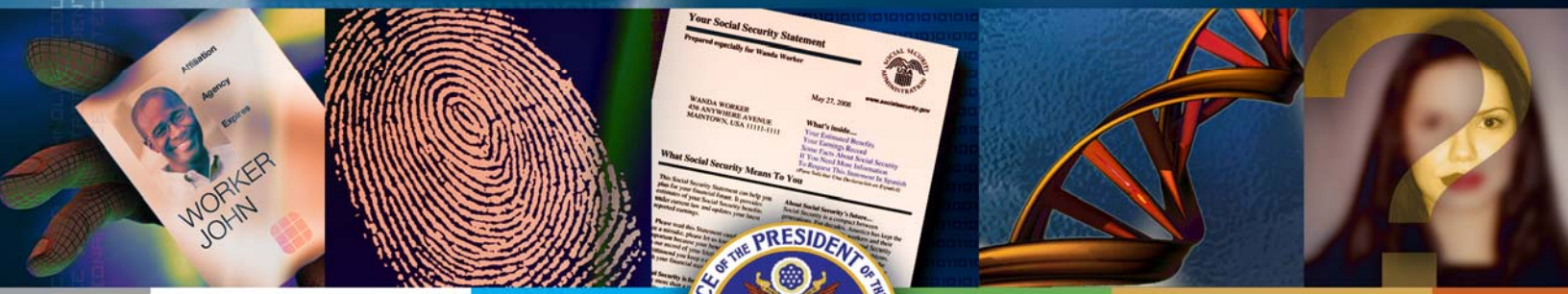
IDENTITY MANAGEMENT TASK FORCE REPORT 2008



EXECUTIVE SUMMARY

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL
SUBCOMMITTEE ON BIOMETRICS AND IDENTITY MANAGEMENT

About the National Science and Technology Council

The National Science and Technology Council (NSTC) was established by executive order Nov. 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the federal research and development enterprise. Chaired by the President, the NSTC is made up of the Vice President, the Director of the Office of Science and Technology Policy, Cabinet Secretaries and Agency Heads with significant science and technology responsibilities, and other White House officials.

A primary objective of the NSTC is the establishment of clear national goals for federal science and technology investments in a broad array of areas spanning virtually all mission areas of the executive branch. The Council prepares research and development strategies that are coordinated across federal agencies to form investment packages aimed at accomplishing multiple national goals.

The Subcommittee on Biometrics and Identity Management was chartered by the National Science and Technology Council (NSTC) Committee on Technology (COT) and has been in operation since 2003. The purpose of the Subcommittee is to advise and assist the COT, NSTC, and other coordination bodies of the Executive Office of the President on policies, procedures, and plans for federally sponsored biometric and Identity Management (IdM) activities. The Subcommittee facilitates a strong, coordinated effort across federal agencies to identify and address important policy issues, as well as researching, testing, standards, privacy, and outreach needs. The Subcommittee chartered this Task Force to assess the status of and challenges related to IdM technologies and to develop recommendations regarding the federal government's science and technology needs in this area. Additional information about the Subcommittee is available at www.biometrics.gov.

Acknowledgements

The Task Force would like to thank the following individuals for contributing to its success:

- Duane Blackburn (Office of Science and Technology Policy) for his vision to establish the Task Force and to populate it with individuals with such varying foci;
- Jim Dray (National Institute of Standards and Technology) and Judith Spencer (General Services Administration) for effectively managing the Task Force through six months of weekly meetings;
- FBI contractors Michelle Johnson (BRTRC) and Martin Harding (BRTRC) for managing the administrative aspects of the Task Force;
- James Ennis (State), Deborah Gallagher (DHS), William Gravell (DOD), Niels Quist (DOJ), and Bill Brykczynski (STPI) for chairing the Task Force's subordinate working teams;
- William Gravell (DOD) for the innumerable hours he personally devoted to massaging the views of the Task Force members into a cohesive, agreeable description in this report;
- Karen Evans (OMB), Carol Bales (OMB), and the members of the CIO Council, for their assistance in identifying the current status of IdM in the federal government;
- The staff at the Science and Technology Policy Institute (under contract to OSTP), for analyzing data received from the CIO Council;
- The staff at BRTRC, Inc., (under contract to FBI) for editing and graphics support; and
- The IDM Task Force members, who provided input and contributed a significant amount of their time over the course of the six-month effort, are listed in Annex B.

