Statement by the Security Industry Association before the U.S. House Subcommittee on Government Management, Organization, and Procurement

April 9, 2008

Chairman Towns, Congressman Bilbray, and members of the subcommittee. Thank you for the opportunity to testify before you about federal agency implementation of Homeland Security Presidential Directive 12 (HSPD-12).

My name is Rob Zivney. I am the vice president of marketing for Hirsch Electronics headquartered in Santa Ana, California. Hirsch Electronics is a manufacturer of physical access control systems for non-residential markets, including the federal government. I also serve as the Chair of the Security Industry Association's (SIA's) Personal Identity Verification (PIV) Working Group.

I am honored to testify today on behalf of SIA, which represents 400 manufacturers, integrators, and dealers of electronic security equipment. SIA members provide electronic systems solutions for physical security that protect your constituents and millions of Americans who access government facilities, ports, local schools, colleges, hospitals, airports, mass transit systems, retail establishments, and other institutions. Many systems have the ability to change operational modes in response to varying threat levels to ensure the security of these facilities and the people within.

As this subcommittee examines the findings of the General Accountability Office (GAO) Report released earlier today, I would like to emphasize that SIA members strongly support the goals of HSPD-12. We welcome this subcommittee's interest in implementation of HSPD-12. SIA members are fully committed to offering our assistance to ensure the successful implementation of this directive by all federal agencies.

Mr. Chairman, I would like to make several points that will contribute to this subcommittee's evaluation of HSPD-12 implementation. Simply put, security is only as strong as the weakest link. In our view, HSPD-12 - and the associated standards developed by the National Institute of Standards and Technology (NIST), specifically the identity vetting processes - forms a far stronger foundation for our federal government agencies' security than we have ever witnessed in the past. Identity verification in routine access transactions are enhanced by the use of the credential bearer's fingerprints template, which are taken from the same fingerprints submitted for and cleared in the background check during the issuance process.

SIA believes the PIV II technical requirements for the implementation of HSPD-12 require an investment both financially and in the development of new infrastructure. However, the scope of the investment and time required for implementation were underestimated by the government when it set goals for the deployment of HSPD-12 through Office of Management and Budget (OMB) Memorandum M-05-24. Traditionally the functions of authentication and authorization have resided locally with

the administrator of the physical access control system (PACS). The HSPD-12 and Federal Information Processing Standard (FIPS) 201 model have changed this: the credential issuer to a large degree now handles authentication while authorization remains a function of the PACS. This has created a unique challenge facing federal agencies, the development of a substantial shared infrastructure to accommodate the increased functionality and security features of the PIV II credential. For many agencies, the development of this new infrastructure presents a significant learning curve that they are working diligently to overcome.

Mr. Chairman, the implementation of HSPD-12 is truly a pioneering effort on behalf of the federal government. It requires that the human resources, information technology, and security departments interface and cooperate on an unprecedented level. These three disciplines traditionally are different in cultures and basic objectives. This creates challenges for all parties involved in implementing HSPD-12.

Although HSPD-12 may not draw the attention of our nation's major media outlets, the world is watching. HSPD-12 is truly transformational. The issuance of OMB Memorandum M-05-24 was a bold move. In spite of the technical and procedural challenges, the subcommittee should note that there has been enough early success to attract scrutiny of HSPD-12 by other nations, state and local governments and other industry sectors.

Mr. Chairman, some may question the value of the PIV II credential because of the significant cost differential compared to traditional security technologies and the additional integration efforts required. How ever, the use of an identity credential coupled with the use of fingerprints for authentication of the bearer and the use of digital certificates and Public Key Infrastructure (PKI), promises to revolutionize government, significantly increase security, and conserve taxpayer dollars.

The methods and technologies needed to utilize the capabilities of the PIV II credential in a logical or physical access control system are still being discovered and developed. In the absence of clear guidance and specifications for the systems that will use the PIV card, some manufacturers have stepped up to the challenge and absorbed substantial research and development costs to produce next generation equipment capable of utilizing the features of a PIV II credential. These costs have been significant and made progress difficult as this work has been conducted without the benefit of having operational PIV II credentials available to manufacturers to develop and test associated products.

