meeting Agenda, March 23, 2011

1. **Open Remarks** (*Mr. Tim Baldridge, IAB Chair*)
2. **Impact of M-11-11 on PACS** (*Ron Martin, HHS*)
3. **FIPS 201-2 Update** (*Bill MacGregor, NIST*)
4. **Status Brief on ICAM Roadmap** (*Shelly Hartsook, Deloitte*)
5. **Status of FPKI Management Authority** (*MA Team, GSA*)
6. **Closing Remarks** (*Mr. Tony Cieri*)

Office of Management and Budget (OMB)

OMB Memorandum 11-11 2/3/2011
Continuation of HSPD-12 Implementation

A Physical Access Control (PACS) Perspective

PACS Reality Check

“...The Physical Access Control System is a significant security component of any enterprise. These systems are an inherent and essential part of the overall security protection environment and must be interfaced to the enterprise Identification Management System (IDMS) and a Card Management System (CMS) to provide full HSPD-12 interoperability and FIPS 201-1 compliance. ..”

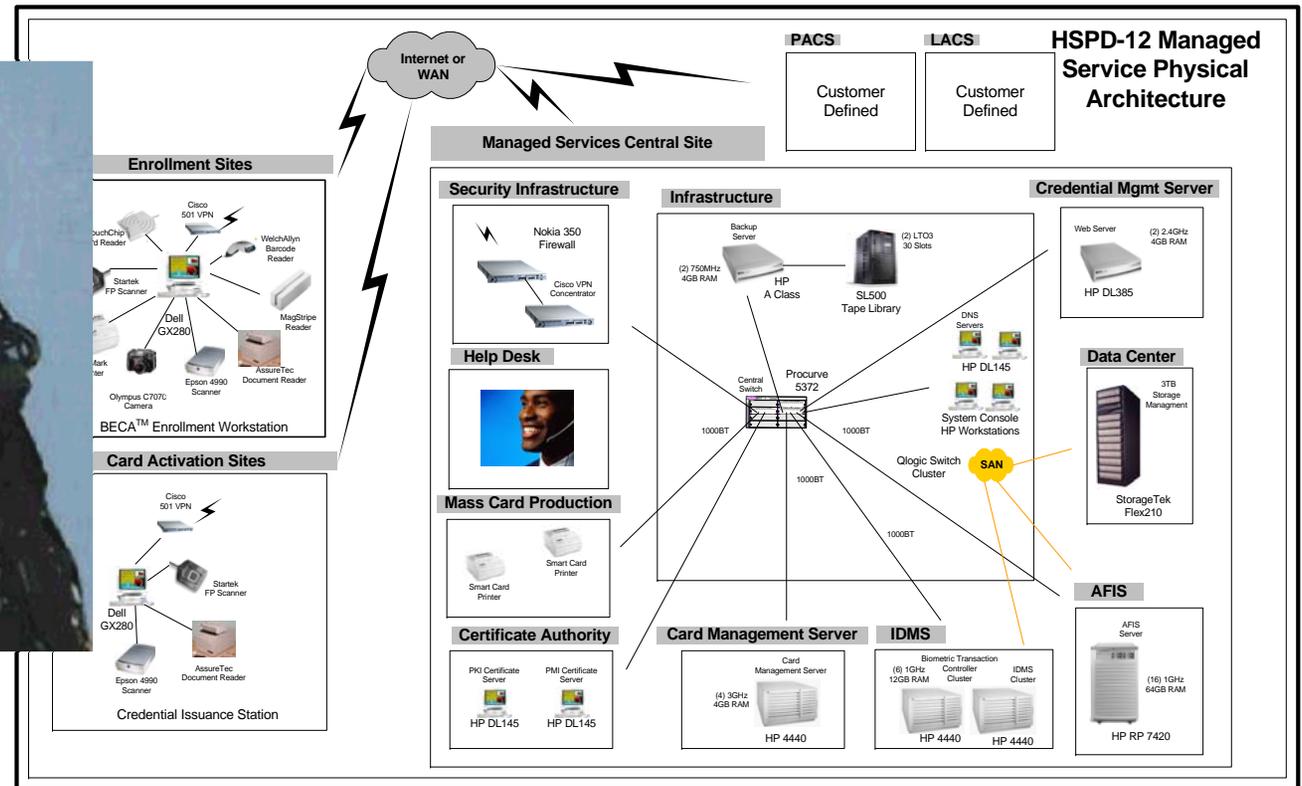
Ron Martin, CPP April 2007

The PACS is an Application that resides on the organization's enterprise. It therefore must adhere to all of the Logical Access Control protocols.

**MARCH
2006**

HSPD – 12

Resistance is Futile!



**LOGICAL & PHYSICAL ACCESS WILL BE
ASSIMILATED INTO THE SMART CARD!**



M-11-11:

Normatively referenced SP 800-116 and The FICAM Roadmap

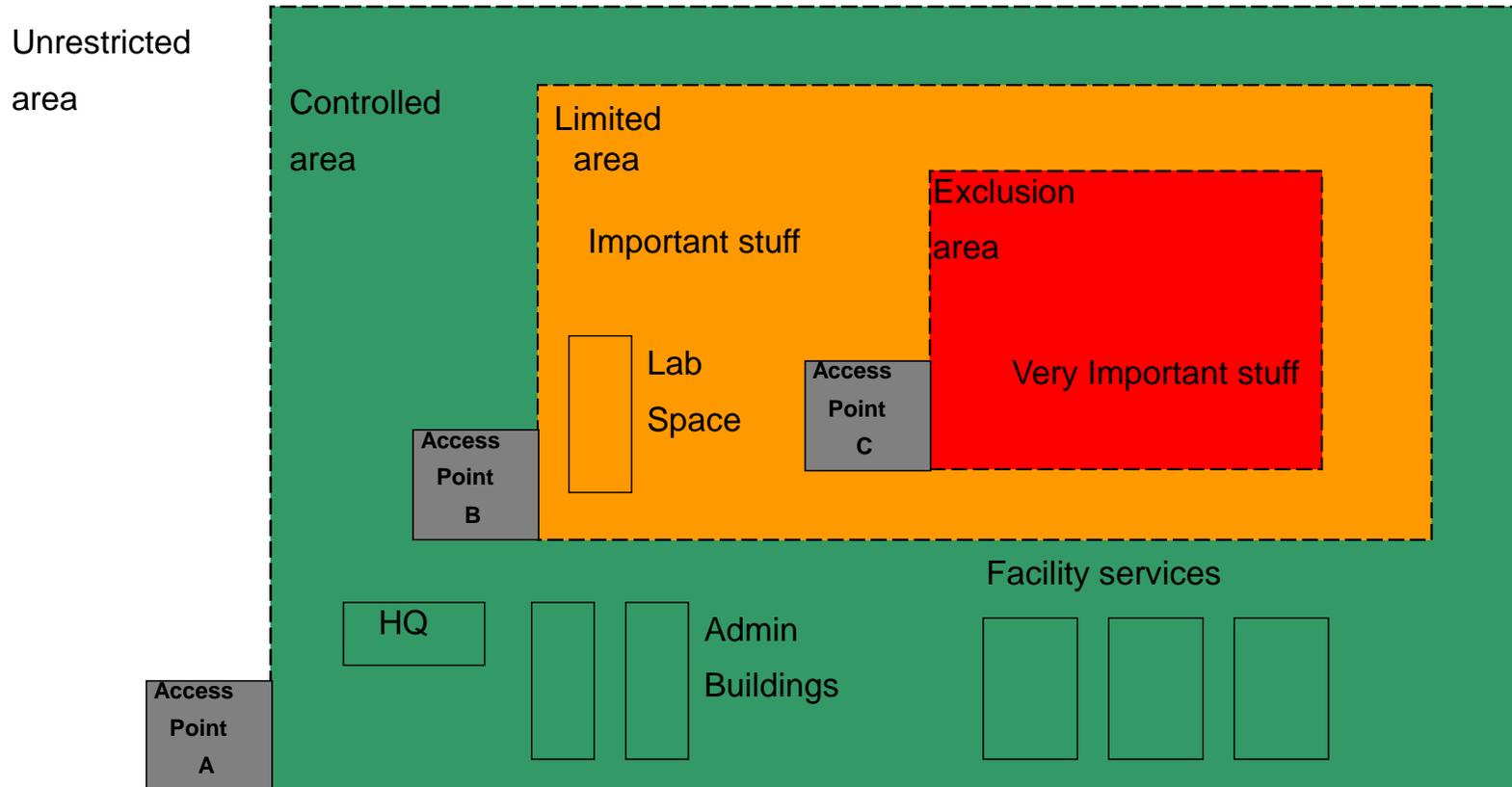
FIPS 201:

