



**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



- **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**

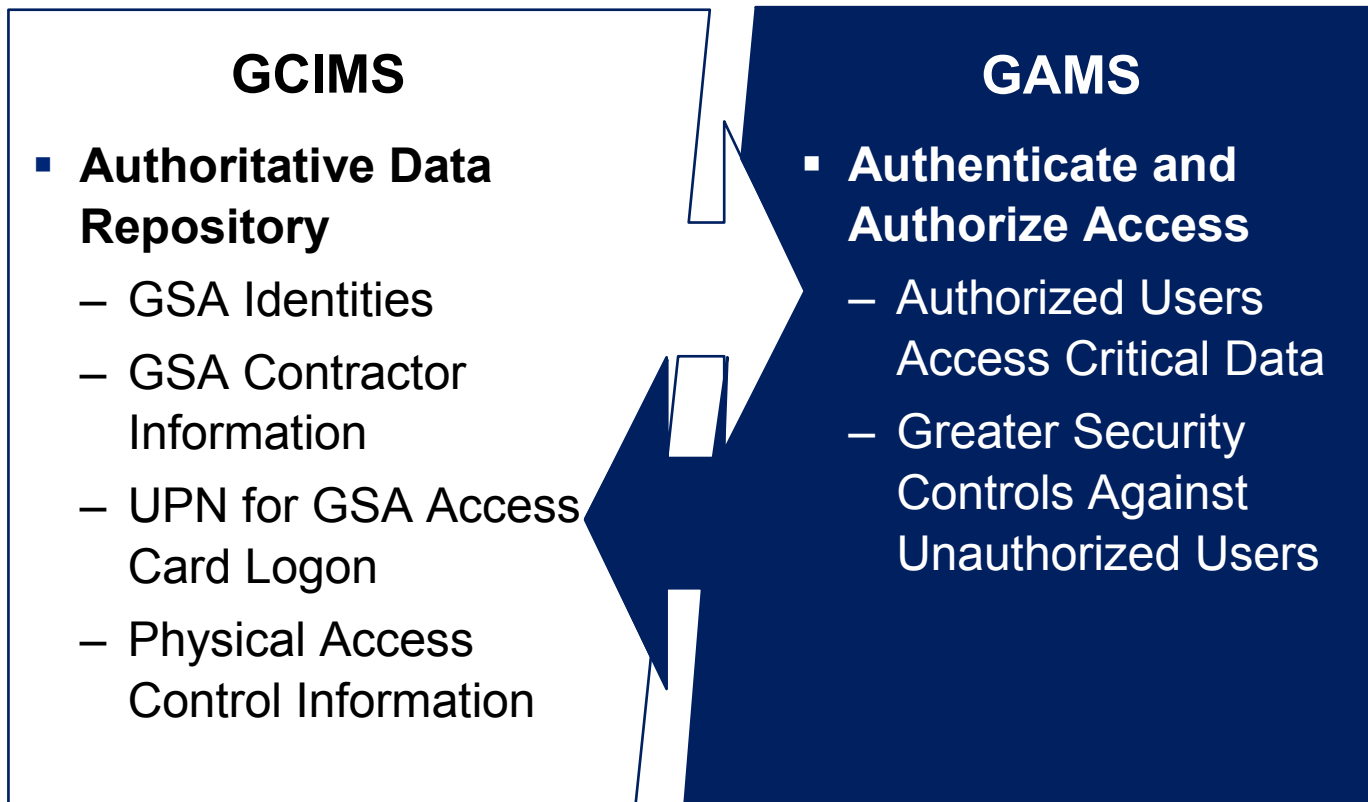


**IC=GSA Credential & Identity Management System (GCIMS)**

**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 works in collaboration with 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...

### User Functions



### NOTICES

Welcome to GCIMS, Bill  
\*\*\* You have 1 FER0 requests to process!!

**NOTE:**  
Please do not use the back/forward buttons in your browser toolbar. This can cause unexpected updates and duplication of data in GCIMS. Instead, use the navigation buttons and hyperlinks provided in GCIMS.  
Please contact the GSA IT Service Desk should you need assistance correcting an GSA email address.

- **NEW** A special Google Mail Release was put into production Sunday, June 19.
- **UPDATED** CIW form updated to v.4 and data population bugs corrected.
- **UPDATED** Self-service module expanded to collect more self-reported data.
- **UPDATED** Sponsorship of 'Applicant' GCIMS record drops the flag requesting PIV card.

### User Resources





# GCIMS Self Service

**WARNING: This document contains Personally Identifiable Information (PII) and is FOR OFFICIAL USE ONLY**  
Printed copies of this information must be protected from unauthorized disclosure in accordance with GSA privacy directives.

**Please Note: Your Personally Identifiable Information (PII) contained in the GCIMS system (GSA/CIO-1) is doubly protected using the Advanced Encryption Standard (AES) at an individual field level in addition to the normal access and privacy controls afforded by the database management system.**  
AES is a highly secure encryption technology adopted by the U.S. Government for its most secure data, which has never been broken. Your PII is decrypted only when viewed and/or modified by yourself or properly trained, authorized, and credentialed personnel in the performance of official duties. All access to your PII data is monitored and recorded in an audit trail.

Employment Information							
Full Legal Given (First) Name	Full Legal Middle Name(s) (or NMN)	Full Legal Family (Last) Name	Suffix	Display Name			
William	L	Erwin		Erwin, W			
Affiliation	Type Contractor	Status	Agency	Sponsor			
Government	N/A	Active	GSA				
Job Title	Region	Office Symbol	Major Organization	Virtual Employee	Virtual Region		
Supervisory IT Specialist	CO	IAM	I	No			
Work Email Address	Start Date	Departure Date	FERO	Reason for FERO			
bill.erwin@gsa.gov			Yes				

### Information Acknowledgement



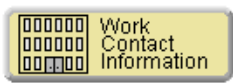
7/25/2011

I have acknowledged that my information shown below is up-to-date.

