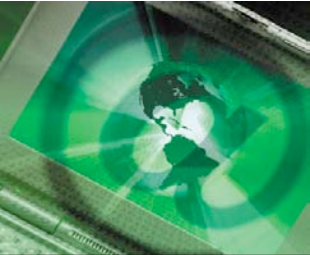


**U.S. Department of Agriculture  
HSPD 12 Program**

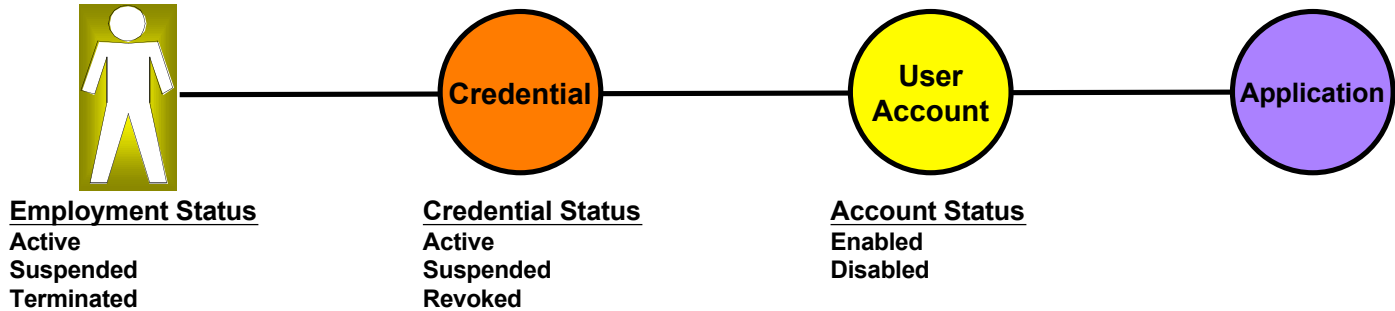
**HSPD-12 Implementation  
Credential Usage @ USDA**

January 16, 2007



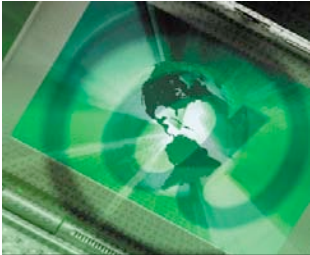
# Let's Start by Discussing Identity Management

**Definition:** **Identity** is the collection of attributes and characteristics that define the oneness of a single discrete individual.



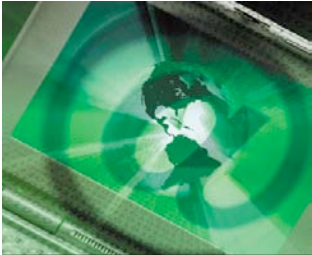
The interface between a user account and the user is the credential or token, which is simply a representation of the user. This representation is linked to the user by what the user knows, has, or is:

- What the User Knows – Password or Shared Secret
- What the User Has – PKI Certificate
- What the User Is – Biometrics



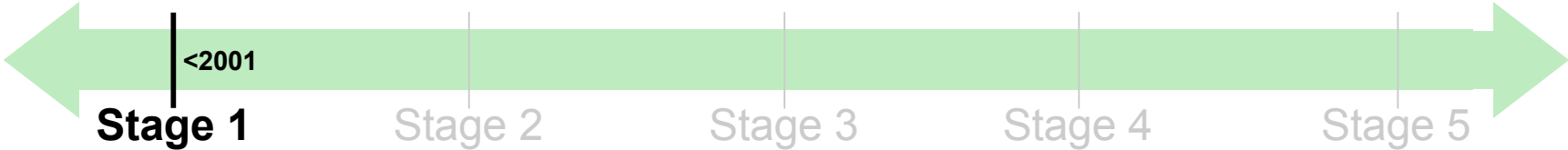
## USDA's HSPD-12 Deployment Plan (Our Catalyst for Credential Management)

Background Investigations	Complete by 10/2008
• <i>Contractors</i>	<i>10/2007</i>
• <i>Employees &lt; 15 years</i>	<i>10/2007</i>
• <i>Employees ≥ 15 years</i>	<i>10/2008</i>
Smart Cards to applicable persons	Complete by 10/2008
• <i>30% of 150,000 persons</i>	<i>10/2007</i>
• <i>70% of 150,000 persons</i>	<i>10/2008</i>
LACS integrations	Complete by 10/2009
PACS integrations	Complete by 10/2011

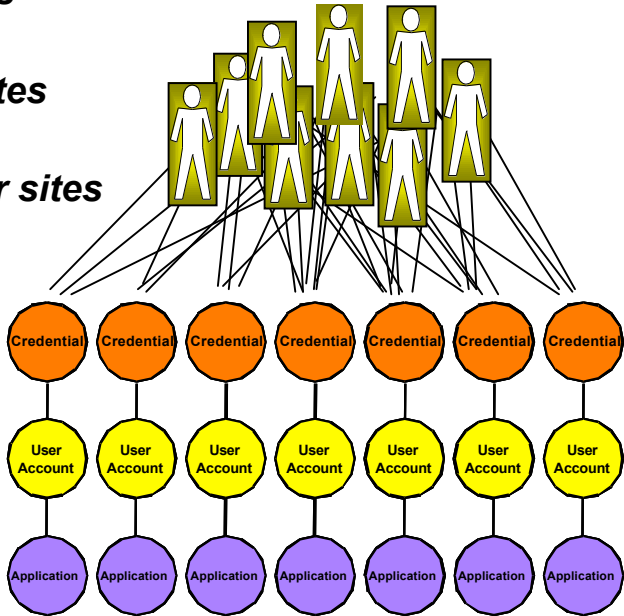


# EVOLUTION

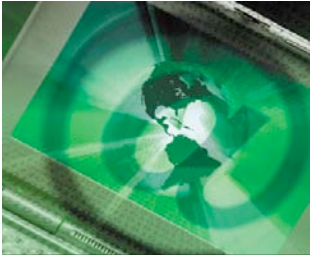
## Stage 1 - Parallel Environments



- 1. *97,000 employees; 50,000 contractors; 1 million other affiliates*
- 2. *25,000 facilities, with offices in every county in the United States*
- 3. *A handful of Physical Access Control Systems (PACS) – other sites mostly traditional key-based*
- 4. **Chaos with Logical Access Control Systems (LACS)**
  - a) Multiple closed networks; stand-alone desktops
  - b) Several hundred web-based/client server systems; some users with > 30 L/P's
  - c) 2 mainframe systems
  - d) >10,000 persons doing some type of credential & account administration

