Monitoring Report – January, 2007

J. Markowitz, Consultants

Program B: Legislative and Regulatory Activities

This report is confidential and intended for registered JMC clients only

Legislation

US Federal

US House of Representatives Amends SAFETY Act to streamline technology procurement

On January, 23rd, the US House passed an amendment to the SAFETY Act for homeland security and anti-terrorism that requires formal criteria and co-ordination within the Department of Homeland Security (DHS).

POTENTIAL IMPACT: It is unclear what the impact of this will be because it may be changed or dropped in the Senate. It is good for technology and, hopefully, good for biometrics because it requires that DHS hire security professionals to evaluate technology and hiring.

DETAILS: Since it is not extremely long, the full text of the amendment (HR 599) is given below. Note that the SAFETY Act charges DHS with the job of evaluating anti-terrorism and national-security technologies.

> Section 1 (a) Personnel- The Secretary of Homeland Security shall ensure that, in addition to any personnel engaged in technical evaluations that may be appropriate, a sufficient number of full-time equivalent personnel, who are properly trained and qualified to apply legal, economic, and risk analyses, are involved in the review and prioritization of anti-terrorism technologies for the purpose of determining whether such technologies may be designated by the Secretary as qualified anti-terrorism technologies under section 862(b) of the SAFETY Act (6 U.S.C. 441(b)) or certified by the Secretary under section 863(d) of such Act (6 U.S.C. 442(d)).
>
> (b) Coordination Within DHS. The DHS Secretary shall
>
> > (1) establish a formal coordination process that includes the official of the Department of Homeland Security with primary responsibility for the implementation of the SAFETY Act, the Chief Procurement Officer of the Department, the Under Secretary for Science and Technology, the Under Secretary for Policy, and the Department of Homeland Security General Counsel to ensure the maximum application of the litigation and risk management provisions of the SAFETY Act to anti-terrorism technologies procured by the Department; and
> >
> > (2) promote awareness and utilization of the litigation and risk management provisions of the SAFETY Act in the procurement of anti-terrorism technologies.
>
> (c) Issuance of Departmental Directive- The Secretary of Homeland Security shall, in accordance with the final rule implementing the SAFETY Act, issue a Departmental management directive providing for coordination between Department procurement officials and any other Department official responsible for implementing the SAFETY Act in advance of any Department procurement of an anti-terrorism technology, as required under subsection (b).

US Privacy and Civil Liberties Oversight Board Reviews Convenes First Meeting

The Privacy and Civil Liberties Oversight Board held its first public hearing the other day on the National Security Agency's (NSA) eavesdropping program.

POTENTIAL IMPACT: This is a program that was created by a Republican Congress and White House and placed under the control of the Republican administration. It has little funding, no real support from the administration, no subpoena power, and any of its requests for documents can be vetoed by the US Attorney General. Thus, it would seem as if it should be of little interest to SIV or biometrics.

It should not be forgotten, however, that this Board was created in response to public and media outcries related to invasion privacy and violation of civil liberties following revelations related to the National Security Agency's eavesdropping program. If the Board fails to discharge the responsibilities the new Democratic Congress could very well establish an oversight body that could take a hard line on civil liberties and privacy. In fact, a bipartisan bill to remake the board as an independent entity with subpoena power and a credible claim to oversight has already been introduced by Representatives Carolyn Maloney (Democrat, New York), and Christopher Shays (Republican, Connecticut)

While protection of privacy and civil liberties is a good thing, we cannot forget that the US has no up-to-date data privacy regulation that covers new technologies such as biometrics and that defines privacy and civil-liberty requirements related to uses of technologies like biometrics. The lack of such regulatory or legislative guidance could easily lead to inappropriate restrictions on and investigations of biometric deployments. Biometrics is one of the easy targets related to fears (warranted and not) of privacy and civil liberties violations. For example, a time-and-attendance deployment of hand geometry for New York City employees has spawned protests from employee unions and the employees themselves who consider the use of biometrics an invasion of privacy and fears about layoffs (see Program C: Report on Government Projects January, 2007). .

