Identity Management

Issue Background

Federal, State, and local governments, international bodies, private sector organizations, and individual end users all depend on robust, reliable, and functional telecommunications networks for national security/emergency preparedness (NS/EP) functions as well as other business and personal needs. The increasing dependence on communications networks for conducting Government and commercial transactions requires the establishment of a strong identity management (IdM) framework that provides unique characteristics to an entity for secure authentication. However, trusted and strong identification of users, devices, and telecommunications service providers has not yet been universally adopted in cyberspace. Additionally, the Internet has evolved into the primary global communications systems and a significant facilitator of the world economy and the dependence on the Internet for communications, financial services, and the operation of much of the Nation's critical infrastructure has stimulated a greater awareness of IdM. This growing dependence has simultaneously highlighted the need for a more robust, comprehensive IdM framework to protect all participants of Internet and other telecommunications-based initiatives.

History of NSTAC Actions

In response to growing concerns about the need for improved authentication capabilities on telecommunications networks, the NSTAC has emphasized the importance of strong IdM during its Research and Development Exchange (RDX) Workshops and various reports, including the 1999 *NSTAC Report on the NS/EP Implications of Electronic Commerce* and the 2000 *Information Technology Progress Impact Task Force Report on Convergence*.

The NSTAC continued its work on identifying the scope of IdM in the 2003 *Trusted Access Report*. Following this study, during the 2003 NSTAC RDX Workshop, participants called for research and development work in emerging areas, including IdM and access control. During the September 2008 RDX Workshop, *Evolving National Security and Emergency Preparedness Communications in a Global Environment*, the NSTAC found that key technical and policy capabilities could improve IdM for NS/EP communications, including the development of a holistic IdM infrastructure, improved interoperability under a federated identity system, and the development of scalable and extendible technical architectures.

Recent NSTAC Activities

In November 2008, the NSTAC established the Identity Issues Task Force (IdITF) to explore the Federal Government's role in IdM and examine how the Government could best serve as a catalyst for broad implementation. As a result, in 2009 the NSTAC approved the *NSTAC Report to the President on Identity Management Strategy*, representing the first time the NSTAC has devoted an entire study to IdM with specific, presidential recommendations. Based on the research and analysis of the IdITF, the NSTAC recommended the President demonstrate national leadership on IdM to help influence public opinion and stand up an IdM office in the Executive Office of the President to develop and implement a comprehensive IdM vision and strategy.

For more information on the NSTAC, visit www.ncs.gov/nstac/nstac.htm or call (703) 235-5525.