

# HIMSS/GSA E-Authentication Initiative A Pilot Project of the HIMSS RHIO Federation

**HIMSS Public Policy Forum  
September 28, 2006**

*Mary Grizkewicz, HIMSS  
David Temoshok, GSA*

# Discussion

- Background
- E-Authentication Service Component Architecture
- HIMSS/GSA E-Authentication Pilot

# *Background*

# Purpose of this Project

This project represents to date the work that is being done by Health Information Technology professionals with their communities to advance the roll-out of security identity management infrastructure in the health IT sector.



# Project Overview

The Healthcare Information and Management Systems Society (HIMSS) and the General Services Administration (GSA) are collaborating on a pilot project to demonstrate the use of the Electronic Authentication Service Component in a healthcare setting.

That setting consists of seven Regional Health Information Organizations (RHIOs) and health information exchanges (IHEs) that are members HIMSS.

# HIMSS/GSA Relationship

The ongoing partnership between HIMSS and the GSA began five years ago when the GSA approached HIMSS with their need to advance the next phase of the Consolidated Health Informatics eGov initiative.

# Office of the National Coordinator (ONC)

## 2004 – “Strategic Framework” Sets the Stage

Goal 1: Inform Clinical Practice

**Goal 2: Interconnect Clinicians**

**Identify interoperability as a major milestone for achieving improved healthcare delivery; encourage regional healthcare information organization (RHIOs) and a national health information network.**

Goal 3: Personalize Care

Goal 4: Improve Population Health

# **HIMSS Responds – Develops the HIMSS RHIO Federation**

HIMSS immediately recognized that the vision for national Health IT infrastructure as articulated by the ONC was consistent with their vision, and the HIMSS NHII Task Force was re-cast as the HIMSS RHIO Federation Task Force.

# Background on HIMSS RHIO Federation

RHIO Federation connects, provides real-world tools, advocacy support and education for organizations involved in regional healthcare information organizations (RHIOs) and health information exchanges (HIE).

The concept of a HIMSS RHIO Federation began four years ago as a result of work done by the HIMSS NHII Task Force, chaired by Dr. C. Martin Harris, CIO of the Cleveland Clinic Foundation.



# *E-Authentication Service Component Architecture*

# Prioritize E-Government

- **President's Management Agenda:**
  - ✓ **Expanded Electronic Government**
  - ✓ GSA to provide common infrastructure for Federal Government to authenticate all users – individuals, businesses, government



# E-Authentication Key Policy Considerations

- **For Government-wide deployment:**
  - No National ID
  - No National unique identifier
  - No central registry of personal information, attributes, or authorization privileges
  - Different authentication assurance levels are needed for different types of transactions
  - Authentication – not authorization
- **For E-Authentication technical approach:**
  - No single proprietary solution
  - Deploy multiple COTS products – user's choice
  - Products must interoperate together
  - Controls must protect privacy of personal information

# Federation Infrastructure

- Trust
  - ✓ Establish common trust model
- Business Relationships
  - ✓ Establish and administer common business rules
  - ✓ Manage relations among relying parties and CSPs
- Interoperable Technology (Communications)
  - ✓ Determine intra-Federation communication architecture
  - ✓ Administer common interface specifications, use cases, profiles

# Four Identity Assurance Levels

OMB E-Authentication Guidance establishes **four assurance levels** for consistent application of E-Authentication across gov't

**Level 1**

Little or no confidence in asserted identity (e.g. self identified user/password)

**Level 2**

Some confidence in asserted identity (e.g. PIN/Password)

**Level 3**

High confidence in asserted identity (e.g. digital cert)

**Level 4**

Very high confidence in the asserted identity (e.g. Smart Card)