DETAILS: The Privacy and Civil Liberties Oversight Board was created two years ago in response to the recommendation by the September 11 Commission to create an independent oversight agency. The Board consists of four Republicans and one Democrat. This first meeting of the Board reviewed the issue of warrantless eavesdropping by the NSA that is supposed to lead to a report the Board is scheduled to submit to Congress in March.

The discussion did consider the NSA program but more attention was devoted to agreeing that the Board should not adopt an aggressive stance with regard to the White House and programs supported by the White House.

Tighter Passport Rules for U.S. Citizens

This month, regulations went into effect that require US citizens returning home by air and all citizens of the Western Hemisphere to carry passports.

POTENTIAL IMPACT: This regulation is part of the US anti-terrorism initiative. Anticipation of that change caused a rush in requests for US passports because previously it was sufficient for US citizens to display a birth certificate or similar official document. Last year, the US issued a record 12.1 million passports. Local passport offices in the US and Canada also reported long lines just before the ruling went into effect.

Canada and several Caribbean countries have expressed their dissatisfaction but it is unlikely that the US will revert to the earlier policy because the main purpose of the change is to reduce fraud even though it is costing the US tourist income. Until this ruling went into effect immigration official needed to know how to validate a plethora of documents. There are more than 8000 styles of birth certificates, alone. In contrast, most US passports can be read by digital

equipment. This could mean that another result of the law would be faster-moving customs and immigration lines.

DETAILS These changes are mandated by a law passed by Congress in 2004 in response to recommendations by the September 11 Commission. Starting January 23, 2007 anyone traveling to the US from any other country, including US citizens returning from Canada or Mexico, must display a valid passport to immigration authorities. The current change applies only to US citizens returning by air but it will be extended to land and sea travel in 2008. Customs will also accept merchant marine cards and Nexus air cards, which are issued to citizens and legal immigrants in the United States and Canada who are frequent travelers and have passed a background check. Active duty military personnel are exempt.

DHS officials said 94% of US citizens returning to the US in early January had already provided documents meeting the new requirements.

US-State and Local

Maine's Legislature rejects federal requirements for Real ID Program

Both legislative houses in the state of Maine voted to "refuse" to force its citizens to use driver's licenses that comply with the digital ID standards established under the Real ID Act in 2005.

POTENTIAL IMPACT: This vote comes as no surprise and has less to do with states rights than fiscal problems even though it asks Congress to repeal the Real ID law. Nevertheless, the vote does represent a setback for the Federal Department of Homeland Security and Republicans who have touted Read ID as an important tool in the war on terrorism. The vote makes Maine the first state to formally reject this potentially-costly, but unfunded, Federal mandate at a time when other costs (e.g., Medicare, Federally-mandated educational testing) are skyrocketing, reduced Federal monies, and a shrinking tax base related to tax cuts at all levels.

Other states are likely to follow suit. Some, including Massachusetts, Georgia, and Washington, are already considering similar measures. This month, the Montana legislature held a hearing on a bill that says "The state of Montana will not participate in the implementation of the Real ID Act of 2005" and directs the state motor vehicle department "not to implement the provisions."

DETAILS: Both chambers of the Maine legislature approved a resolution that flatly refuses to force its citizens to use driver's licenses that comply with digital ID standards established by the Real ID Act of 2005. It was approved by a 34-to-0 vote in the state Senate and by a 137-to-4 vote in the House of Representatives. The resolution further asks Congress to repeal the Act.

The majority leader of Maine's House of Representatives stated that the Real ID Act would have cost Maine $185 million over five years and required every state resident to visit the motor vehicle agency so that several forms of identification (including an original copy of the birth certificate and a Social Security card) could be uploaded into a Federal database.