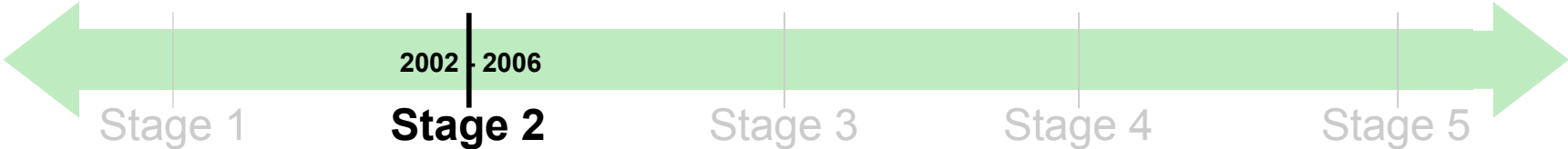


Stage 1 - Parallel Environments

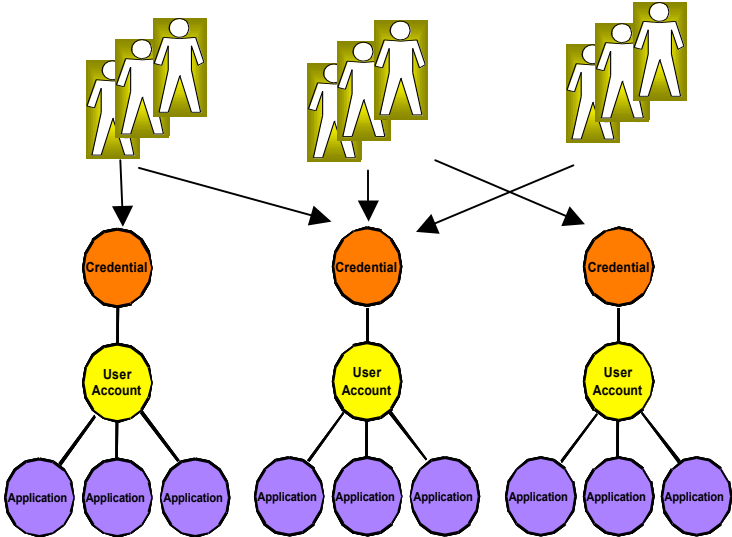


# EVOLUTION

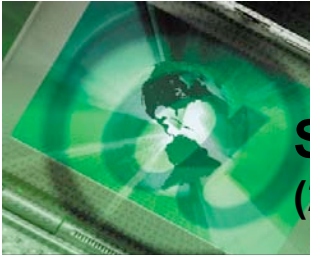
## Stage 2 – Use of Security Domains & eAuthentication



- 1. **Same user base**
- 2. **Same # & location of facilities**
- 3. **Physical Access Control Systems (PACS) at 250 sites; other sites mostly traditional key-based**
  - a) 50 different legacy PACS systems – each stovepiped
- 4. **Logical Access Control Systems (LACS)**
  - a) 36 Active Directory forests and few trusts
  - b) Limited single sign-on for non-domain based resources (e.g. eAuthentication)
  - c) Legacy client-server and mainframe
  - d) Still had several thousand credential & account administrators



Stage 2 – Use of Security Domains



# Selected Statistics for USDA's eAuthentication (221 Integrated Business Applications)

Uptime Percentage		
Goal	Last Month	Current Month
99.50%	100.00%	100.00%

Number of Customers		
Level	Last Month	Current Month
1	64,563	66,396
2	60,434	61,965
3		
4		
<b>Totals</b>	<b>124,997</b>	<b>128,361</b>

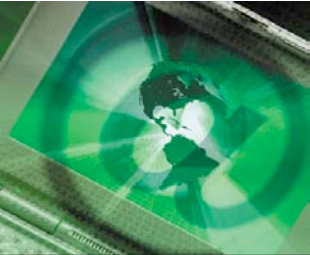
Number of Authentications		
12 Months Ago	Last Month	Current Month
1,190,010	1,409,039	1,488,526

Number of Authorizations		
12 Months Ago	Last Month	Current Month
16,895,892	48,593,430	55,640,695

Number of LRAs		
Agency	Last Month	Current Month
FSA	9,249	9,230
NRCS	2,947	2,949
RD	1,052	1211
FNS	97	98
OCIO	-	-
APHIS	155	170
Other	117	118
<b>Totals</b>	<b>13,617</b>	<b>13,776</b>

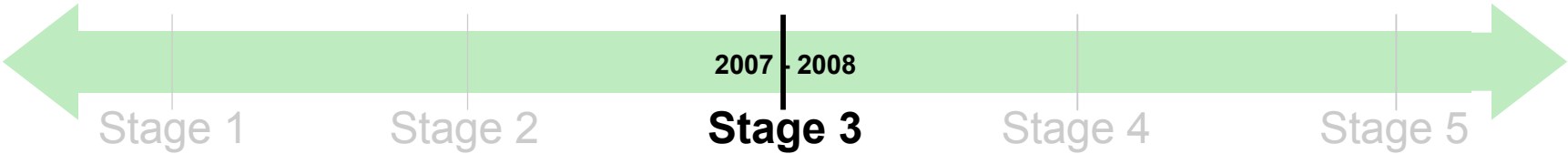
Number of Employee Credentials		
Level	Last Month	Current Month
2	96,875	96,326
3		
4		
<b>Totals</b>	<b>96,875</b>	<b>96,326</b>





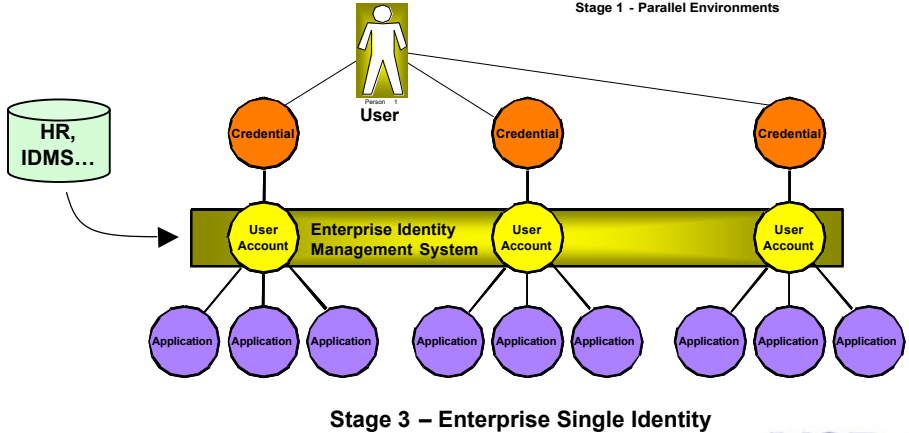
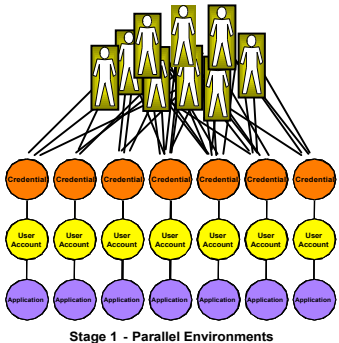
# EVOLUTION

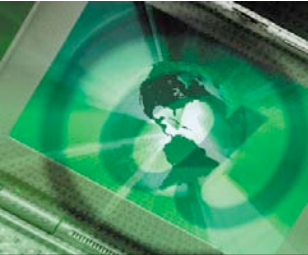
## Stage 3 – Enterprise Single Identity



**Like most other Departments, we’re moving to identity management:**

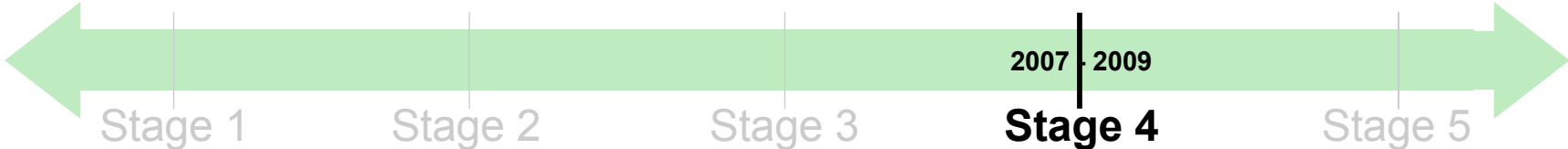
- 1. *We achieve more precise identity management:*
  - a) Improved confidence of identity
  - b) Improved background/suitability
  - c) Improved status of employment
  - d) Absolute agreement on authoritative data source
  
- 2. *We achieve more automatic account provisioning and de-provisioning among connected systems.*
  
- 3. *We still have:*
  - a) Multiple credentials
  - b) Mixture of Au techniques
  - c) More user “pains”
  - d) Same old credential administration
  
