Identity and Access Management Initiatives in the United States Government

Executive Office of the President
November 2008
Importance of Identity Management within the Federal Government

"Trusted Identity" is a key enabler for ensuring the safety and security of our national assets

A growing need to authenticate identity
- Determining access rights on a moment's notice is essential
- Denying access to those who would cause us harm

The following are among our objectives:
- Improve our security by implementing recommendations of the 9-11 Commission, etc
- Achieve appropriate identity assurance for
  - physical access
  - electronic access
- Implement common vetting processes, to extent practicable
- Increase use of cryptographic and biometric identity credentials
Federal Partnership with Private Sector

The United States government has partnered with the private sector on key identity and access management initiatives, to:

- Improve Homeland Security
- Identify solutions for enabling secure Electronic Authentication (E-authentication) through identity proofing and technical standards
- Ensure interoperability between federal credentialing programs (e.g. HSPD-12, First Responder Authentication Card, Transportation Working Identification Card) and the private sector
- Ensure appropriate privacy protections are effectively implemented
Implementing Secure Authentication and Ensuring Interoperability

E-Authentication Policy Framework (M-04-04 and NIST SP 800-63)
- Established a government-wide framework
- Describes four levels of identity assurance
  - 1- Little Assurance, 2- Some Assurance, 3- High Assurance, 4- Very High Assurance
- Requires agencies to review new and existing electronic transactions and implement appropriate identity proofing and technical solutions

General Services Administration works with private sector to:
- Ensure Products and Services offered to the federal government meet specific technical and policy requirements and facilitate interoperability
- Enable reuse of identity credentials through trust relationships between different government programs and external entities

Enablers of the E-authentication policy include HSPD-12 and Federal PKI
HSPD-12 & Federal PKI

Homeland Security Presidential Directive 12

- Enhances security, increases Government efficiency, reduces identity fraud, and protects personal privacy by establishing a mandatory, Government-wide standard for identity proofing and credentialing of federal employees and contractors.

- HSPD-12 credentials are used for both physical and logical access to federally controlled facilities and information systems.

- Technical standard is being leveraged by other federal programs (such as the First Responder Authentication Cards and Transportation Workers Identification Card) and external organizations to facilitate interoperability across domains.

- Successful interoperability testing between credentialing programs: Exercises include “Winter Storm” and “Summer Breeze” led by the Department of Homeland Security.

Federal Public Key Infrastructure Policy Authority

- An interagency body set up under the Federal CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.
Ensuring Privacy Protections

Federal Laws & Policies

- Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPPA)
- Office of Management & Budget privacy policies include:
  - M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
  - M-06-15, Safeguarding Personally Identifiable Information
  - M-07-04, Use of Commercial Credit Monitoring Services Blanket Purchase Agreements
  - M-08-10, Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements

Policies are intended to address recommendations of the Identity Theft Task Force

Federal CIO Council Security and Identity Management Committee (SIMC) established in September 2008

Inviting Private Sector Participation

- Identity Theft Task Force
- American Health Information Community
- DHS First Responder Partnership Initiative (FRPI)
Identity Management Task Force

• National Science and Technology Council chartered the IdM Task Force to assess the status of and challenges related to IdM technologies and to develop recommendations

• Three primary tasks were given:
  ➢ Provide an assessment of the current state of IdM in the U.S. government;
  ➢ Develop a vision for how IdM should operate in the future;
  ➢ Develop first-step recommendations on how to advance toward this vision.

• Twelve recommendations were provided which focus on:
  • Public Key Technology
  • Privacy
  • Interoperable digital identities
  • Identity applications interface
  • Secure authentication
  • Scalable authentication mechanisms
  • Biometrics
  • Federation with systems outside the federal government
  • Supply chain management
  • Security vulnerability analysis
  • Usability
  • Governance
Moving Forward

• The incoming Administration, which will be provided with the recommendations of the NSTC IdM Task Force etc, will determine next steps

• General Services Administration (GSA) to focus on:
  - Reducing authentication system development & acquisition costs
  - Facilitating more cost effective solutions for providing credentials to business partners or, through trust relationships, leverage credentials issued by external entities
  - Ensuring interoperability

• GSA and Federal CIO Council groups, in coordination with other IdM program representatives and industry, to develop the Federal Identity Management Handbook
http://www.whitehouse.gov/omb
http://www.biometrics.gov
http://www.cio.gov
http://www/nist.gov
http://www.idmanagement.gov
http://www.idtheft.gov

Contacts
Duane Blackburn (OSTP), Duane_M._Blackburn@ostp.eop.gov
Carol Bales (OMB), Carol_Bales@omb.eop.gov
Legislative Background

Clinger-Cohen Act of 1996
- Provides processes for executive agencies to analyze, track, and evaluate the risks and results of major IT investments
- Mandates reporting on the program performance benefits

Paperwork Reduction Act of 1995
- Establishes information resources policy & principles

E-Government Act of 2002
- Promotes the dissemination of government information through:
  - USA.gov
  - Regulations.gov

Federal Information Security Management Act of 2002
- Provides a comprehensive framework for information security standards and programs
- Provides uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes

Government Performance Results Act
- Holds Federal agencies accountable for achieving program results
- Emphasizes results, service quality and customer satisfaction

Freedom of Information Act
- Protects democracy by establishing presumption all government information is public unless exempted from disclosure (e.g., classified)

Privacy Act
- Requires Federal agencies to develop systems of record for any information in their possession that identifies an individual by name, number, or any identifying particular assigned to that person
Privacy Act

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

Scope

• The Privacy Act does apply to the records of every "individual," but the Privacy Act only applies to records held by an agency

Access to Records

Each agency that maintains a system of records shall...

