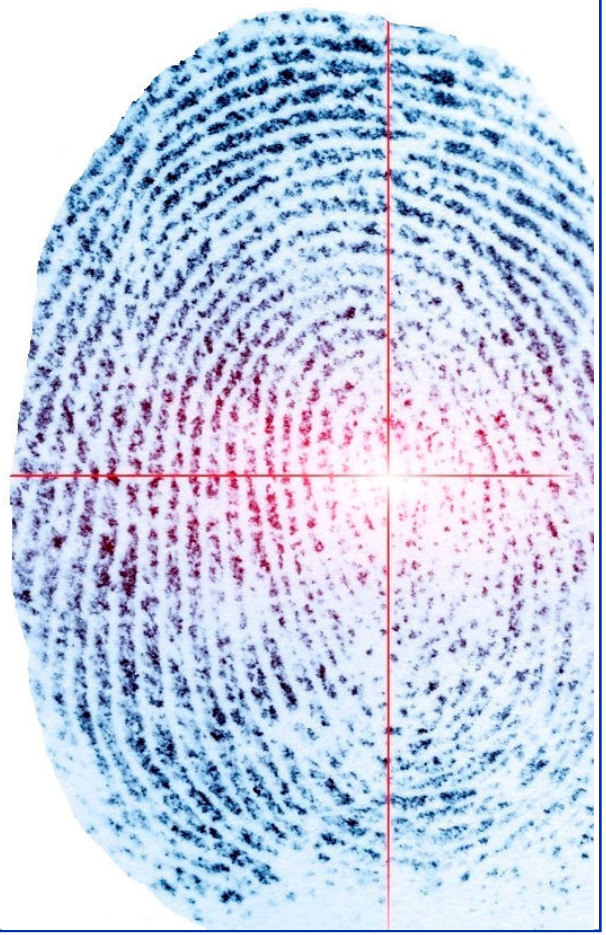
GSA OCIO

GSA Progress Towards Meeting HSPD-12 and M-11-11 Goals

Presentation to the Smartcard Industry Alliance



Identity, Credential and Access Management (ICAM) Division

November 2011

GSA Progress towards achieving HSPD-12 & M-11-11 Goals

- **Credentialing of Personnel – 99% of employees have PIV cards**
  - Contractors lagging in remote areas – but don't have systems access
- **Mandatory use of PIV Card for login – 99% of users using PIV card for workstation login**
  - Fallback to temporary username/password for lost or damaged PIV cards
- **Implementation of a COTS IAM Suite (GAMS) underway to meet FICAM recommendations**