FIPS 201-2 "the Standard" is about to be revised

FICAM PART "B" Phase 2 and FIPS 201-2 will be finished CY-2011

A PACS Model from SP 800-116

Unrestricted, Controlled, Limited, Exclusion

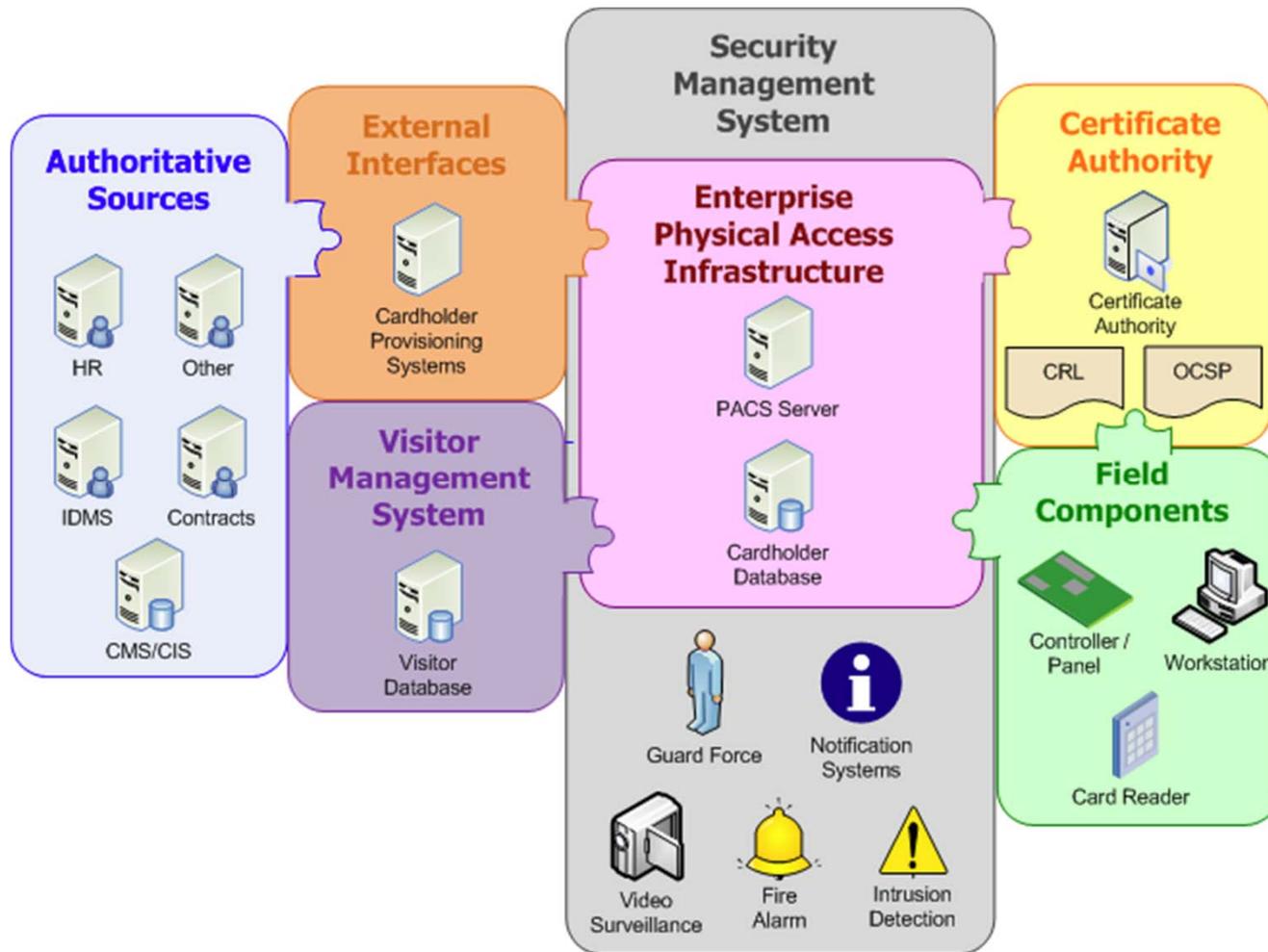


PIV Implementation Maturity Model (PIMM)

- **Maturity Level 1—Ad Hoc PIV Verification**: A site has the ability to authenticate PIV Cards by performing required authentication mechanisms on an ad hoc, on-demand basis. For example, card and cardholder authentication is achieved with a handheld terminal or a specific PC, for special or occasional uses.
- **Maturity Level 2—Systematic PIV Verification to Controlled Area**: At the outer perimeter of the site (Controlled area), PIV Cards are accepted as proof of identity, possibly in addition to legacy PACS credentials. A visitor registration procedure exists to accept PIV Cards and if necessary convert PIV authentication to a temporary legacy PACS credential.
- **Maturity Level 3—Access to Exclusion Areas by PIV** : Access to Exclusion areas (the most sensitive areas) is permitted by PIV authentication or "exception" only. Here, exceptions are the exceptions to PIV issuance (e.g., less than six months association). However, all access to exclusion areas is also subject to authorization, and authorization would typically only be granted to PIV cardholders. The exception case might be applied to exclusion areas for VIP visitors, for example. At Level 3, legacy PACS or badges are not acceptable for authentication to exclusion areas.
- **Maturity Level 4—Access to Limited Areas by PIV**: Access to Limited areas (generally, those permitting clearance level- or role-based authorization) is permitted by PIV authentication or exception only. At level 4, legacy PACS or badges are not acceptable for authentication to Limited areas.
- **Maturity Level 5—Access to Controlled Areas by PIV**: Access to Controlled areas (showing evidence of organizational affiliation, or registration for a visitor, with or without escort) is permitted by PIV authentication or exception only. At level 5, legacy PACS or badges are not acceptable for authentication to controlled areas.