- 4. *But, we do have*
  - a) Reduced account administration





# EVOLUTION

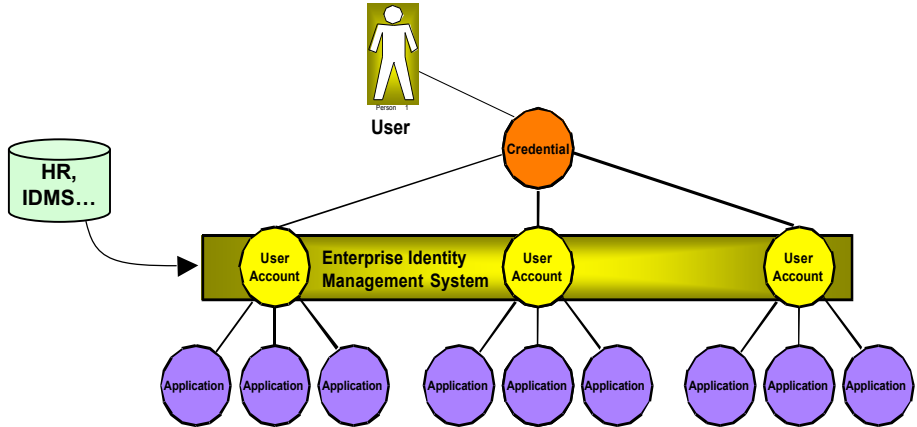
## Stage 4 – Enterprise Single Credential



**For identity management & credential management, HSPD-12 delivers a great 1-2 punch!**

**Single identity & single credential solves so many problems!**

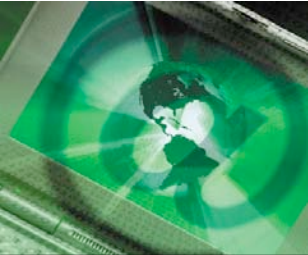
- Confidence of identity
- Standardized background investigation
- Accurate & timely employment status
- 1 credential per individual
- No more crazy password mgmt (55% of HD)
- Reduced credential & account administration
- Accurate provisioning/de-provisioning
- 2 Factor; Dig Sig; other security improvements



Stage 4 – Enterprise Single Credential

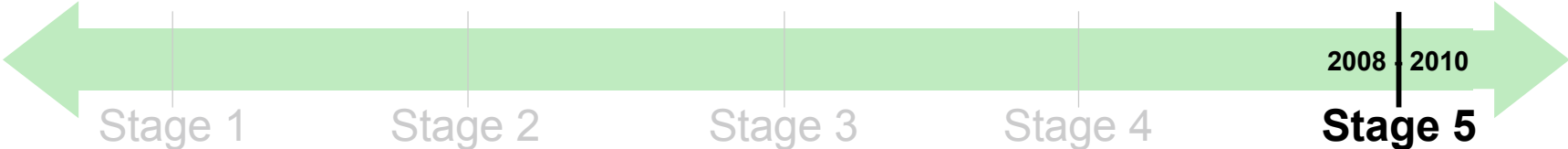
**How many credential & account administrators will we need?**



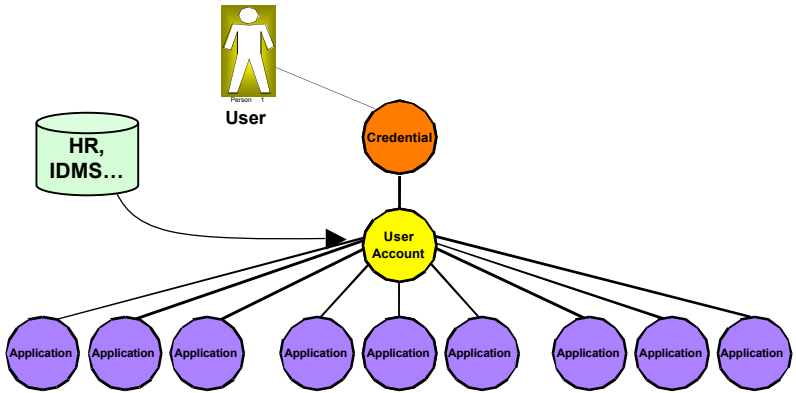


# EVOLUTION

## Stage 5 – Enterprise Single-On

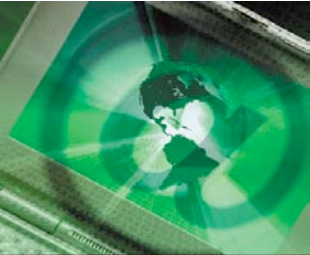


- **Single Sign-On provides an even richer, more efficient user experience.**
- **Security boundaries don't change, but the authentication occurs without user intervention or awareness.**

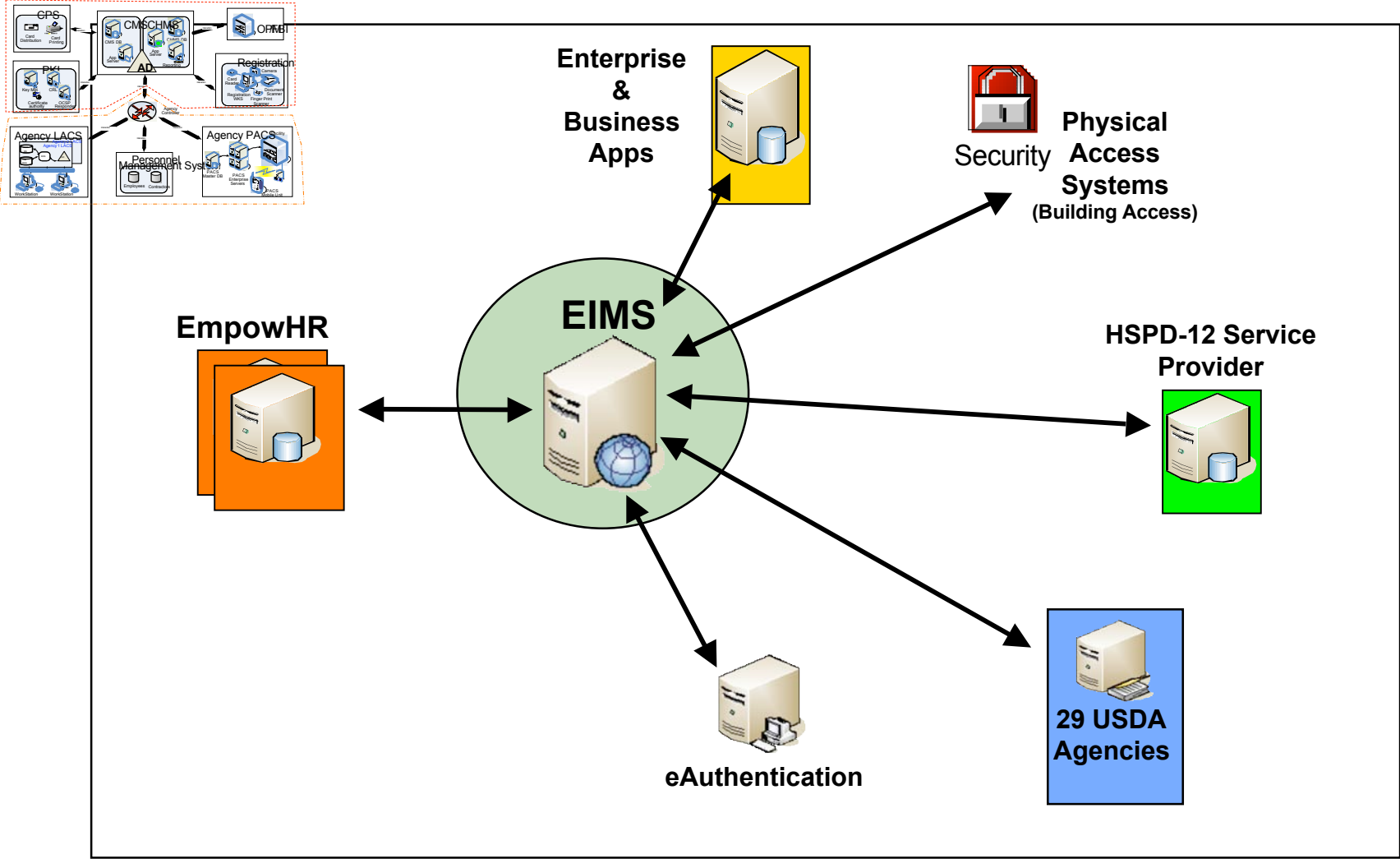


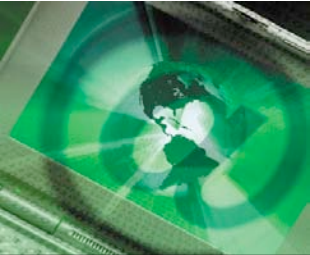
Stage 5 – Enterprise Single -On (User Perspective)