GAMS
GSA Access Management System

ICAM
Identity, Credential, and Access Management

Identity, Credential, and Access Management

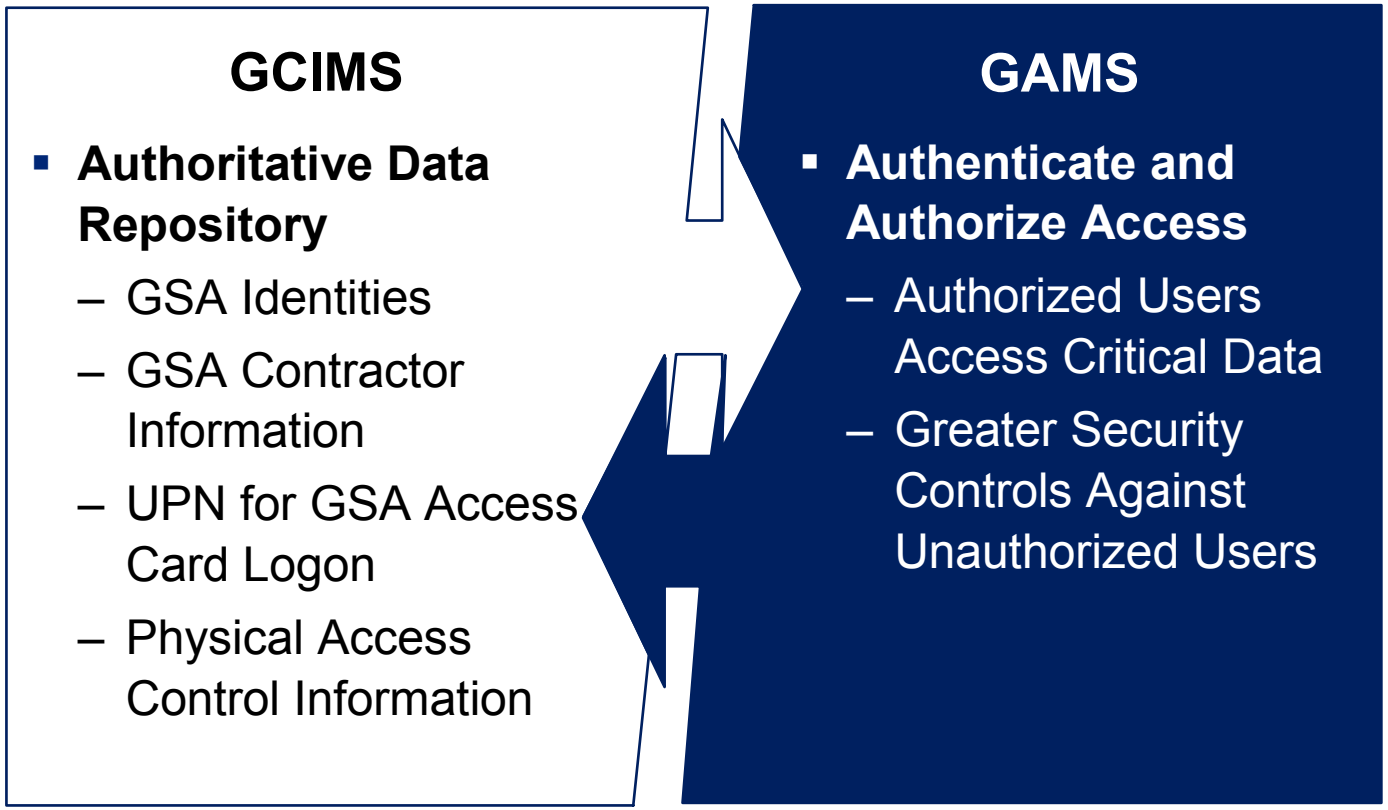
IC=GSA Credential & Identity Management System (GCIMS)

AM=GSA Access Management System (GAMS)

GSA Access Management System (GAMS) and GSA Credential and Identity Management System (GCIMS) provide a complete Identity, Credential, and Access Management (ICAM) solution for GSA!