CONTENTS

EXECUTIVE SUMMARY

Introduction

Identity Management (IdM) has existed throughout history to serve both public and private purposes. It has continuously evolved to match changing operational needs, to take advantage of new capabilities, and to stay consistent with the societal conventions of the day. The most recent advancement in IdM has been its transition into the modern digital world, which has provided a wealth of previously impossible capabilities to support both security and convenience needs. Digital IdM systems are becoming increasingly commonplace, and their explosive growth is expected to continue.

> For the purposes of this Task Force, Identity Management means "the combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information. The primary goal of the IdM process is to assign attributes to a digital identity and to connect that identity to an individual." The terms of reference for this Task Force are at Annex A.

To date, this growth has been driven by the need to meet independent mission needs (including both screening applications and access control). As these missions continue to expand, overlaps across missions will become more and more pervasive. This is an undeniable truth, as all IdM systems relate back to an individual — actions taken within one system will potentially impact data and/or decisions in other systems. A holistic, cross-mission analysis and planning cycle has not previously been performed, presumably because of the tremendous scope of the task and the duty's inherent social sensitivity. This daunting task was as-

signed to the National Science and Technology Council's (NSTC) Task Force on Identity Management (Task Force), as a continuation of independently developed and managed government IdM systems will encounter operational, technological, and privacy issues that will become increasingly difficult to manage.

The Task Force's scope was limited to federal government systems, with the full understanding that these systems frequently rely on and impact IdM systems beyond federal control. This report presents an overview of the current state of federal IdM systems and also presents a high-level vision of how these systems can be holistically designed to provide better services while increasing privacy protection. The purpose of this report is to initiate further discussion on this vision, inform policy decisions, and provide direction on which to base near-term research.

Task Force Work

The Task Force was chartered to study federal IdM over a six-month period, with a broad range of representation from different government missions, and was given three primary tasks:

- 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.

The Task Force undertook two overlapping approaches to determine the current state of IdM in the U.S. government, a detailed assessment of publicly available Privacy Impact Assessments and an OMB-issued survey to the Federal Chief Information Officers' Council. The combined analysis showed that there are more than 3,000 systems within the U.S. government that utilize Personally Identifiable Information (PII), and the vast majority of these were designed and are managed independently from one another. These facts contribute to several issues with the current state:

- Duplicative identity data is often stored in multiple locations within the same agency, as well as across agencies, causing a negative impact on accuracy and complicating an individual's attempt at redress;

- A lack of commonly used standards makes appropriate cross-function collaboration difficult, thus impacting both time-sensitive mission needs as well as reducing personal privacy;

- Privacy protection efforts vary in complexity across agencies;

- There is no single government-wide forum responsible for coordinating and homogenizing IdM efforts across the U.S. government.

The IdM Task Force's vision for the future is a substantially more organized Identity Management framework. A fundamental precept for this vision is a realization that not all PII is created equal. Some PII will be useful for broad range of applications, while others are only useful within the context of a specific application and should not be shared outside that application. PII within both of these categories also have varying levels of sensitivity and should be managed accordingly.