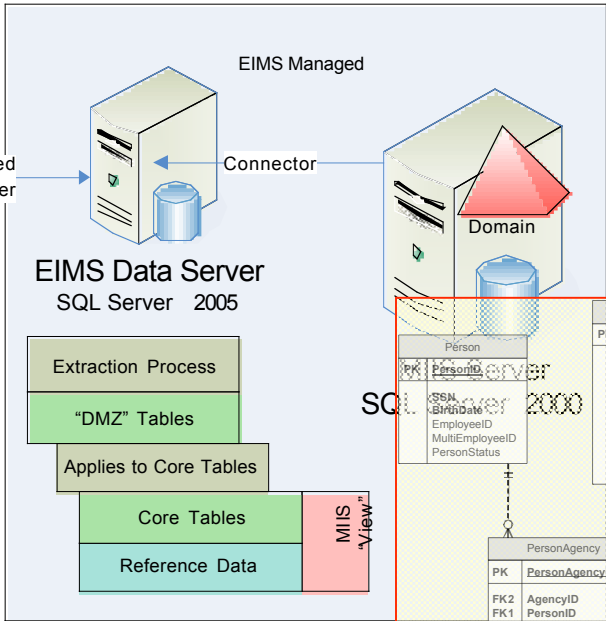
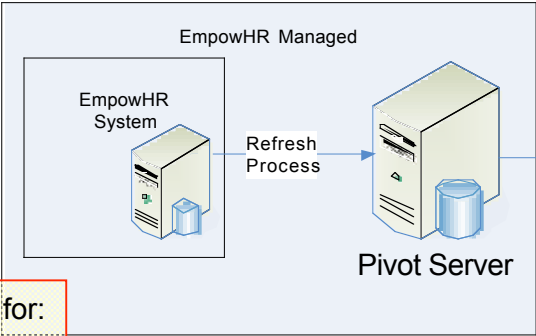
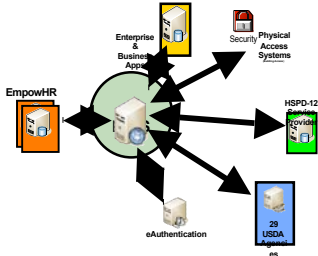


# Drilling Down into USDA's Responsible Area



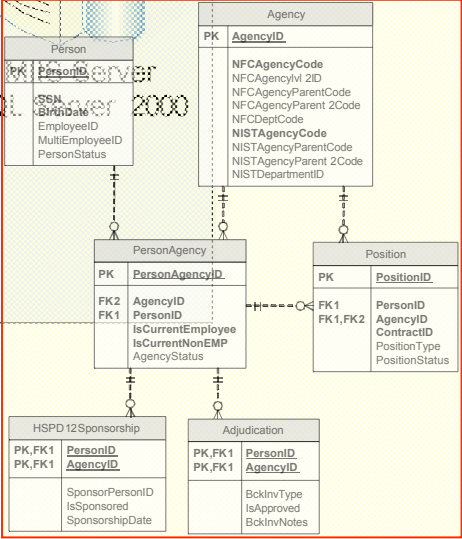


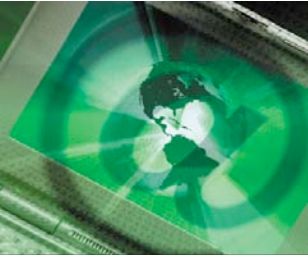
# HR System & Identity Management



- Authoritative Source for:**
- employees
  - contractors
  - affiliates
- Including:**
- employment status
  - position(s)
  - agencies
  - sponsorship
  - adjudication Results

- Design Issues Considered:**
- Data Mapping & Transformation
  - Data Protection & Security
  - Scheduling (30 min. refreshes)
  - Logging/Rollback/Data Integrity





# HR - Employees

## Employee Record – Personal Data

USDA Jaguar, Mark US Dept of Agriculture

Menu: PAR Processing, Action Table Setup, Flexiplace Work Agreement, Hire Employee, Update Reports To, Mass Reports to Update, Address Processing, Applicant Hire, HR Processing, Update Applied Action, Correct Applied Action, Cancel Applied Action, History Override, Update NFC Flags, Create New Opnd, Employee Password Reset, Mass Actions, Departmental Transfer, Employee Security Clearance, Position Management, HR Reports, Recruiting, HR Processing, Training Administration, Worklist Admin, LOC Transit Subsidy

Personal Data: SMITH JR, JON DAVID EmplID: 110227 Empl Rcd#: 0 SSN: 678-98-1575

Effective Date: Transaction# /Seq PAR Status: Processed Empl Status: Active

NOA Code: Act Type: Empl Status: Active

Name: First: JON Middle: DAVID Last: SMITH Suffix: JR Name: SMITH JR, JON DAVID Alias Name: DOE Pref First Name: Jonny Gender: Male Handicap Cd: No Handicap Date of Birth: 10/12/1965 Draft Status: Not Applicable

## Employee Record - Security

USDA Orlebar, Roxanne E US Dept of Agriculture

Security Info: EmplID: 090166 Empl Rcd#: 0 Brown, J, Jocelyn GAIL

Effective Date: 06/09/2006 Transaction # / Sequence: 11 Transaction Status: NFC R

Action: NAM Name Chg from Reason Code: NAM Name Change NOA Code: 780 Name Chg from

PAR Status: PRO Proce

Security Clearance: Not Required Sensitivity Code: Computer Sensitivity:

Financial Disclosure Required Due Date: 01/01/1900

## Position Record – Specific Information

USDA Orlebar, Roxanne E US Dept of Agriculture

Investigation: Existing BI Notes: Testing PIV Card Required Card Activation Information

Submitting Office Number: 1234 SOI: 1234 OPAC/ALC Number: e-QIP tracking number: 2353456568 HSPDUSER

Investigation: NACI by HR, Requirements Met, Initiated by PSO, Not Required

Position Record: Position Number: 90009160 State Dr Headcount Status: Open Current Head Count: 0 out of 2

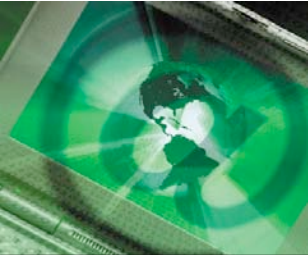
Effective Date: 8/26/2005 Station: Active NFC Proc Num: 90009160

Job Profile ID: Max Head Count: 2

Work Phone: Health Certification: Signature Authority: Position Pool ID: \*Pre-Encumbrance Indicator: Encumbrance Salary Option: Encumbrance Salary Amount: Classified Indicator: FTE: Add to FTE Actual Count

US Federal: Computer Sensitivity: Security Clearance: LEO Indicator: Language Required: Training Program: Staff Line Position: Seasonal, Drug Test (Applicable), Intelligence Position, Mobility Position, Procurement Sling Post, Presidential Appoint Post, Emergency Response Official