GAMS and GCIMS Work Together

GAMS works in collaboration with GCIMS



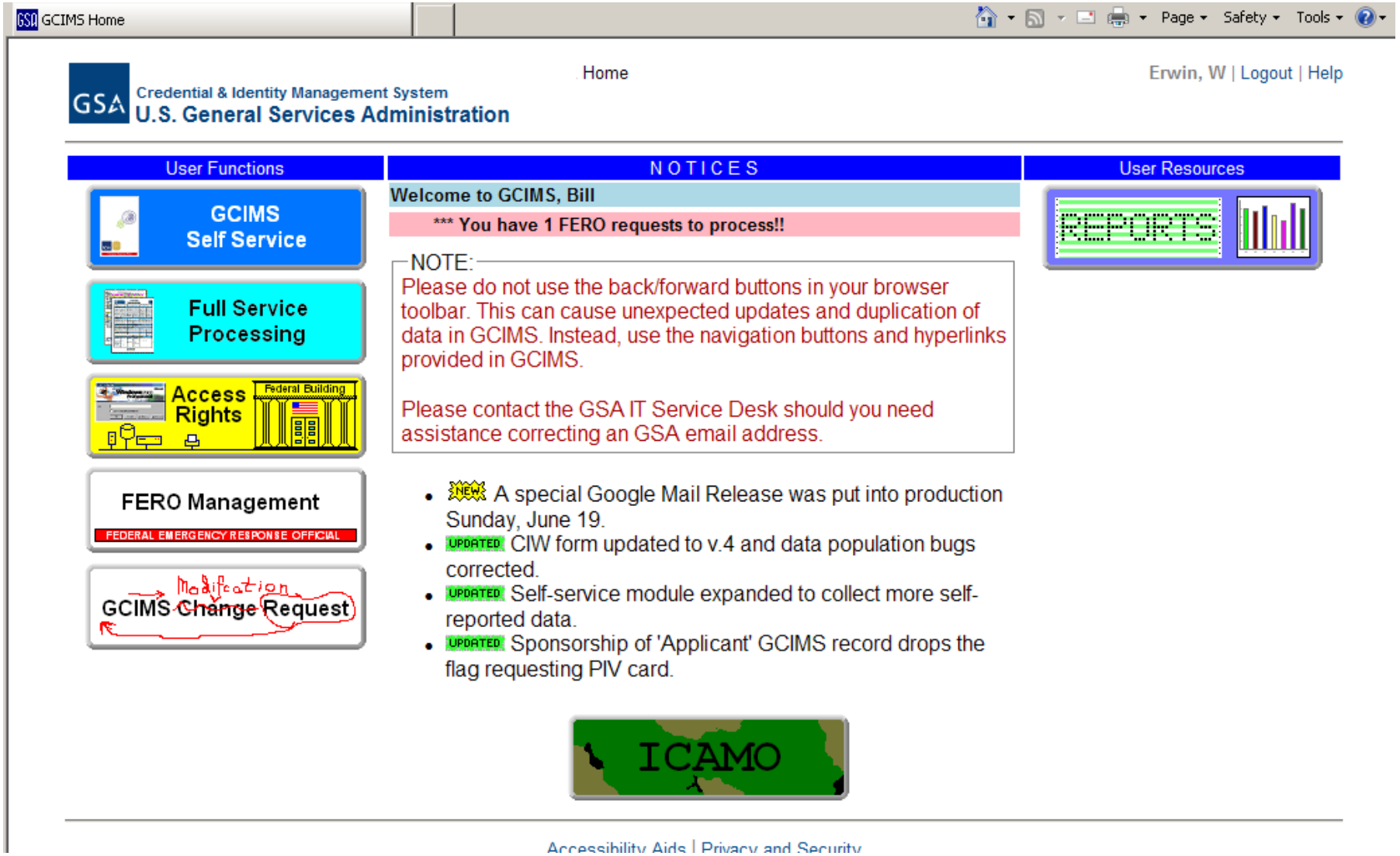
GSA Credential and Identity Management System (GCIMS)

- **Began life as an "identity aggregator" in 2007**
  - Pull information from HR and Personnel Security
- **Grew into ultimate source of identity for GSA personnel**
  - First system into which new personnel are entered (electronic fingerprints through MSO)
- **Communicates with GSA MSO through web services**
  - Can also fall back to passing "bulk upload" files and pulling reports
- **Links to many other systems**
  - Active Directory (assigns UPN)
  - Email (provisions and maintains employee directory)
  - Personnel system (CHRIS) (pull and coming soon, update as well)
  - PBS Building Inventory (no more mis-typed work addresses)
  - PACS systems (including external agencies)
  - Others…