The Task Force's vision includes a federated approach for leveraging broad-use PII elements to maximize accuracy, availability, privacy protection, and management of this data. Individual applications would access this data through a network grid, which can be established using common technical standards and policies to ensure appropriate use and control. Once verified, broad-use PII can be augmented with application-specific PII in order to make operational decisions. To this end, we make the following assumptions:

- Identity and the management of all the personal identifiable qualities of identity information are considered a critical asset in sustaining our security posture;

- To the extent available and practicable, a very high confidence in an asserted identity is recommended as the basis for authorization for access to government applications regardless of assurance level re-

quired. For example, Personal Identity Verification (PIV) credentials required by HSPD-12 and used by federal employees and contractors are available and provide for a very high level of confidence and could be used for accessing all applications — even those requiring lower levels of assurance;

- There is an expectation that revocation of identity data and the related authorizations are executed in accordance with government-wide standards throughout all applications (whether used to support logical or physical access);

- There is an understanding that management and protection of identity is not the responsibility of any one or a few federal agencies, but rather the responsibility of all federal agencies to enable. Identity is a component of each and every transaction. If one federal agency fails to carry out their responsibility, access to our networks and facilities will be significantly jeopardized.

Several top-level goals and characteristics for the government's proposed state of IdM can thus be described as:

- Configuration and operation of a "network of networks" to securely manage digital identities, based on a set of common data elements for stored PII that will allow it to be leveraged by a broad range of applications;

- Security of process, data transmission, and storage; this includes and embraces all features of confidentiality, integrity, authenticity, and privacy, including use of encryption and multifactor authentication;

- Auditability of processes, with complete, automatic, and secure record keeping;

- Ubiquitous availability, at global distances, of strong verification of stored digital identity when called for or needed to support an authorized application;

- Standards-based connectivity, interoperability, and extensibility of supporting IT architecture;

- Preservation of application-specific PII data under control of application sponsors, with minimal exposure to unauthorized access or unnecessary transmission across networks;
- Ability of prospective application sponsors to develop, install, and operate applications in a way that permits the supporting IT grid to be seen as a freely available, ubiquitous service.

The above elements form the tenets of a strategy to manage and protect identity within all federal agencies. Anticipated benefits over the current state include:

- Enhanced accuracy and management of PII that is used by multiple applications;
- Clear separation of application-specific PII and tighter controls to ensure this information isn't shared across domains;
- A uniform, more transparent approach of handling PII;
- Minimization of duplicative efforts to generate, maintain, and safeguard PII;
- Providing the government a better understanding of and ability to macro-manage its IdM activities.

This report offers a set of recommendations (see Section 4) organized into specific subject areas as follows:

- Standards and Guidance;
- Architecture;
- Science and Technology Considerations;
- Government-wide Coordination.

The Science and Technology recommendations may be acted upon immediately, as the success of those efforts will impact further analyses and policymaking required to provide depth and direction to the Task Force's initial vision.

Toward that end, the Task Force recommends an enduring IdM forum to visualize and address IdManagement issues holistically, in policy and technology. This process should seek to frame the governmental agenda in this broad area, inform the standards and guidance development activities, and guide the further refinement of the IdM architecture. In so doing, it should guide activities that will expand and refine our total understanding and support the development of consensus within an informed public regarding the whole range of IdManagement issues and opportunities within the federal enterprise.

Conclusion

It is important to note that the Task Force does not see this report as being the "final" analysis of the IdM needs of the federal government, nor is it considered to be a comprehensive treatment of the subject in a level of detail sufficient to determine formal policy. Rather, it is an initial study that provides a common foundation and vision on which to base future research, discussions, studies, and, eventually, policymaking. The Task Force aimed to make this report as intellectually comprehensive as possible within available time and resources, seeking, above all, to recognize and treat IdM in its full dimensions, including its growing importance to the conduct of government.

In contemplating the current state of IdM in the federal government, and thinking about the future direction, one may paraphrase Winston Churchill:

"It is not the end, nor even the beginning of the end; but it is, perhaps, the end of the beginning…"

The complete Task Force report is now available online at two locations:

http://www.ostp.gov/cs/nstc/documents_reports

and

http://www.biometrics.gov/NSTC/Publications.aspx