1. Upon request by any individual, permit them to review the record and have a copy made of all or any portion thereof in a form comprehensible to them
2. Permit the individual to request amendment of a record pertaining to them

Exceptions

• For statistical purposes by the Census Bureau and the Bureau of Labor Statistics
• For routine uses within a U.S. government agency
• For archival purposes "as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government"
• For law enforcement purposes
• For congressional investigations
• Other administrative purposes
In an effort to properly safeguard our information assets while using information technology both on-site and remotely, all departments and agencies are recommended to:

- Implement the National Institute of Standards and Technology’s checklist to protect remote information.
- Encrypt all data on mobile computers/devices which carry agency data (unless the data is determined to be non-sensitive);
- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- “Time-out” remote access and mobile devices’ users after 30 minutes inactivity and require re-authentication; and
- Log all computer-readable data extracts from databases holding sensitive information and verify that each extract has been erased within 90 days or its use is still required.
M-07-16 -- Safeguarding Against and Responding to the Breach of Personally Identifiable Information

To safeguard and prevent the breach of personal information possessed by the government is essential in retaining the trust of the American public. As such, agencies are required to develop and implement a breach notification policy that applies to all Federal information and information systems (e.g. paper, electronic, etc.).

In formulating a breach notification policy, agencies must:
- Review their existing requirements with respect to Privacy and Security;
- The policy must include existing and new requirements for Incident Reporting and Handling as well as External Breach Notification;
- Finally, this document requires agencies to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information.

Notes
- As part of the work of the Identity Theft Task Force, this memorandum requires agencies to develop and implement a breach notification policy within 120 days
- Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months.
- Materials created in response to M-07-16 should be made available to the public through means determined by the agency (e.g. posted on the agency web site, by request, etc.)

Cost-Effective Steps
- Reducing the volume of collected and retained information to the minimum necessary;
- Limiting access to only those individuals who must have such access; and
- Using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.
M-06-15, Safeguarding Personally Identifiable Information

This memorandum reemphasizes your many responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and train your employees on their responsibilities in this area.

**Agency Responsibilities:**

- Senior Official for Privacy conduct a review of your policies and processes
  - take corrective action as appropriate to ensure your agency has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.
  - Shall address all administrative, technical, and physical means used by your agency to control such information, including but not limited to procedures and restrictions on the use or removal of personally identifiable information beyond agency premises or control.
  - Shall be completed in time for you to include the results in your upcoming reports due this fall on compliance with the Federal Information Security Management Act (FISMA).
  - Include any weaknesses you identify in your security plans of action and milestones already required by FISMA.

**Reminder**

- Agency responsibilities under FISMA and related policy to promptly and completely report security incidents to proper authorities, including Inspectors General and other law enforcement authorities.
This memorandum is to alert you to the recent establishment of government-wide blanket purchase agreements (BPAs) for commercial credit monitoring services and encourage agency consideration of these vehicles to the maximum extent practicable.

**Purpose**

- To help protect affected individuals if their personally identifiable information has been lost or stolen, credit monitoring services may be utilized when the agency has determined that mitigation efforts, including credit monitoring, are required to mitigate potential damage due to a data security breach.
- To assist in making these determinations, agencies should follow the recommendations developed by the President’s Identity Theft Task Force and provided in OMB’s September 20, 2006 memorandum “Recommendations for Identity Theft Related Data Breach Notification.”

**Credit Monitoring Services Initiative**

- Includes the establishment of BPAs against Federal Supply Schedule contracts to provide the government a fast and effective way to order commercial credit monitoring services.
- **The BPAs:**
  - Offer a variety of protection levels, depending on the degree of risk, vulnerability, and exposure encountered, and supports a consistent approach to mitigating the adverse impacts of personal data loss.
  - Do not obligate funds and the government is obligated only to the extent that authorized task orders are issued
  - Will not exceed a period of performance of five years
  - Will not be limited on the dollar value of task order purchases
  - Leverages the government’s spending power by offering reduced prices and enable improved oversight and better reporting.
M-08-10, Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)

This memorandum is to alert you to the establishment of government-wide blanket purchase agreements (BPAs) for independent risk analysis services and encourage agency consideration of these vehicles to the maximum extent practicable.