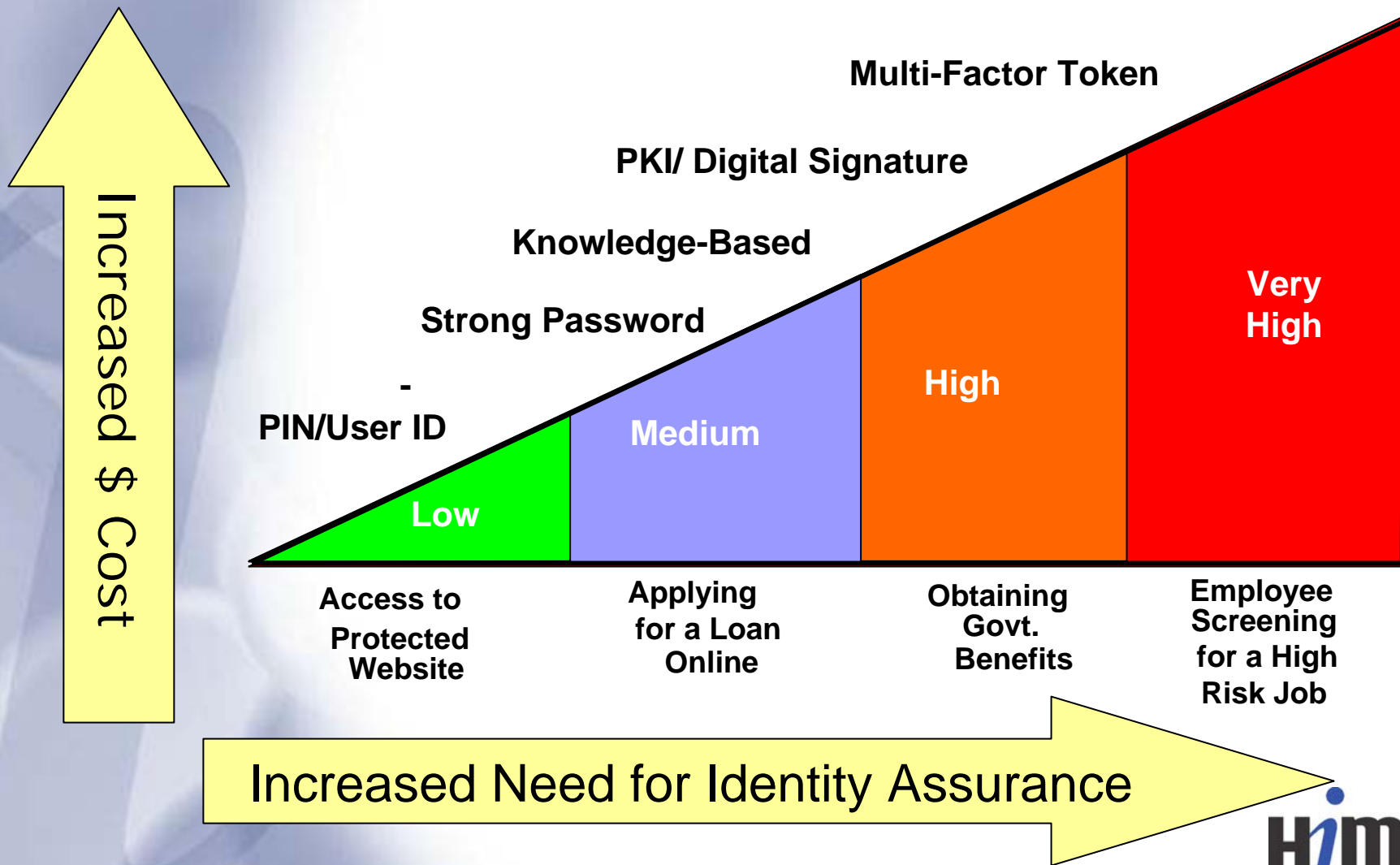


E-RA tool assists agencies in defining authentication requirements & mapping them to the appropriate assurance level