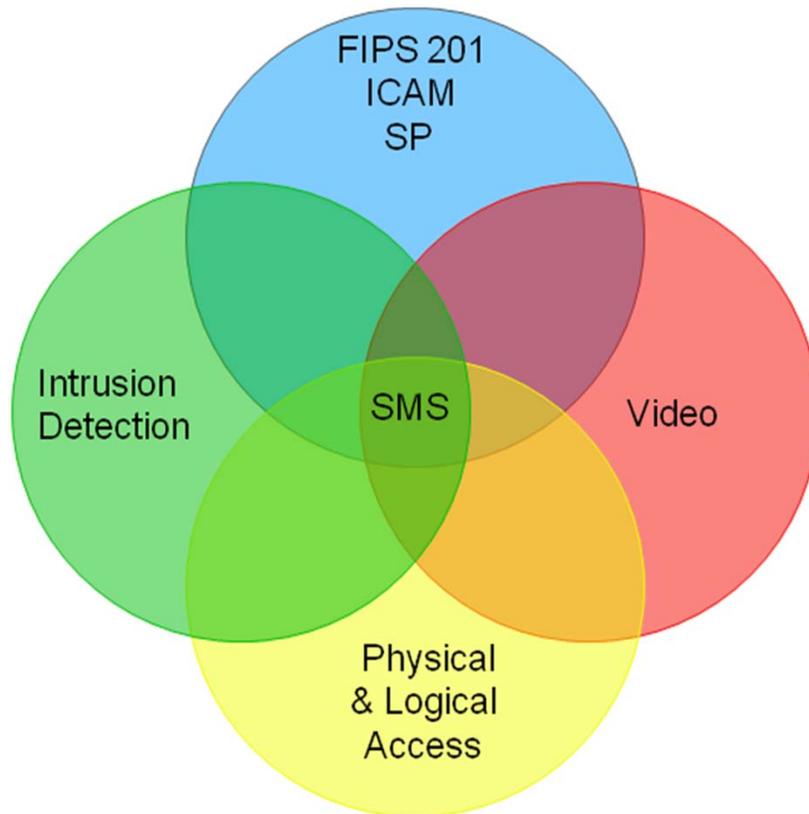
NOTE: *Maturity levels are progressive*: for example, Maturity Level 1 must be achieved before Maturity Level 2 can be achieved. Maturity levels can be applied to individual facilities, or by extension to multiple facilities within an organization. When applied to multiple facilities, a maturity level is achieved when each of the facilities in the group has achieved the maturity level individually.

FICAM Chapter 10 Solution Architecture



FICAM Recognition

The enterprise PACS is depicted as a piece of the larger **Security Management System (SMS)**, which has interconnections with other physical security elements.



- Fire Alarm Systems
- Video Surveillance
(Closed Circuit Television)
- Short-term visitor MGT
- Intercoms and
Emergency Management
Notification
- Security Officer touring
- Intrusion and explosive
detection systems



Budget and Conformance

M-11-11 FIVE Tenets

1. Effective immediately, all new systems under development must be enabled to use PIV credentials
2. Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials
3. Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation.
4. Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.
5. The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "FICAM"



A Physical Access Control System is Information Technology

BUDGET

OMB Memorandum May 23, 2008 titled Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation :

“... agencies should continue to follow the requirements of Office of Management and Budget (OMB) policy, such as A-130, “Management of Federal Information Resources” and A-11, “Preparation, Submission and Execution of the Budget,” when developing plans...”

Tenet 1 and 2

- Effective immediately, all new systems under development must be enabled to use PIV credentials
- Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials

PIV enablement is more than door card readers.

PIV cards are to be used to access PACS

CONFORMANCE

Part 1

Tenet 3:

Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation.