In the event of a data breach
- OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” requires agencies to promptly conduct a risk analysis and be prepared to submit a report containing the findings to the Congressional Oversight Committees of the U.S. Senate and House of Representatives, as appropriate.
- GSA has created a Government-wide vehicle for acquisition of independent risk analysis services.
  - Focuses on the need for independent risk analysis documenting the level of risk for potential misuse of sensitive information associated with a particular data breach.

Use of BPAs
- Reduce administrative costs to the Government by acquiring commercial items and services from GSA Multiple Award Schedule contracts.
- The BPAs offer a variety of services, including:
  - metadata analysis
  - pattern analysis
  - risk analysis
  - data breach analysis
  - response (one time assessment, not continuous monitoring)
  - privacy impact analysis
  - statistical analysis
  - reports on the probability compromised data has been used to cause harm
FISMA Act

Created in order to bolster computer and network security within the Federal Government and affiliated parties (such as government contractors) by mandating yearly audits.

Purpose

1. provide a comprehensive framework
2. recognize the highly networked nature of the current Federal computing environment
3. provide for development and maintenance of minimum controls required to protect Federal information and information systems
4. provide a mechanism for improved oversight of Federal agency information security programs
5. acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions
6. recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies

FISMA Compliance Process for an Information System

- FISMA imposes a mandatory set of processes that must be followed for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency.
- These processes must follow a combination of Federal Information Processing standards (FIPS) documents, the special publications SP-800 series issued by NIST, and other legislation pertinent to federal information systems, such as the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act.

<table>
<thead>
<tr>
<th>Processes</th>
<th>Determine the Boundaries of the System</th>
<th>Determine Information Types, Perform FIPS-199 Categorization</th>
<th>Document the System</th>
<th>Performing Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select and Implement a Set of Security Controls for System</td>
<td>Certification of System</td>
<td>Accreditation of System</td>
<td>Continuous Monitoring</td>
</tr>
</tbody>
</table>
Facilitating E-Government through IdAM


### OMB E-Authentication Guidance establishes Four Assurance Levels for Consistent Application of E-Authentication Across Government

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Little or no confidence in asserted identity – Self identified user with password (e.g. citizen accesses website using self-registered userid/password)</td>
<td>Some confidence in asserted identity – Userid/Password (Single factor) (e.g. citizen changes address of record through SSA website)</td>
<td>High confidence in asserted identity – Digital Certificate/PIN (multi-factor) (e.g. first responder accesses disaster reporting website to share operational information)</td>
<td>Very high confidence in the asserted identity – Smart Card/PIN (multi-factor) (e.g. officer accesses law enforcement database with criminal records)</td>
</tr>
</tbody>
</table>

**How do we credential users?**

Federal agency provided credentials for Levels 1 & 2 authentication (covers citizens, business partners, federal employees and contractors)

Trust relationships with external entities for Levels 1 & 2 (e.g. Fidelity, Wells Fargo, IdenTrust, InCommon)

Federal PKI provides up to Level 4 assurance and is a key enabler of trust in HSPD-12 credentials, as well as other credentialing programs cross-certified with the federal bridge.

Other internal agency capabilities.

Increased Need for Identity Assurance
HSPD-12 Directive

**HSPD-12 Objective:** Improve the security of our federal facilities and information systems by implementing common processes for identity proofing and ensuring interoperability through use of standardized credentials for physical and logical access.


http://csrc.nist.gov/publications/PubsSPs.html

**OMB guidance** – How agencies are to implement the Directive and Standard (M-05-24, M-06-06, M-07-06, M-08-01, etc)
http://www.whitehouse.gov/omb/memoranda/index.html

**GSA guidance** – Focuses on interoperability of HSPD-12 system components
http://www.smart.gov/awg/
Benefits of HSPD-12 Credentials

- Provide for digital signature, encryption, and archiving of documents to improve security and facilitate information sharing.

- Attain very high trust in identity credentials during disaster response, disaster recovery, and reconstitution of government scenarios.

- Attain a very high confidence in an asserted identity when logging onto government networks from remote locations.

- Protect PII on government laptops by enabling full disk encryption using the HSPD-12 credential as the encryption key.

- Use a single authentication token for physical and logical access to all applications within and across domains.
HSPD-12 Implementation Status

As of October 27, 2008:
HSPD-12 credentials issued to Employees: **1,249,685** (28%)
HSPD-12 credentials issued to Contractors: **338,427** (30%)

As of September 1, 2008:
Background investigations completed for Employees: **2.5 million** (52%)
Background investigations completed for Contractors: **600K** (42%)

Remaining Employees Requiring PIV credentials: **3.1 million**
Remaining Contractors Requiring PIV credentials: **800k**

Remaining Background Investigations to be completed for Employees: **2.4 million**
Remaining Background Investigations to be completed for Contractors: **800k**

* “US Military Personnel are included in Employee Numbers.
* Some Numbers are approximate.
The Federal Public Key Infrastructure (FPKI) Policy Authority is an interagency body set up under the Federal CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.