# HR – Non-Employees

## Contract/Affiliation Record

Contract Information

Contract ID: BRO1234

Agency: 13

Company: BRO Broncos

\*Contract Expiration Date: 04/20/2009

Notes:

EmpID	Name	Date	Screened By
1		01/12/2009	Col.Peter

## Non Employee Record – Personal Data

Non Employee Info

Name: COSTELLO, JRELVIS ANRCLO EmpID: 12558 Empi RNUM: 0

Effective Date: 04/02/2009

Social Security Number: 987-65-43210

First: JRELVIS Middle: ANRCLO

Last: COSTELLO Suffix: JR

Work Name: Sub-4

Alias Name: ST4090

Date of Birth: 04/24/1970

Gender: Male

Business Email: jrelvscostello@usda.gov

Current Station: LOS (Contract Administration)

SSN: JRELVIS, not of Hispanic origin

Effective Date of Status: 04/24/1955

Non-Employee Status: [ ]

Non-Employee Type: [ ]

Work Address: 970223-1111

## Contract – Non Employee Link

Contract Assignment

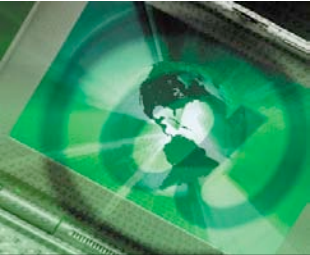
Contract ID: BRO1234

Company: BRO Broncos

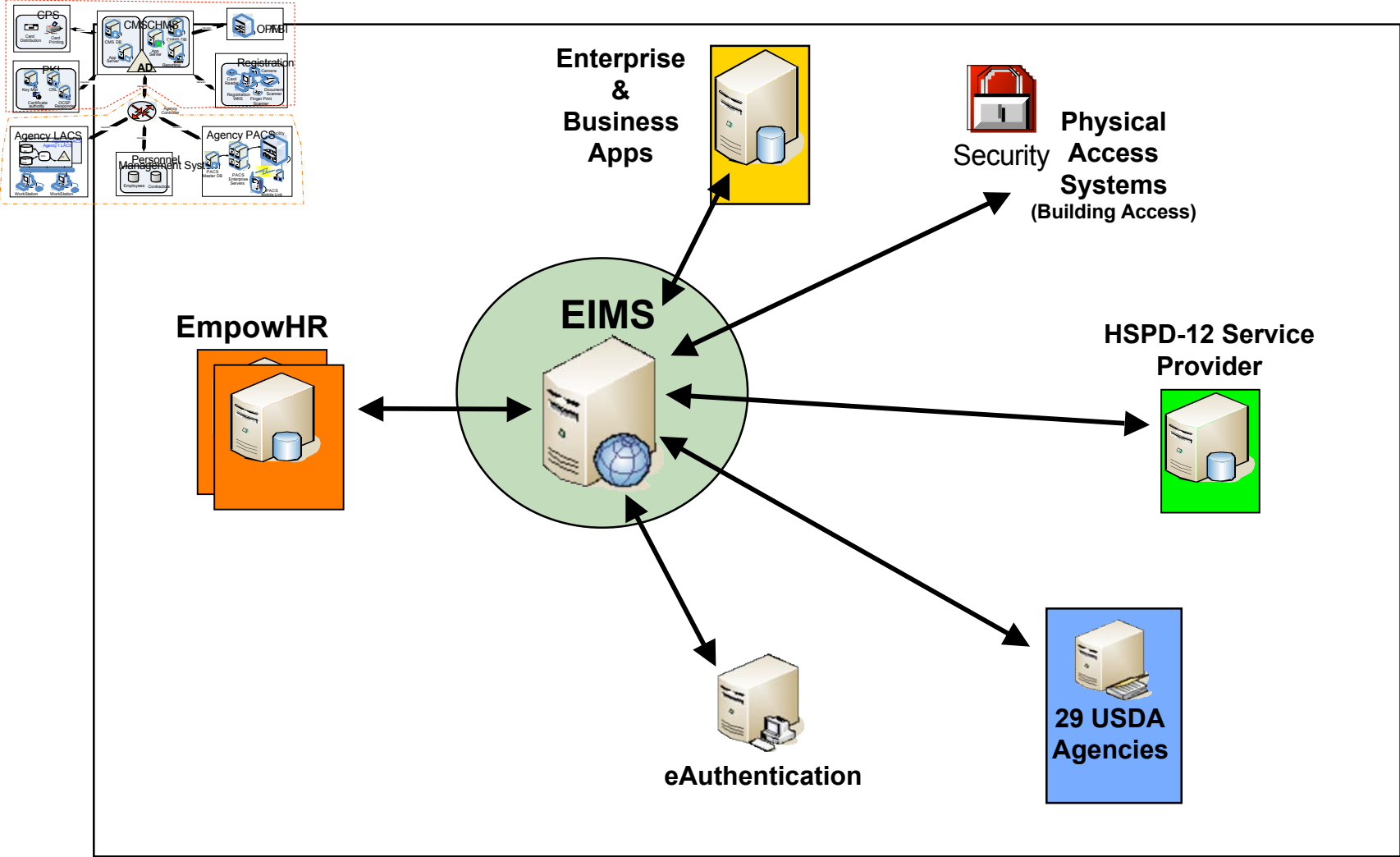
Select  
De Select All

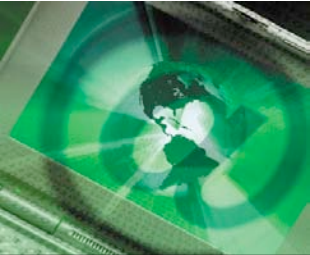
EmpID	Name	Assignment Date	Contractor Status	PIV Card Required	Card Activation Information
1200001	ANDERSON, MICHAEL J	12/09/2005	Active	<input checked="" type="checkbox"/>	Card Activation Information





