Identity is the cornerstone for Cybersecurity

The security in any transaction comes from knowing exactly with whom one is doing business. Cyberspace is no different. Knowing the person on the other side of the network is who they claim to be is critical for our underlying economic and network security. Identity management offers the ability to know who specifically is authorized to access information and networks.

Both the report Securing Cyberspace for the 44th President issued by Center for Strategic and International Studies (CSIS) issued in December 2008 and the White House Cyberspace Policy Review released in May 2009 highlight identity as a key element in ensuring only those that are authorized can gain access to sensitive and secure networks.

CSIS - Securing Cyberspace for the 44th President

1. US should make strong authentication of identity, based on robust in-person proofing and thorough verification of devices, a mandatory requirement for critical cyber infrastructure
2. Anonymity is important but weak online identification is inappropriate in circumstances where all legitimate parties to a transaction desire robust authentication of identity.
3. Weak identification and authentication limit an organization's ability to enforce security policies to protect sensitive information and systems, and it hinders effective governmental and industry response to cyber attacks.
4. Implementing a digital credentials for transactions could reduce fraud while increasing security and privacy protection.

White House - Cyberspace Policy Review:

1. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interest, leveraging privacy enhancing technologies for the Nation.

2. Identity management also has the potential to enhance privacy through additional protection against the inappropriate release of personal identifiable information.
3. Increased use of on-line transactions involving financial, health and commerce require a basis for building trust between the parties to a transaction
4. The Federal Government should ensure resources are available for full federal implementation of HSPD-12.
5. The Federal Government should consider extending the availability of federal identity management systems to operators of critical infrastructure and to private sector emergency response and repair service providers for use during national emergencies.

It is with these findings and information in mind that the Secure ID Coalition agrees with Robert

Lentz, Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance, more needs to be done to protect identity and protect critical infrastructure networks. We support the **appointment of a Cyber Czar to address identity** as reducing anonymity is key to ensuring security and resiliency of the network. We also support a
date certain for full implementation of HSPD-12
for logical access to computer networks not only for all federal government employees and contractors but, also critical infrastructure personnel. Finally, we encourage the support of HSPD-12 as an underlying standard for State and Local governments to meet cybersecurity requirements under any grant or funding program.