



October 2006

Delays & in-fighting mar HSPD-12 implementation: October 27th deadline looms

By JACOB GOODWIN

Ron Martin, a top official at the U.S. Commerce Department involved with the government-wide implementation of HSPD-12 personal identification programs, has a PowerPoint slide he likes to present at briefings which shows a futuristic warrior clad in menacing black armor issuing a stern warning: "Resistance is Futile!"

Audiences chuckle nervously when they see Martin's illustration because they realize that despite the resistance of large swaths of the federal bureaucracy, and despite discontent among portions of the security industry, the push to issue interoperable smart cards to all government employees and all government contractors has begun to build an unstoppable momentum.

Many people refer to this huge undertaking by the name of the White House document issued in August 2004, known as Homeland Security Presidential Directive-12, or HSPD-12, which has provided its bureaucratic underpinning. Others refer to the same initiative by the name of the standards document, FIPS-201, which was issued by the National Institute of Standards and Technology (NIST) in February 2005 to help carry out the mandate of HSPD-12.

As the program approaches an important deadline on October 27, government officials, potential vendors and other observers are asking whether the complicated effort is on schedule and whether the



government's procurement strategy is fair and logical.

The answer to the first question – have federal agencies met their announced deadlines? – depends on your definition of the word compliance. (Recall Bill Clinton's tortured testimony in 1998, "It depends on what the meaning of the word 'is' is.")

The General Services Administration (GSA) which has been handed overall responsibility for administering HSPD-12 implementation by the Office of Management and Budget (OMB), which issued a

schedule on August 5, 2005 that declared that each federal agency must “begin compliance with FIPS-201” by October 27, 2006. Elsewhere, the document says, “By October 27, 2006, all departments and agencies must begin deploying products and operational systems meeting these requirements...”

Precisely what that phrase “begin deploying products” means has been subject to interpretation. Does it mean that all federal departments and agencies must issue fully-operational cards to all of their employees and contractor personnel by Oct. 27 and that all of the card readers, biometric devices and associated infrastructure and software must be in place to actually use the cards? Apparently not.

Because such a tight definition would be virtually unachievable, the GSA has backed off in recent weeks and embraced a far looser definition of compliance.

Currently, a federal department or agency will be deemed to have met the imposed deadline if it issues at least one smart card that contains the required biometric data – even if the organization has not installed the equipment necessary to actually read the card. Alternatively, a department or agency can meet the Oct. 27 deadline simply by signing a contract with a commercial vendor, known as a “shared-services provider,” which agrees to handle the HSPD-12 implementation in the future, but has not yet issued any smart cards.

In other words, the government has relaxed its definition of compliance in order to make it easier for government organizations to comply.

Observers have reacted to this program slippage in two ways. Most executives working for security industry suppliers hoping to participate in HSPD-12 projects have been patient and understanding. They recognize that a massive undertaking that entails the development of brand-new technologies, revised business procedures and the interaction of dozens of separate identification devices, will take a long time to perfect.

“The task at hand is a very complicated task, and the government is moving in the right direction,” said Tony Damalas, a vice president of technology for Actcom Security Solutions, of Virginia Beach, VA. “If an agency misses its deadline by only 90 days, I say ‘God bless you’,” he added.

Not everyone is as forgiving. Another industry executive involved in HSPD-12 implementations, who requested anonymity, complained, “As a U.S. citizen, I would have hoped for a more stringent directive.”

Some agencies plan to “comply” by issuing one smart card, which contains the required personal data, photo, fingerprint and second biometric, even if they have made little headway in installing the readers, databases and management software necessary to actually use the cards.

Other agencies will comply by signing up with BearingPoint, Inc., of McLean, VA, which has been designated by GSA as a “shared-services provider,” to whom they can largely outsource their HSPD-12 responsibilities.

The flexible definition of compliance with the Oct. 27 deadline has stirred some minor controversy, but that has been overshadowed by the debate kicked up by the GSA’s procurement strategy.

GSA has determined that government agencies that wish to buy smart cards and access control card readers – key ingredients in any HSPD-12 compliant system – must do some from companies that have negotiated contracts with GSA under what is known as Schedule 70, which covers IT products, rather than Schedule 84, which covers the more traditional physical security products and includes a larger number of security vendors.

The decision represents an unmistakable tilt toward the larger systems integrators – such as Lockheed Martin, BAE, General Dynamics and GE Security – which are accustomed to complex computer- and network-oriented IT solutions, and away from the traditional security firms – such as The Stanley Works

and ADT Security – which are more accustomed to installing physical security systems such as access card readers, electronic door alarms, video surveillance systems and motion detectors.