# Let's Look at PACS

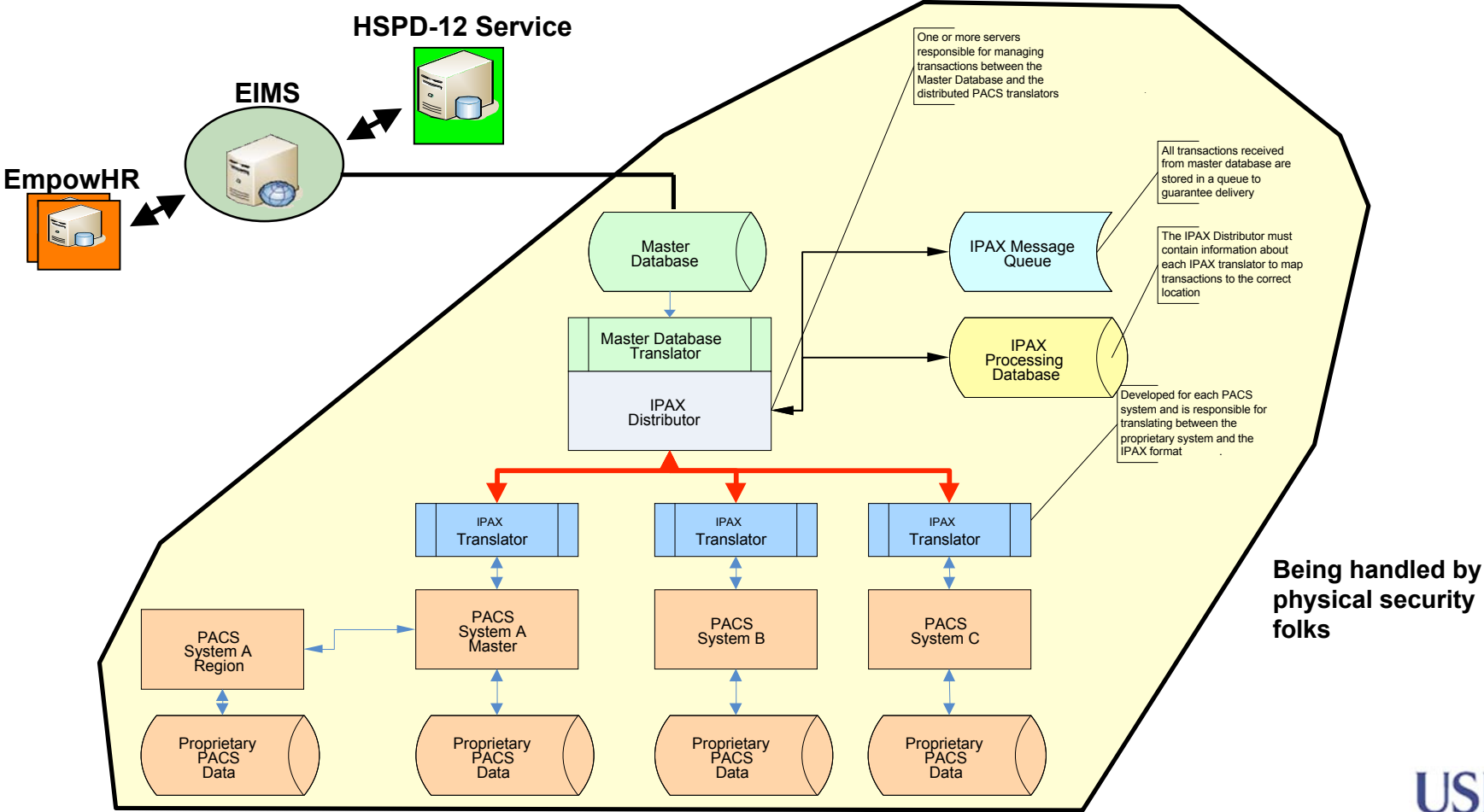


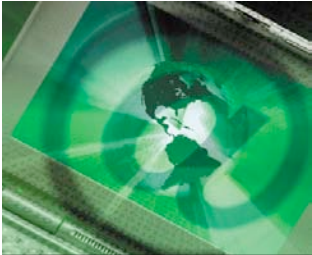


# Enterprise PACS Architectural Concept

## Intra-Physical Access Control XML

- Using XML, each PACS translator is responsible for converting the proprietary data to/from a common XML format, move/store data securely & perform auditing/alerting functions



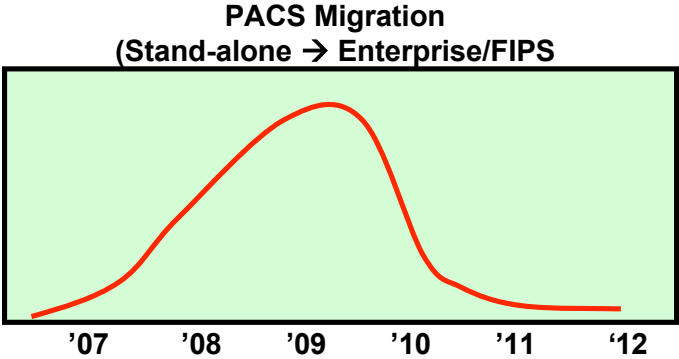


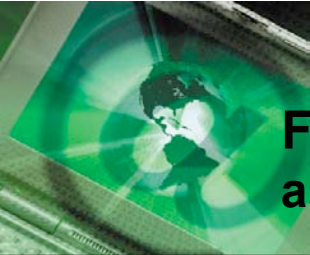
# PACS Migration Strategy

## Measured Migration Plan

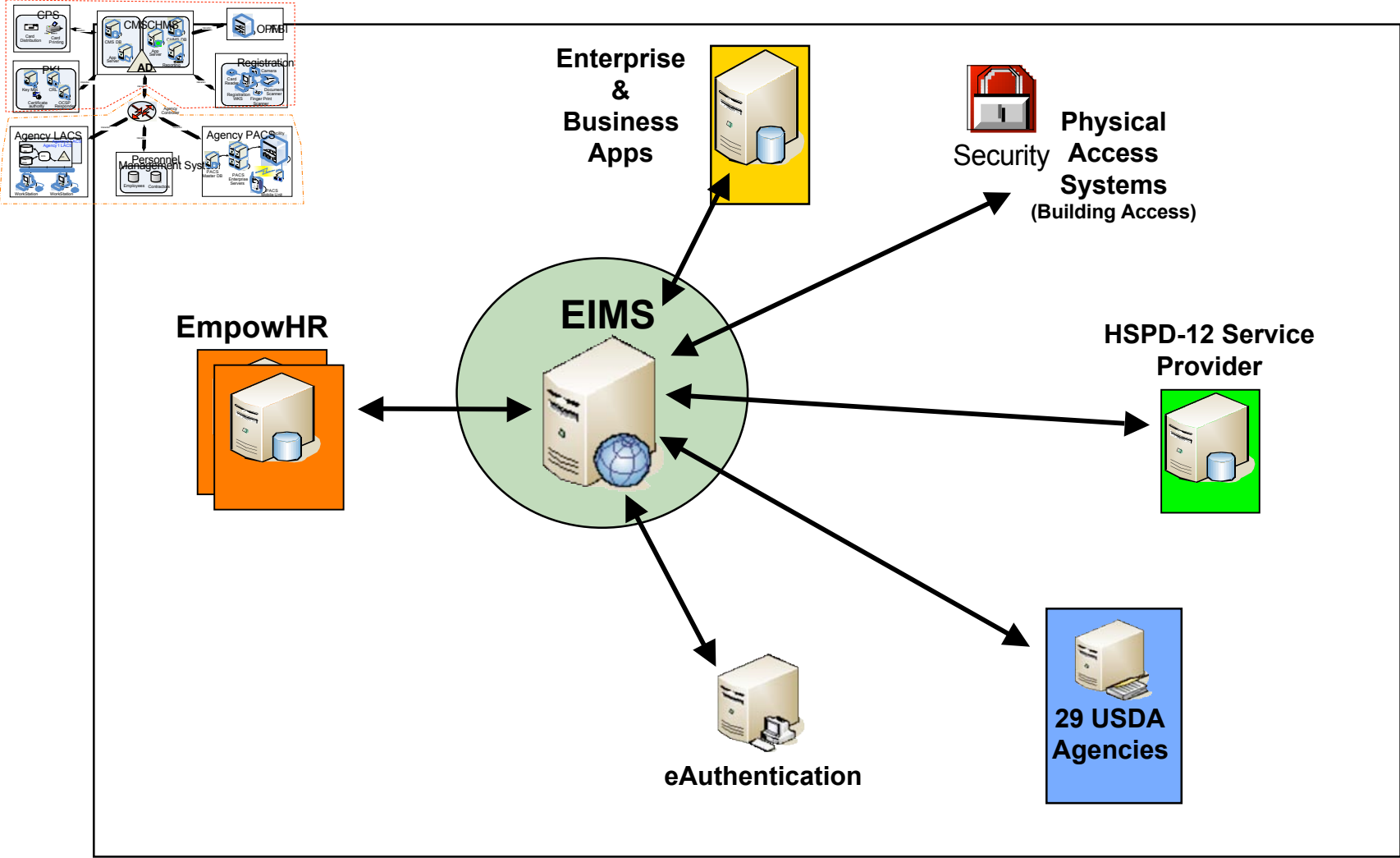
- 33% of smart cards will be a triple technology card to allow for maximum leverage of existing legacy PACS systems <\$4 increased cost/card>
  
- Installation of dual technology card readers allowing legacy cards to work during migration period < \$250 cost/reader>
  
- USDA will allow legacy PACS to reach their lifecycle before being replaced to leverage previous investments (All legacy PACS will be compliant by October 2011)

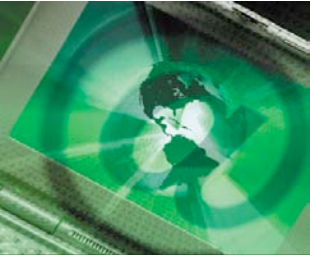
Need to further cooperate w/ other migration strategies!