**NIST SP800-63  
Electronic  
Authentication  
technical guidance  
matches technology  
to each assurance level**

# Four Authentication Assurance Levels to Meet Multiple Risk Levels



# *Federal Trust Model for Federated Identity*

1. Establish & define authentication risk and assurance levels

2. Establish technical standards & requirements for e-Authentication systems at each assurance level

3. Establish methodology for evaluating authentication systems at each assurance level

5. Perform assessments and maintain trust list of trusted CSPs

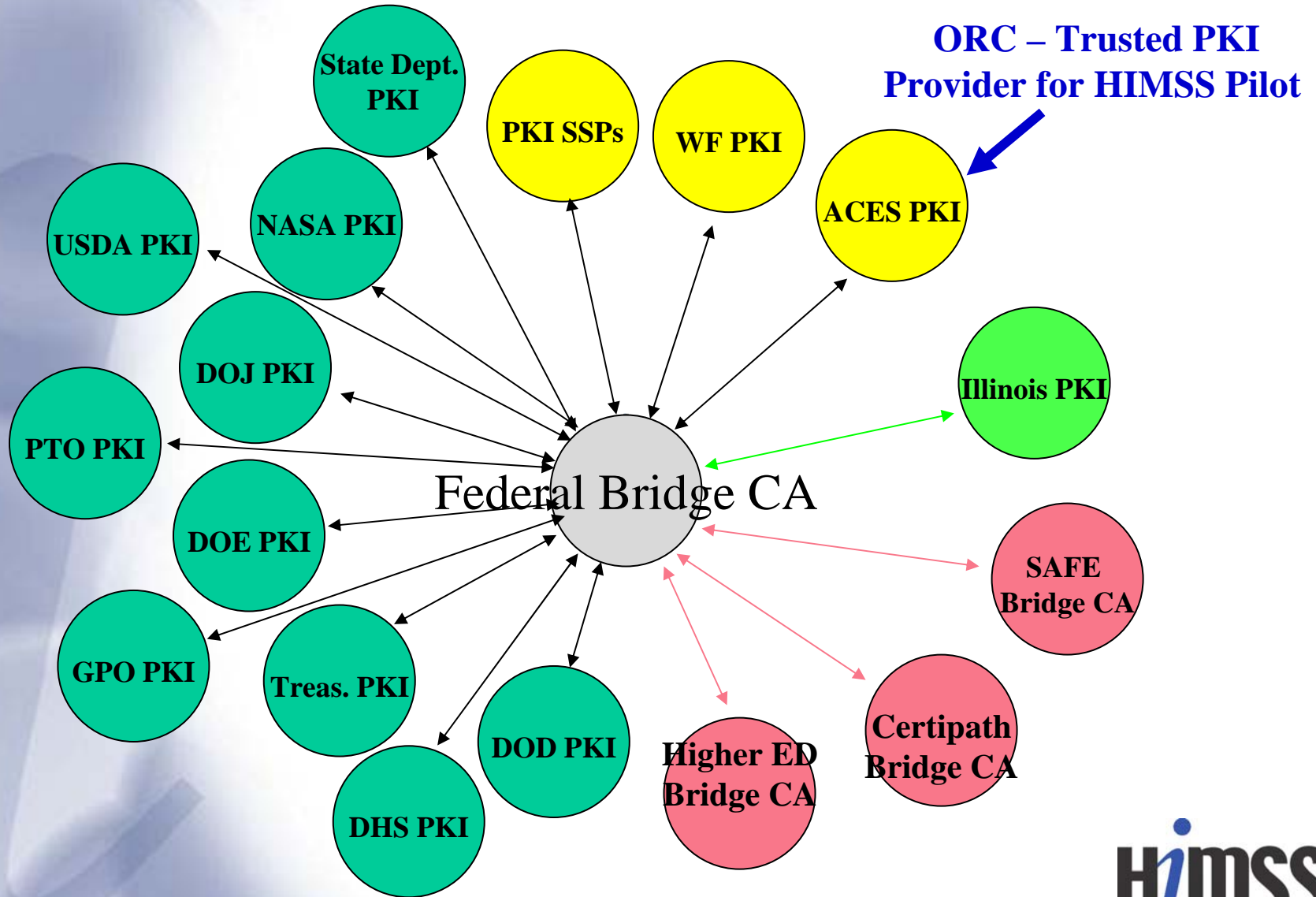
6. Establish common business and operating rules for participants