OMB M-06-18: Two Federal Acquisition Regulation requirements

Subpart 4.13--Personal Identity Verification

4.1301 Contractual implementation of personal identity verification requirement.

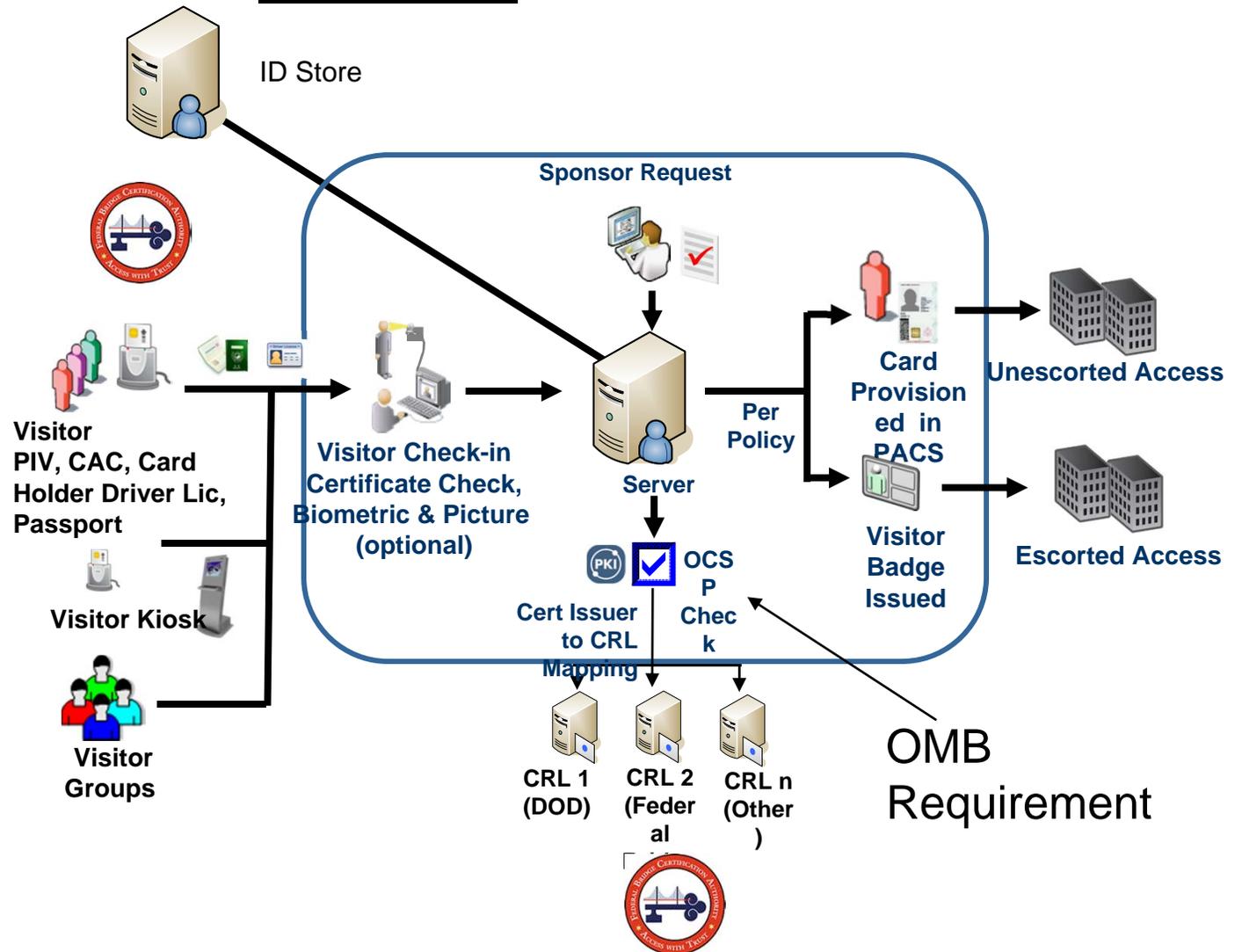
4.1302 Acquisition of approved products and services for personal identity verification.

Subpart 52.204-9 -- Personal Identity Verification of Contractor Personnel.

CONFORMANCE

Part 2

4. Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.



CONFORMANCE

FICAM

Tenet 5:

The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "FICAM"