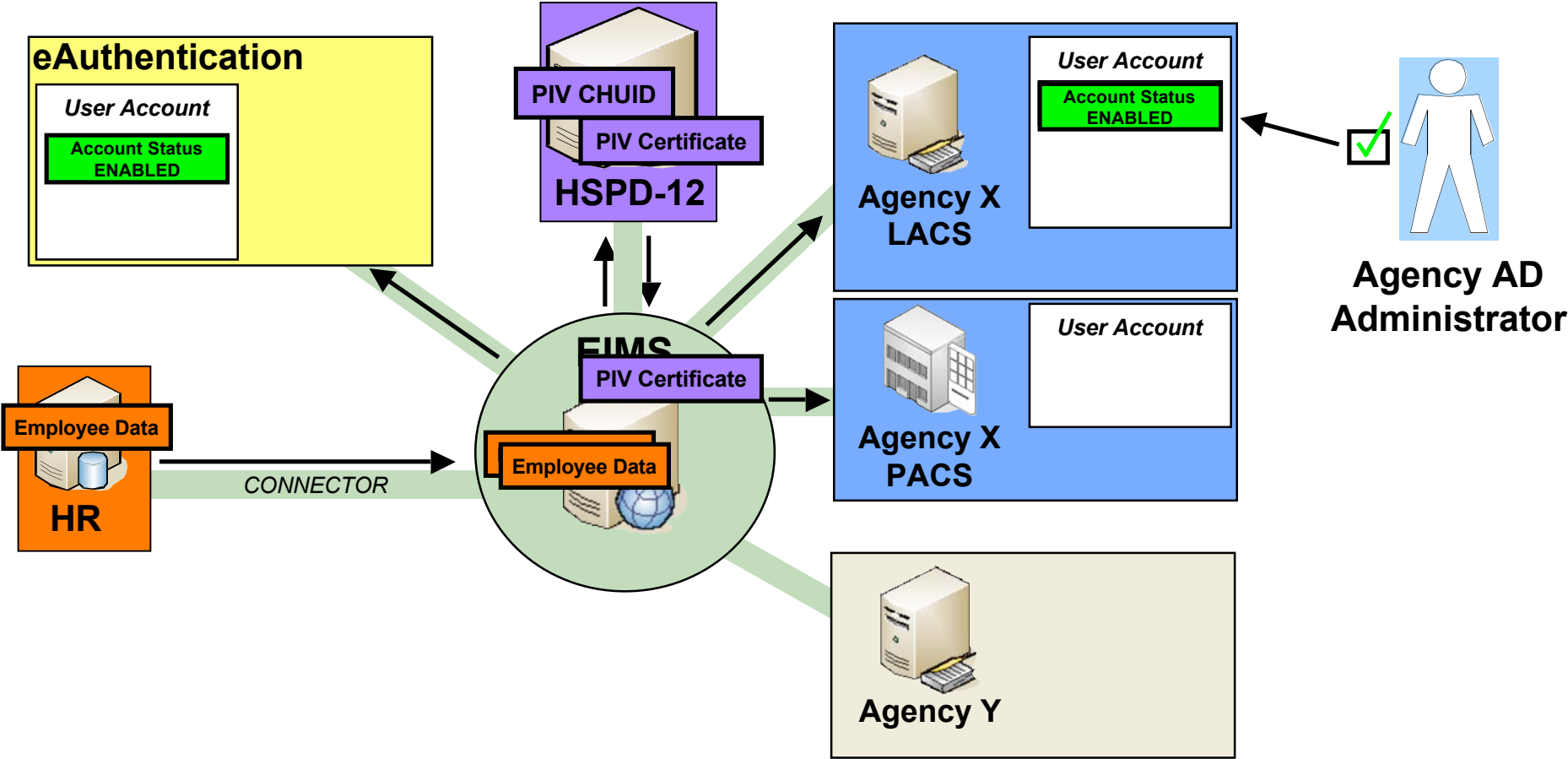


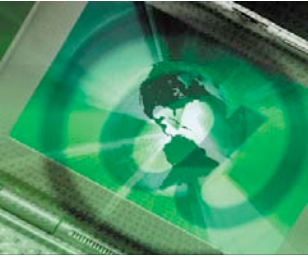
# Finally, Let's Look at LACS... and everything else