GAMS
GSA Access Management System

ICAM
Identity, Credential, and Access Management

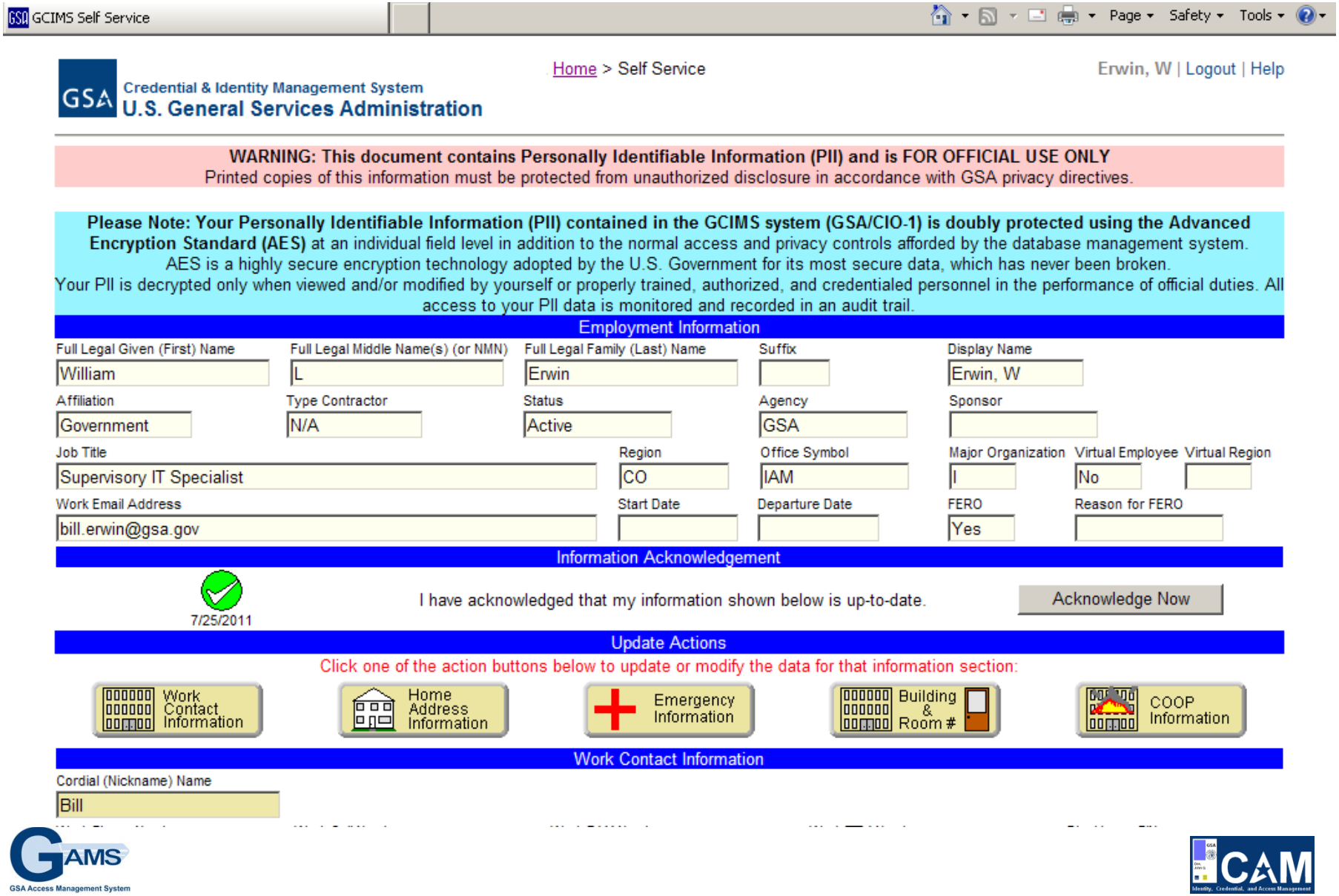
GCIMS Main Menu



GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management

GCIMS Self Service



GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management

GCIMS Data Benefits

- **System combining identity management data (Name, SSN, DOB, Gender, Home Address) combined with agency specific data (Office Symbol, Region, Work Building, Pay Grade) provides unique opportunities in addition to such things as feeding employee directories and the like:**
  - Building gender/age profile (HR – wellness)
  - Home-Work commuting distance (CFO – commuting profiles)
  - Personnel numbers by locality (Mobile enrollment planning, etc.)
  - Building occupancy profile (Feds/Contractors by building – space planning)
  - Building occupancy list (emergency management)
  - Building SSO occupancy breakdown (CFO – chargeback for space)
  - Full-time teleworkers (HR – policy)
  - FERO areas of expertise (FEMA requirements)

GSA Access Management System (GAMS)

GSA Access Management System (GAMS)

