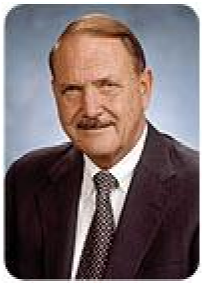
SECURITY
SOLUTIONS FOR ENTERPRISE SECURITY LEADERS

The Politics of Deadlines

by Clarissa Jacobson
November 21, 2006

A telephone survey by Security Magazine of chief security officers at enterprise-level companies discovered confusion and lack of knowledge or the Homeland Security Presidential Directive 12 (HSPD-12). A New York City CSO, working for a major financial firm, told Security Magazine's researcher, "I still don't see agreement on much of the plan." The goal of the mandate is to enhance security and increase government efficiency by reducing identity fraud.

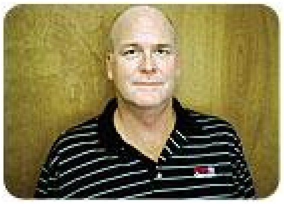
Ambitious and difficult, compliance is no easy feat. Unlike other types of security technology introduced to government chief security officers and their business brothers and sisters, this time security manufacturers will have to start the ball rolling.



The HSPD-12 is now in their court. “Not knowing what actually is required makes it difficult to develop products,” points out Larry Midland of Hirsch.

HSPD-12 spells out big money for the companies that supply the services and products that organizations and their security executives will be forced to implement, but a final deadline may be unrealistic. Is it possible? Is the technology there? What is expected and needed to make it a reality? Four top industry experts were asked these questions to get their opinions on the impact HSPD-12 is having on the industry and how they’re responding.

IDENTIFICATION AUTHENTICATION



Says Keith Wilson of Smartnet, “I think the embedded culture and resistance to change which is encountered in many agencies is the most significant hurdle which needs to be overcome for successful implementation.”

The first issue facing the successful implementation of HSPD-12 is the determination of the criteria necessary to authenticate an employee’s identity. The Federal Information Processing Standards publication (FIPS 201-1) lays out a thorough process for applicant verification. Traditional methods of identity validation include a Driver’s License, a passport, Social Security card, and a birth certificate. However, with the HSPD-12 directive, the process becomes much more difficult. The smart card (an ID card implanted with computer chips or radio frequency identification “RFID”) must carry two fingerprints, a photo, personal data and a Public Key Infrastructure (PKI) certificate.
Larry Midland, president and CEO of Hirsch Electronics, explains the hurdle that organizations are now facing, and said “the concept of “verifying identity” now means that a government employee or contractor, must go through a formal process of collecting personal identifying data, followed by a background check prior to being issued a credential.” FIPS 201-1 is broken down into two processes: Personal Identity Verification (PIV) I and II. Keith Wilson at IT firm Smartnet points out that PIV II requires fingerprints and facial biometrics to be captured during the identity proofing and registration and re-verified during the issue of the card.

Midland believes that once the federal, state and local governments accept the approach, then it will become more of a standard. Midland says, “Corporate IT departments are already using PKI to enable a single card to gain access to the computer network as well as doors in buildings throughout the enterprise.”

The standards outlined by FIPS 201-1 are only useful if the cards themselves are designed to prevent fraud and tampering. Erik Larsen of Lenel Systems International lists visual safeguards, such as micro printing, guilloche printing (spirograph-like curves) and holograms as some of the techniques currently used.

Kirk Brafford at government-centric MAXIMUS feels that the best fraud and tampering safeguard is the verification of the PIV through reading the contact integrated circuit chip on the card. This requires a computer-based program, middleware, a card reader and the cardholder’s PIN entered by the person using the card. In addition to incorporating these security features, PIV II further requires that all smart cards work in conjunction with biometrics.

Accreditation is just beginning. All suppliers have to go through an accreditation process before the awarding of contracts. Larsen says it does not matter who does it, whether it’s the National Institute of Standards & Technology (NIST) or the General Services Administration (GSA), but the process is firmly defined and that manufacturers and suppliers must submit for accreditation. Brafford goes further to say that it should be mandatory that a laboratory run by an accredited government testing organization that test and certify suppliers’ hardware be FIPS 201-1 certified.

Compliance with the standards set up by FIPS 201 is step one in being accredited. The GSA has established an Approved Product List and testing procedures to confirm compliance with the significant aspects of the NIST standards. A consumer will be able to check the GSA website to see if products and services are listed as having passed compliance requirements. Wilson adds that the Federal Acquisitions (FAR) and Defense Federal Acquisition Regulations (DFAR) clauses govern the awarding of contracts and once the product(s) is certified, then normal competition for contracts will occur.

IMPLEMENTATION DIFFICULTIES

Additional difficulties exist in the implementation of HSPD-12. According to Midland, one of the main challenges is that there have been so many specifications published that the target is always moving. “Not knowing what actually is required makes it difficult to develop products.” He also states that government customers previously put projects on hold until they were assured of compliance, which adversely affected a number of companies.

Wilson said it comes down to budget. “Most agencies mandated by OMB [Office of Management and Budget] don’t have the budgets to implement these systems and no money is planned.” Furthermore, many government agencies are waiting for an OMB decision on the centralized PIV Card issuance plan and the related costs for using this Shared Issuance Provider (SIP). Brafford explains, “This delay of an SIP plan or the approval for federal agencies to go forward on their own has slowed the process for many hardware vendors to commit resources for an unknown business case model.”

For Larsen, the problem comes down to having several pieces from different vendors working together. “There are a lot of companies offering one piece of the solution and leaving the integration up to the integrator or the end-user.” Larsen sees value in a complete solution. It should also meet the requirements of NIST, FIPS 201 and, according to Larsen, “address the real world struggles of getting a new PIV credential to an applicant using a secure process.”

SO, IS IT POSSIBLE?

Though the road to HSPD-12 compliance is rocky, everyone interviewed agreed that the technology exists today to execute the directive. However, interfaces between components still need development as well as finalization of specifications. Wilson cites the example of PIV II fingerprint requirements; it was not confirmed until a month or so ago. That leaves little time for manufacturers to finalize design and integrate the solution prior to the HSPD-12 mandate.

Clarissa Jacobson
Clarissa Jacobson is with Peter A. Sokoloff & Co., an investment-banking firm that specializes in mergers and acquisitions of companies in the security industry. Visit them at www.sokoloffco.com*. Email the author at cjacobson@sokoloffco.com.*

Source: www.securitymagazine.com