The Real ID Act requires all Americans to have a Federally-approved ID card in order to receive benefits from Federal programs, such as Social Security, travel by airplane, or engage in common activities, such as opening a bank account. That ID must be machine readable. Each state must conduct validation checks of its citizens' identification papers which makes driver's licenses the most likely candidates for Real ID identity documents. The provisions of the Real ID Act go into effect in May of 2008 but the DHS has yet to issue final requirements for the machine-readable portion of the ID but it is likely to include biometrics.

Regulation

US Federal

US Requires Places Restrictions on Nokia-Siemens Telecom Deal

The US government conducted a national security review of the proposed $21bn joint venture between Nokia and Siemens, and forced them to sign a "mitigations agreement" that imposed restrictions on the new joint company.

POTENTIAL IMPACT: Normally, CFIUS is charged with evaluating national-security risks tied to foreign takeover of US assets. This move to restrict the joint venture between Nokia and Siemens – both European telecom equipment makers– extends the reach of the committee to include foreign companies involved in creating sensitive infrastructure components. Even before this move against the Nokia-Siemens venture CFIUS's activities with regard to vetting foreign takeovers had produced friction with the US Treasury Department whose goal includes encouraging foreign investment.

Many view this increased sensitivity as a result of the firestorm that occurred over the plan to sell US port management operations to a Dubai-based company. In fact, Congress is considering legislation to further restrict the ability of non-US companies to buy or build what it considers to be critical US infrastructure. Consequently, the restrictions are not unlike those the U.S. government imposed on the merger of Alcatel and US-based Lucent because Lucent operates Bell Labs which does highly sensitive work is being done for the U.S. intelligence community – including SIV and other biometrics. In fact, all Federal agencies involved in the national security review process have increased scrutiny of companies that manufacture components for mobile and fixed-line networks globally

The Nokia-Siemens joint venture does not specifically involvement biometrics but biometrics falls within the scope of sensitive technologies and is seen as important to national security. This includes SIV which is used for surveillance by intelligence agencies and for other Federal programs.

DETAILS: The interagency Committee on Foreign Investment in the United States (CFIUS) investigates foreign takeovers of US assets for possible security threats. It imposed security requirements on the new venture between Nokia and Siemens, including procedures that dictated whether foreigners could work on US equipment and software. The Nokia-Siemens joint venture will create the third largest supplier of equipment to telecom companies (after Alcatel-Lucent and Ericsson). The security requirements include procedures that dictate whether foreigners may work on U.S. equipment and software. This prompted the national security review by U.S. authorities of the proposed $21 billion joint venture agreement between Nokia and Siemens. The findings of the review led CFIUS to require the joint venture to sign an agreement that imposes considerable restrictions on the new company.

US Transportation Workers Identity Card (TWIC) Card Fees Higher Than Expected

The US Department of Homeland Security released a final rule for the price of TWIC cards. Most maritime workers in the United States will pay $139 or more for an initial TWIC card and $60 for a replacement card. These prices are higher than was expected. The Transportation Security Administration has invited public comments on some of the fees

POTENTIAL IMPACT: These increases are likely to spawn further resistance to TWIC. States such as Florida which have their own ID cards and their own requirements tied to those cards had already expressed dissatisfaction with what they consider to be duplication of credentials. Segments of transportation industry have objected to the cost of paying for duplicate cards and undergoing multiple certifications.

DETAILS: The 469-page final rule applies to implementation of the TWIC biometric identification cards in the maritime sector. It makes a number of changes in fees, compliance dates, definitions of what and who is covered under the rule and other parts of the program. It also extends the compliance dates slightly by adding two more months.
Workers who have complied with specified TWIC requirements through other programs will pay reduced fees (from $107 to $127) but most will pay the new, higher fees. The new price for initial credentials is $10 higher and the price of the replacement card rose from $36 to $60, a 65% increase from the initial proposed rulemaking issued in May, 2006. The fees were raised to offset the increased cost of the identification management system (an increase of 135% over 5 years, or $44 million) and to cover the cost of card production (an increase of 39% to $28 million). The only factor that has decreased in cost is the threat assessment.