- OMB M-04-04 - *Established and defined 4 authentication assurance levels as Governmentwide policy*
- FBCA Certificate Policy - *Established 4 authentication assurance levels for Federal PKI domains*
- NIST Special Pub 800-63 Recommendation for E-Authentication – *Established authentication process & technical standards at 4 established assurance levels*
- FBCA Common, Commerce Certificate Policies – *Established PKI-specific standards and requirements.*
- Credential Assessment Framework – *Standard methodology for assessing authentication systems of credential service providers.*
- FBCA Cross-Certification Requirements – *Standard methodology for policy mapping, audit, and testing interoperability for cross-certification with the FBCA.*
- E-Authentication Trusted CSP List – *CAF, boarding & Interoperability testing*
- FBCA Trust List --*tests for policy mapping,, audit compliance, cross-certification & directory interoperability*
- EAI Federation Business and Operating Rules and Participant Agreements
- MOA with Federal PKI Policy Authority

# Key Architecture Design Considerations

- No central registry of personal information, attributes, or authorization privileges – decentralized approach means federation.
- Different authentication assurance levels are needed for different types of transactions.
- Architecture must support multiple authentication technologies.
- Architecture must support multiple protocols.
- Federal Government will not mandate a single proprietary solution, therefore, Architecture must support multiple COTS products.
- Federal Government will adopt prevailing industry standards that best meet the Government's needs.
- All architecture components must interoperate with ALL other components.
- Controls must protect privacy of personal information.

# A Snapshot of the U.S. Federal PKI



*HIMSS/GSA E-  
Authentication Pilot*

# The Problem ...

- “Can I trust that my personal health information remains private and only used when needed by an authorized professional?”
- Emerging health information exchanges, Regional Health Information Organizations (RHIOs), and the National Health Information Network (NHIN) all require security and privacy infrastructure **before a single transaction or health information exchange can take place**



# The Opportunity

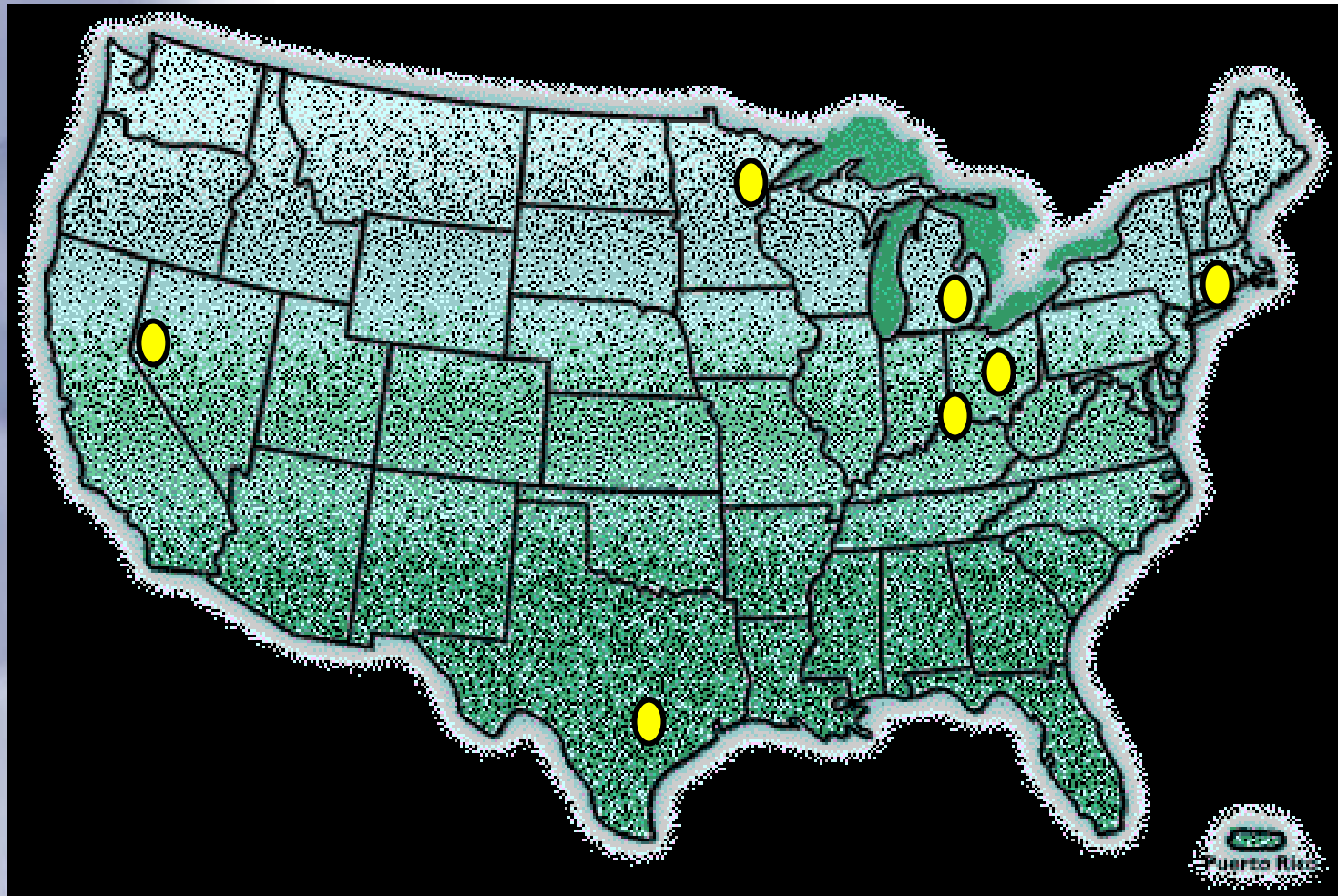
- Deploy scalable and interoperable security and identity management infrastructure for Federal e-Government in RHIO operating environment.
- Provide secure, trusted identity credentials.
- Leverage interoperability and trust with the Federal Government and multiple entities through the Federal Bridge CA.