Some observers consider this tilt to be appropriate and inevitable, as the IT aspects of modern security systems become more predominant. In fact, many of the companies that hope to win large chunks of HSPD-12 work have already completed negotiations with GSA to be included under Schedule 70.

“It became obvious that if you were going to go after security work, you had to get on Schedule 70,” said Ray Lorenzo, a consultant to Actcom, which was recently acquired by Diebold Inc., of North Canton, OH. “That trend has been going on for two or three years.”

Other security companies have complained that GSA placed its HSPD-12 buying responsibility with the office that manages Schedule 70, in part, due to pressure applied by some of the largest integrators and, in part, because the Schedule 70 office has seen its revenues decline in recent years. (GSA offices are paid fees for the procurement projects they handle on behalf of the buying agencies.)

Michael Mostow, government programs director of The Stanley Works, of New Britain, CT, said GSA’s decision was unwise because it fails to recognize the indispensable role that traditional access control suppliers will play in HSPD-12 implementations. He said GSA had tilted unfairly toward large systems integrators, who will reap their usual 15 percent management fee, but inevitably turn to the traditional vendors anyway to implement these HSPD-12 programs.

“They’re not adding any value,” said Mostow, of the largest integrators, who he sees as having won this latest battle in the HSPD-12 procurement war.

In order to get back into the HSPD-12 game, traditional physical security suppliers must now sign GSA Schedule 70 contracts, a lengthy procedure which might be sped up somewhat by GSA’s pledge to “streamline” the process, but which might still take some vendors about one year to compete.

Stanley Works and other companies in the Security Industry Association (SIA) have raised this complaint with staff members working for Speaker of the House J. Dennis Hastert (R-IL) and chairman of the Senate Homeland Security and Governmental Affairs Committee Susan Collins (R-ME).

“We’re simply asking for the right to compete for work we’re regularly engaged in,” said Mostow, who acknowledged that as yet his group has not found much satisfaction on Capitol Hill.

George Martinez, who manages HSPD-12 programs for GE security, does not see it that way. Martinez believes that IT is becoming more and more central to most security systems, especially HSPD-12-type systems, and that GSA made the appropriate choice for these projects.

“It’s definitely closer to an IT product,” said Martinez. “The GSA will have access to a larger number of suppliers” under Schedule 70.

Robert Zivney, vice president of marketing for Hirsch Electronics, a longtime supplier of access control systems which is now offering end-to-end HSPD-12 compliant systems, believes there is a little bit of truth to both positions. “A lot of people who are fighting it [the shift from Schedule 84 to Schedule 70], are fighting change,” said Zivney. “Success will come when GSA hits a balance between IT and physical.”

Zivney thinks some of the traditional access control suppliers are also upset that one of the unique contractual benefits they enjoyed while selling products under Schedule 84 will no longer be available to them under Schedule 70. In the past, when a company bid a job under Schedule 84, they had to supply firm pricing for the materials they would be installing, but not for the actual labor involved, Zivney explained. Consequently, some of these companies earned very handsome profit margins on their labor costs. That special advantage will not be available to vendors selling products and systems under Schedule 70, Zivney concluded.

Even if the access control world is more heavily emphasizing IT systems these days, some observers believe that GSA must pay careful attention to the specialized knowledge that still resides with the physical security community. “Yes, things are moving toward IT, but GSA hasn’t taken into account the views of the physical security companies,” said Zivney.

For its part, Hirsch is trying not to make any enemies. “We don’t want to just fight it,” said Zivney. “We want to identify problems and eliminate problems.”

Faced with the insurmountable task of meeting the Oct. 27 deadline – as well as the difficulty of implementing an HSPD-12 compliant system under any timetable – GSA has developed the concept of shared-services providers.

In one of the bolder moves in this competitive arena, two huge systems integrators, Lockheed Martin and General Dynamics (though they weren’t designated as GSA’s “official” shared-services provider), have joined forces to offer a similar form of managed services to government agencies that might be eager to implement HSPD-12 smart card programs for their employees and contractors. Lockheed Martin and General Dynamics plan to offer government agencies the ability to perform enrollment checks, issue smart cards and maintain the database without having to invest in their own HSPD-12 compliant systems. Lockheed Martin and General Dynamics will handle everything, from soup-to-nuts, for a flat fee per card, requiring no upfront investment by the customer agency.

Lockheed has decided to invest its money in the infrastructure necessary to extend such an offer because it sees a large opportunity beyond the federal government for interoperable smart cards and integrated identity verification systems. Beginning with its own 135,000 employees, Lockheed plans to offer this outsourced capability to state and local governments in the U.S. and to large global enterprises throughout the world.