Mr. Chairman, given this subcommittee's oversight responsibility over the General Services Administration (GSA), you will be interested to know that this situation is exacerbated by the fact that the GSA has had to design a specification for the credential readers, and is testing to that specification, a role it has never undertaken in the past. As a result, the GSA Approved Product List (APL) testing program had to be created from scratch. The test specifications had to be inferred from the NIST specifications that were silent on the logical and physical access control systems that would actually use the

cards and card production apparatus. This made for a very lengthy process, which was challenging for both GSA and the manufacturers submitting equipment for evaluation. There is also a catch 22; only federal employees and contractors are authorized to possess PIV cards. However, manufacturers need PIV cards to develop products that will use the cards. Operational card stock for R&D and testing remains a key priority for the electronic security industry, due to the many options and variations allowed for in the NIST specifications.

GSA's current implementation of the approved products restricts these items to procurement from GSA Schedule 70, the Information Technology Schedule. However, the majority of the physical access control system components are assigned to Schedule 84, where they have always been. This makes it difficult both for the manufacturers submitting products and the government purchasers attempting to assemble systems from multiple GSA schedules. The decision to place the new PIV components "exclusively" on Schedule 70 was mandated by OMB. We believe this subcommittee should encourage the dual listing of approved HSPD-12 products on both Schedule 70 and Schedule 84 to serve both the IT security and physical security needs of agencies.

Despite challenges, SIA finds there are some agencies doing an exemplary job of provisioning credentials for their employees and upgrading their infrastructure to meet the requirements of HSPD-12. For those agencies that continue to work to improve their implementation of HSPD-12, SIA has formed a Government Infrastructure Security End User Group to assist in this process.

This SIA group serves as a bridge between industry and government and it is a conduit for information between these two entities. Over the past several months SIA has conducted non-product-specific training for federal employees to try to shorten the learning curve that agency security personnel are experiencing. These interactive sessions provide our industry with a means to learn about the needs of federal agencies. This helps our members develop products that meet those needs. I am pleased to say that this training is provided by SIA at no cost to federal employees. It is intended to help develop a federal security workforce that is better informed about physical security technologies so that the goal of maximizing tax dollars to provide security for government facilities is met.

Mr. Chairman, as part of SIA's efforts to advance HSPD-12 implementation, we have proactively engaged NIST in extensive conversations related to FIPS-201 and its supporting Special Publications. SIA's PIV Working Group also serves as a mechanism to quickly address government technical needs or questions related to physical security infrastructure. SIA also is an active participant in the Government Smart Card Interagency Advisory Board (IAB) and we take every opportunity to help government understand the ramifications of HSPD-12 on currently deployed security and life safety technologies as well as future technologies. We regularly and consistently provide comments on new and revised draft NIST publications that are posted for public review. In addition, we sponsor workshops and briefing sessions for industry, often with the

participation of GSA, NIST, and other agencies involved with the development and implementation of the standards.

In conclusion, SIA would like to offer additional recommendations for the subcommittee's consideration that may expedite full implementation of HSPD-12:

First, we would encourage this subcommittee to direct OMB to establish a dedicated team of professionals within its Office of E-Government and Information Technology. These employees have substantial knowledge of physical security technologies and physical security infrastructure within federal agencies.

This proposed OMB "physical security team" should regularly coordinate with the private sector toward implementation of HSPD-12 and the development of future Executive Branch policies and directives that may impact physical security at government facilities. As part of its responsibilities, this physical security team of experts would support the ongoing efforts of the Interagency Security Committee (ISC) that is charged with developing physical security policies, standards, and strategies at non-military government facilities. Established in 1995 under Executive Order 12977, the ISC is chaired by the Department of Homeland Security and comprised of senior level officials from federal government agencies.

Secondly, we recommend that OMB establish a policy for implementation of physical security similar to the policy document M-05-24. We have progressed to date with an "unfunded mandate" for PIV-I and PIV-II. However, physical access control systems are outside of that scope, and as such have neither funding nor a mandate. This requested policy must recognize that the PIV card is not compatible with most installed PACS currently in use and that the PACS will have to be, at a minimum, upgraded or, most likely, need to be replaced.

Finally, we encourage you to consider SIA as a resource for the effective utilization of the PIV credential with physical access control systems. We not only have the skills and knowledge for deployment and use, but are also an ANSI standards development organization (SDO). As such we are able to produce standards for physical security systems and indeed have many such applicable standards in development now.

Thank you for the opportunity to testify before you and the subcommittee. I applaud your interest in this important initiative and look forward to answering your questions.