Acknowledge Now

### Update Actions

Click one of the action buttons below to update or modify the data for that information section:



### Work Contact Information

Cordial (Nickname) Name  
Bill



- **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)
  - FERRO areas of expertise (FEMA requirements)

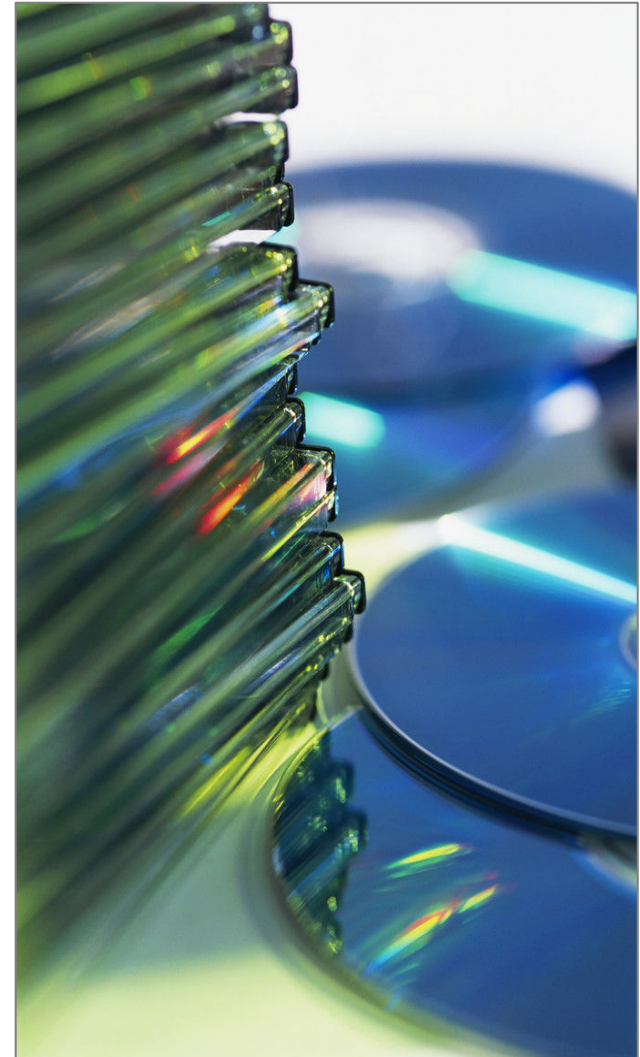




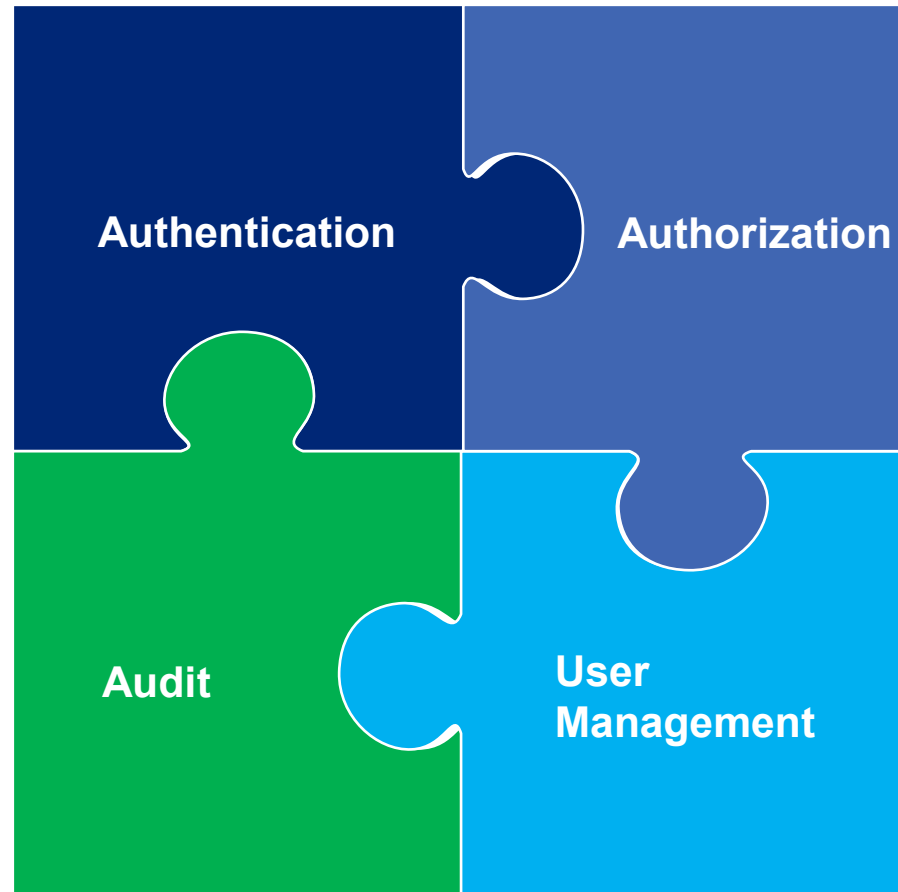
## GSA Access Management System

- **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**

- 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



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





### Authentication

- **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

- **Authorization Services**

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



### Audit

#### ■ 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

#### ■ 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 Services



- **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**



- **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**



## Contact Information

---

### **Bill Erwin**

Director

Identity, Credential, and

Access Management Office

General Services Administration

(202) 501-0758

[bill.erwin@gsa.gov](mailto:bill.erwin@gsa.gov)

1275 1st Street, NE

Washington, DC 20417