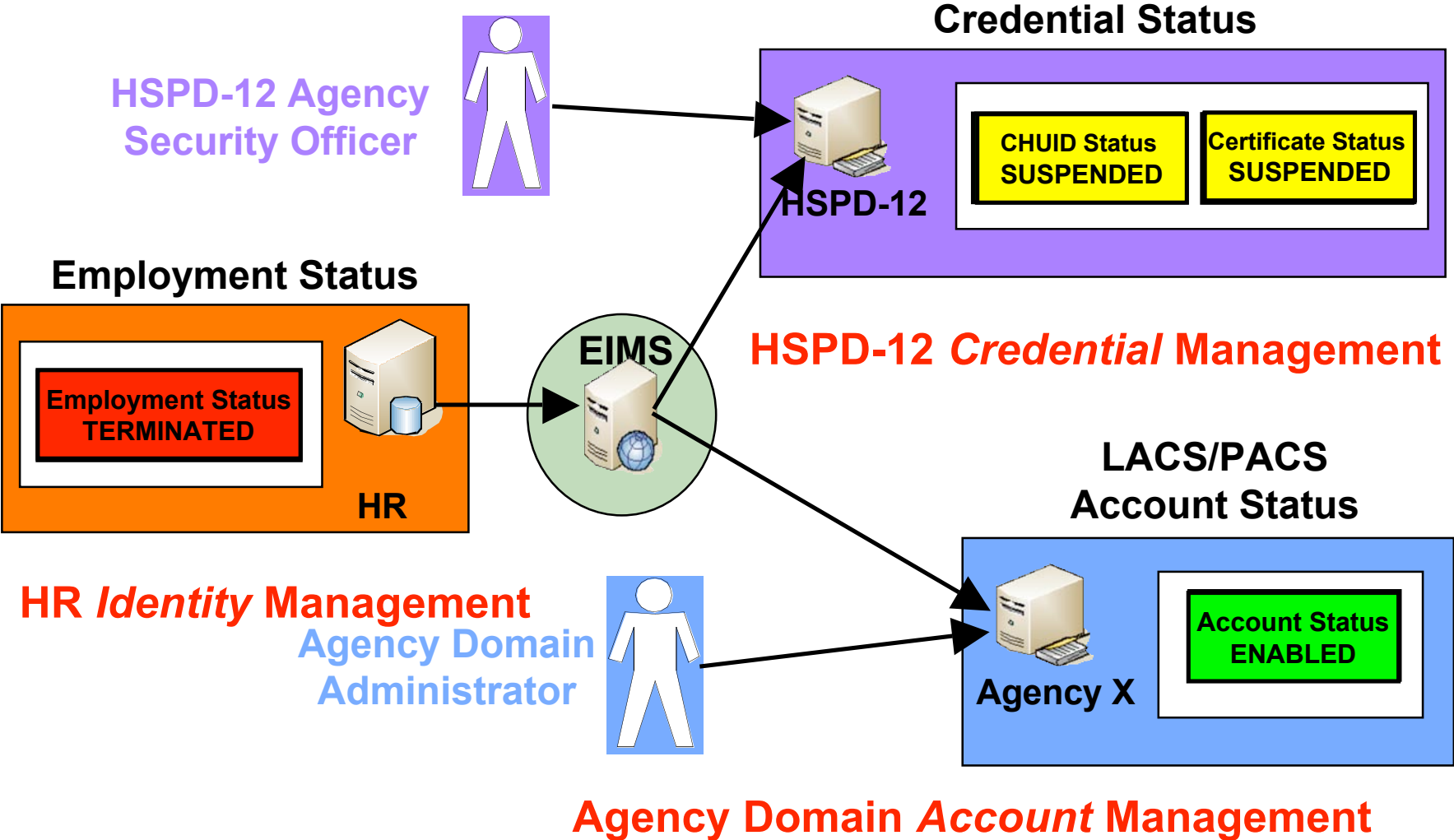


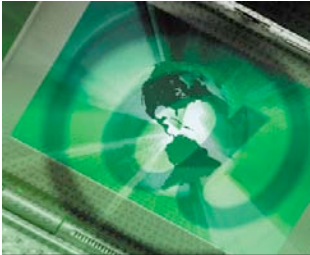
# Process Steps – New Hire Activation





# Suspension/Termination Actions

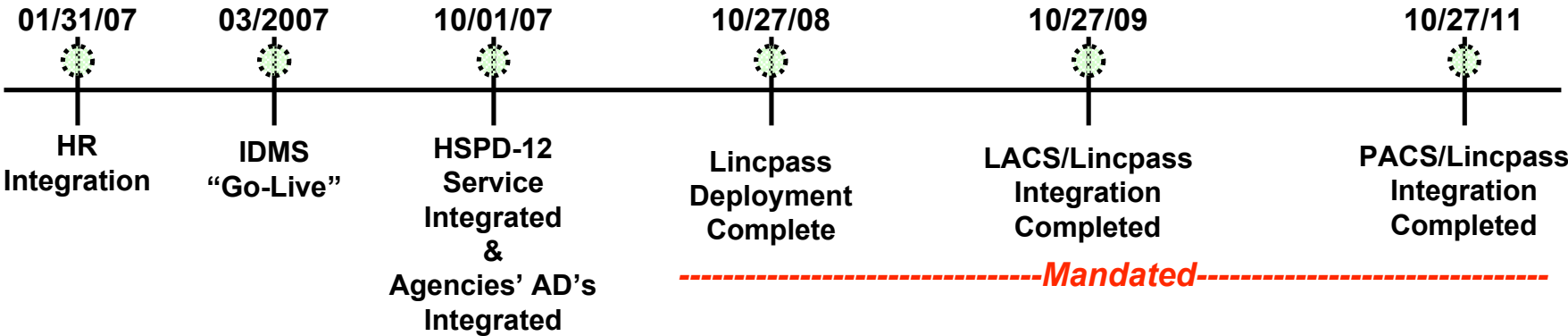


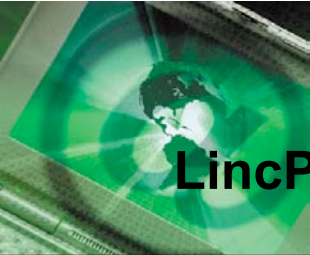


# EIMS Implementation Schedule

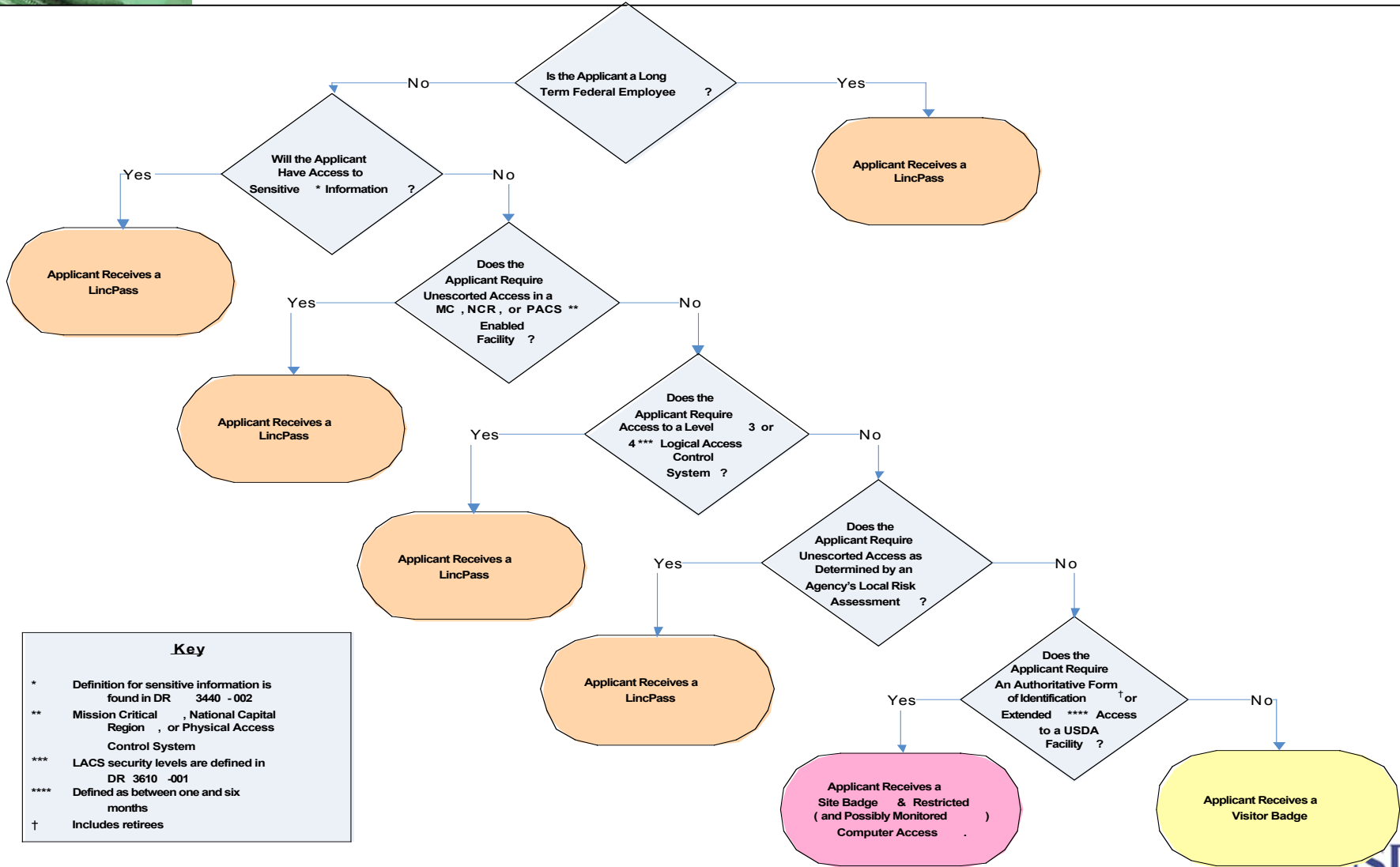
*The EIMS implementation schedule is key to fulfilling the HSPD-12 mandate:*

## High Level Timeline





# LincPass Risk Assessment Decision Tree (DRAFT)



**Key**

- \* Definition for sensitive information is found in DR 3440 - 002
- \*\* Mission Critical, National Capital Region, or Physical Access Control System
- \*\*\* LACS security levels are defined in DR 3610 - 001
- \*\*\*\* Defined as between one and six months
- † Includes retirees





***Feedback?***

***Are we way off track?***

***What other strategies are occurring?***

***Where are conversations happening?***