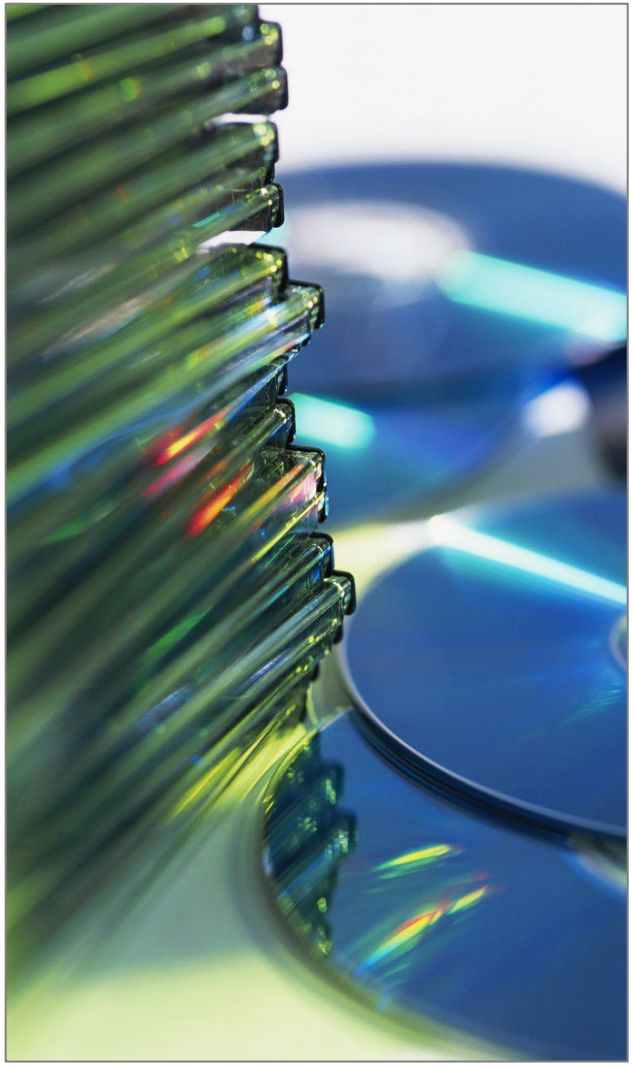
- **Industry standard Identity and Access Management (IAM) System**
  - Started life as a pilot with Sun Identity Manager
- **Was first implementation of combined Sun and Oracle Identity Management product lines**
  - GSA and Oracle teams had each other on speed dial
- **Authority to Operate (ATO) held up for over 6 months for security review and re-architecture**
  - SAISO concerned over “keys to the kingdom”
  - Delay allowed completion of all planned releases instead of Version 1.0
- **Went live in June 2011**
  - First system integrated in July 2011
  - Three other systems in-progress, up to 150 systems will ultimately be integrated
- **Expected savings of $23 million per year upon full implementation**

GAMS
GSA Access Management System

ICAM
Identity, Credential, and Access Management

GAMS Services Based on Oracle IAM Platform

- Oracle Access Manager (OAM)
- Oracle Identity Manager (OIM)
- Oracle Virtual Directory (OVD)
- Oracle Identity Federation (OIF)
- Oracle Internet Directory (OID)
- Oracle Entitlement Server (OES)
- Oracle OpenSSO Fedlet + STS Technologies
- Oracle Enterprise Single Sign-On (OESSO)
- Oracle Identity Analytics (OIA)
- Oracle 11g Database