# Participating RHIOs

1. e-Health *Connecticut*
2. Michigan Data Sharing & Transaction Infrastructure
3. CHRISTUS Health of Texas
4. Community Health Information Collaborative  
(Minnesota)
5. Nevada Single Portal Medical Record
6. Ohio Supercomputer Center Bioinformatics
7. Virtual Medical Network (Cincinnati, Ohio)

# National Coverage



# Technology Overview

- Pilot focus on strong authentication to securely and privately communicate and transfer data within and between RHIOs.
- Federal eAuthentication is providing trusted PKI service provider – ORC.
- Certificates used for single factor authentication, digital signature.
- Tokens (smart cards) used for security, multi-factor authentication, generate digital signature, and secure data storage and transport.

# Use Cases

While each RHIO has a unique initiative that requires an electronic authentication solution, the common functionality needed is for:

- Authenticating Digitally Signed Communication
- Authenticating Users at Health Portals

# Pilot Use Cases

<b>IHE/RHIO</b>	<b>Use Case Summary</b>
1. e-Health <i>Connecticut</i>	Authenticating clinician users for reviewing EHR data for encounters and follow-up.
2. Michigan, Data Sharing & Transaction Infrastructure	Authentication of clinical, administrative and billing (claim information).
3. CHRISTUS Health of Texas	Authentication of EHR data for first responders from RHIO participating hospitals
4. Community Health Information Collaboration, Minnesota	Portal Authentication, of clinicians users for reviewing clinical data.

<b>IHE/RHIO</b>	<b>Use Case Summary</b>
5. Nevada Single Portal Medical Record	Authentication for Emergency room referrals information for authorization between clinicians and insurers.
6. Ohio, Supercomputer Center Bioinformatics	Authentication of researchers for research data.
7. Virtual Medical Network (Cincinnati, Ohio)	Authentication of referral information between RHIO care providers.

# Project Status

1. Use Cases Identified – Completed
2. HIE/RHIO Registrars identified - Completed
3. HIE/RHIO Registrars trained - Completed
4. Certificates Issued – In process
5. Certificates in use – In process
6. Summarize findings – October, 2006
7. Initial Whitepaper issued – October, 2006
8. Updated issued – February, 2006 HIMSS Annual Conference, New Orleans

Questions?

# Contact Information

Marc Wine – [marc.wine@gsa.gov](mailto:marc.wine@gsa.gov)

Pete Palmer - [pete.palmer@wellsfargo.com](mailto:pete.palmer@wellsfargo.com)

Mary Griskewicz – [Mgriskewicz@himss.org](mailto:Mgriskewicz@himss.org)