FICAM Implementation Roadmap – November 2009

FICAM Implementation Roadmap – PART "B" Phase 1 – February 2011

FICAM Implementation Roadmap – PART "B" Phase 2 – TBD CY 2011

FICAM Implementation Roadmap – PART "B" Phase 2 – TBD CY 2011

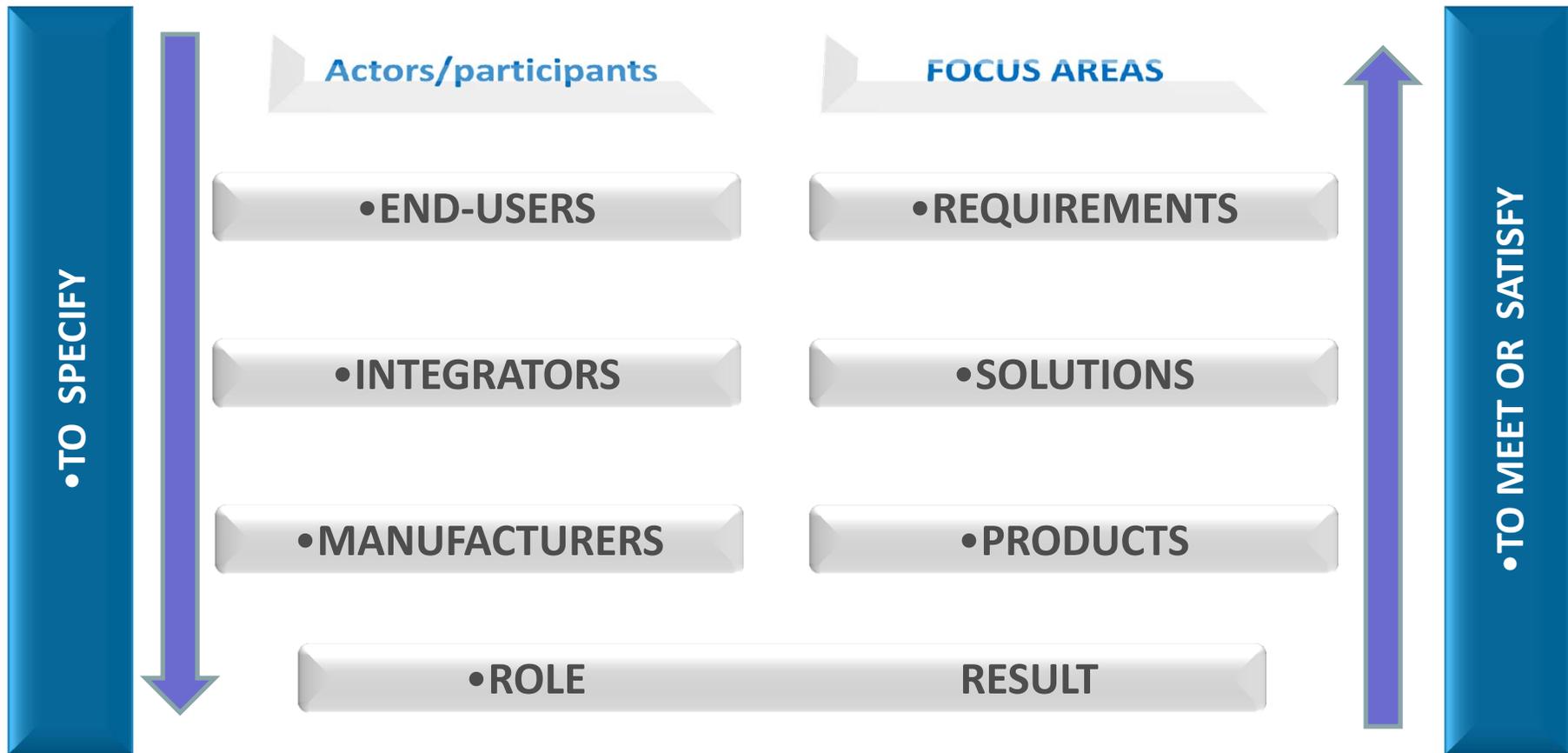
Part "B" Phase two will have these chapters:

Chapter 7. Initiative 5: Streamline Collection and Sharing of Digital Identity Data.

Chapter 8. Initiative 6: Fully Leverage PIV and PIV-interoperable Credentials.

Chapter 12. Initiative 9: Implement Federated Identity Capability.

M-11-11 Framework for Implementation



The implementation of M-11-11 is applicable to end-users, integrators/solution providers and manufacturers/developers



iAM@
HHS