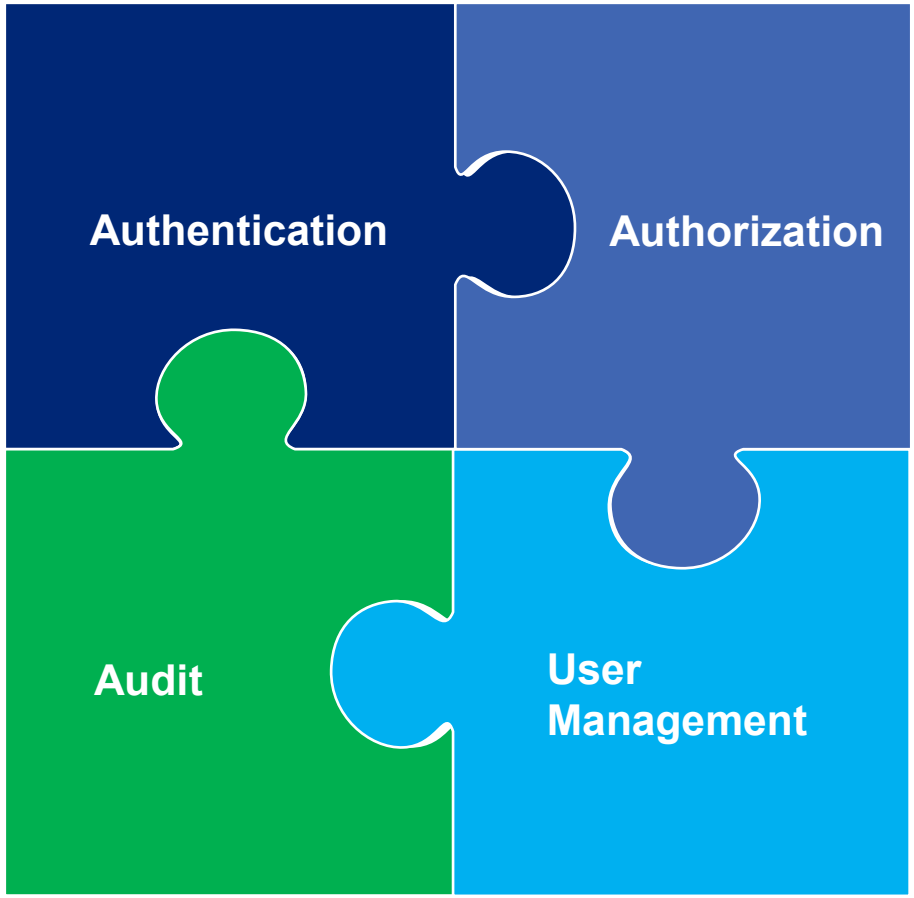


GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management

GAMS Delivers Agency-Wide Functionality

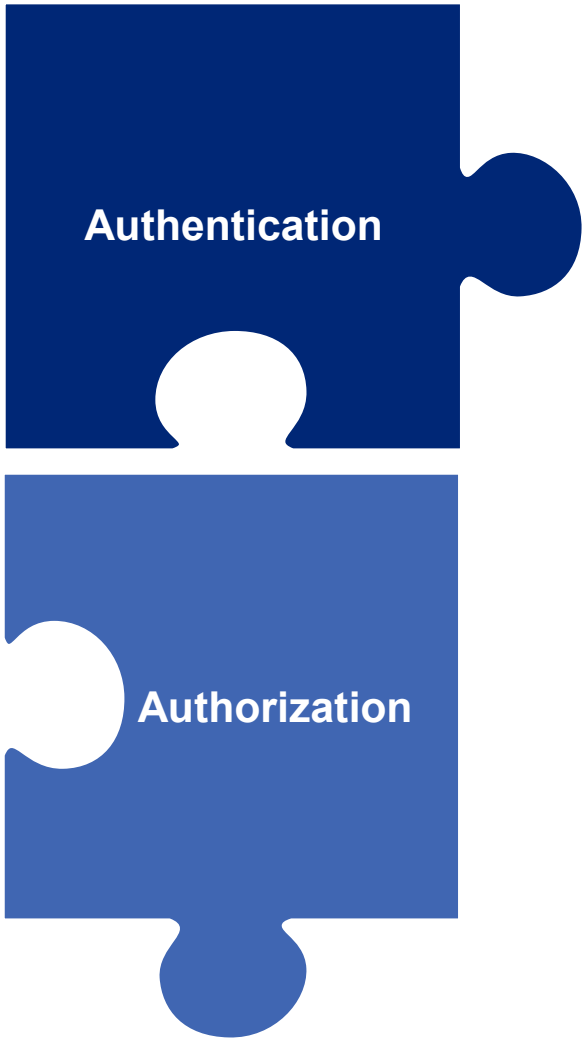
Shared identity and access management services for application business owners to verify and authorize user access requests



GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management

GAMS Delivers Agency-Wide Functionality (Continued)



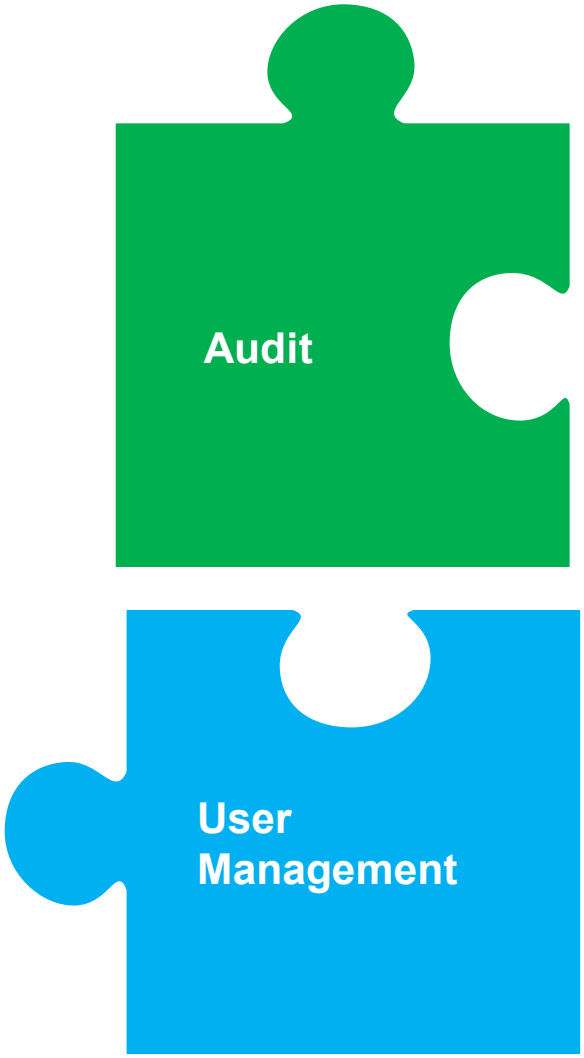
- **Authentication Services**
  - Logon-related services that validate the identity of users attempting to access GSA applications or network
  - Ensures users are who they claim to be when they attempt to access applications protected by GAMS

- **Authorization Services**
  - Enables and controls application access for GAMS users
  - Supports the creation of IT accounts and the assignment of access privileges

GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management

GAMS Delivers Agency-Wide Functionality (Continued)



- **Audit Services**
  - Identifies policy non-compliance issues and violations (e.g. segregation of duties violations)
  - Provides access forensics including who has accessed, or attempted to access, an application and when

- **User Management**
  - Provides a self-service Web portal where users can request access to IT applications and physical GSA assets
  - Automates logon to IT applications for users
  - Prevents unauthorized access to private data by providing greater security controls

GAMS
GSA Access Management System

ICAM
Identity, Credential, and Access Management

GAMS Services

GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management

GAMS Issues

- **Oracle acquisition of Sun in mid-procurement caused 4-month delay**
- **Security concerns caused re-architecture of entire GSA network to provide multi-tier security – GSA Secure Network (GSN)**
  - About 6 months to plan, implement, and test
  - New hardware, software, support arrangements
  - Move to GSN took a month for reconfiguration of all GAMS components
- **Initial customer enthusiasm turned to ??**
  - What – you actually completed it?
- **Changes in personnel**
  - Champions moved to new positions or left agency
- **Newer applications have IAM capabilities built-in but legacy applications can require extensive retrofit**
- **Budget cuts may impact planned system integrations**

GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management

In Conclusion

- GSA well along the path to meeting goals of HSPD-12 and M-11-11
- Slower than desired but lots of relatively new ground to break
- Users finding it easier (single sign-on)
- System owners will benefit through automated provisioning and workflows
- Business line owners will benefit by getting their people to work faster
- Lots of money up front (hardware, software, user licenses) but great return on investment down the road

GAMS
GSA Access Management System

ICAM
Identity, Credential, and Access Management

Contact Information

Bill Erwin
Director
Identity, Credential, and
Access Management Office
General Services Administration
(202) 501-0758
bill.erwin@gsa.gov
1275 1st Street, NE
Washington, DC 20417

GAMS
GSA Access Management System

CAM
Identity, Credential, and Access Management