Eventually, millions of port, airline, trucking and transport workers will be issued a TWIC credential after being scrutinized to determine whether they pose potential threats to US national security (called a "threat assessment"). Once they are issued the TWIC card they must display it before being allowed to enter secure areas.

GAO Report Recommends Changes to Improve Rail Safety

This report is based on testimony the Government Accountability Office done in 2005 (GAO-05-851) combined with a recently-completed risk assessment of US passenger rail systems.

POTENTIAL IMPACT: The assessment was initiated following London's subway bombings and railway attacks in Mumbai, India and is intended to provide the DHS's TSA with information and guidance following its own assessment of US railway passenger systems. The GAO was also responding to complaints by the rail industry and others that the security procedures that TSA implemented in 2006 were not based on best practices. This report appears to be nudging the TSA to complete its new risk assessment quickly and to develop a better security framework using the information in this report and the GAO's earlier report.

calls for a rapid completion changes in TSA's to complete its risk assessment soon and to quickly establish a security framework based on best-practices.

DETAILS: The DHS Office of Grants and Training conducted risk assessments of passenger rail systems to identify and protect rail assets that are vulnerable to attack, such as stations and bridges. This report provides information on

1, how DHS assessed the risks posed by terrorism to the US passenger rail system
2 actions that TSA and other federal agencies have taken to enhance the security of U.S. rail systems (which do not appear to be based on industry best-practices) and
3. rail-security practices implemented by domestic and selected foreign passenger rail operators.

There is no mention of biometrics or any other specific kind of security in the report.

US State and Local

New York state's Governor Cancels Medicaid Fingerprint Program

New York's Governor Spitzer terminated an anti-fraud program based on fingerprints from Medicaid recipients in New York City.

POTENTIAL IMPACT: There is a great deal of fraud in Medicaid programs and many state and local governments have implemented biometrics as a way to control it. Spitzer's move is reportedly consistent with his opposition to a US Congressional law requiring Medicaid recipients to provide proof of citizenship. Spitzer's move has already caused ripples within New York because the state's attorney general Andrew Cuomo is a strong and vocal supporter of this anti-fraud measure (see details).

DETAILS: Former New York Governor Pataki implemented the fingerprint program as a way to control Medicaid fraud in New York City. In 2006, the New York State Health Department had begun putting the program in place. Current Governor Elliott Spitzer stopped the program but little more about his actions was reported. In response, Attorney General Andrew Cuomo's point man on attacking Medicaid fraud made a firm statement in support of using fingerprinted to deter Medicaid fraud: "I think if someone is getting public money, it's perfectly appropriate to have them fingerprinted," Brooklyn DA Joe Hynes (The Post).

Global

Fewer Regulatory Issues Favor the Emergence of the Asia Pacific Biometrics Market

Frost & Sullivan released a report showing that lack of regulation in Asia is supporting the growth of biometric usage in Asia.

POTENTIAL IMPACT: Despite the title of the announcements for this report, the lack of regulation is only one of the things that are driving biometric deployments in Asia – as elsewhere. Most of them are things we have discussed in our monitoring reports. Concern about security and terrorism is high globally and those concerns are promoting the use of biometrics. Our monitoring reports have clearly shown that the deadlines for implementing biometric passports and the growth of identity theft are also driving use of biometrics in government and private sector. Frost & Sullivan's findings also support our observations that most of the funding is going for fingerprint and face recognition. Frost & Sullivan see voice as having strong future growth resulting from acceptance of fingerprint and face. Our view is that the FFIEC guidance and other regulations are driving voice deployments in North America and Europe and that the market for voice is already expanding. .

DETAILS: The report, titled *Asia Pacific Biometrics Market - Investment Analysis and Growth Opportunities* benchmarks the biometrics industry and discusses market estimates until 2008. Biometrics is only one segment of the report. In that segment, Frost & Sullivan report that in the wake of increasing security concerns, biometrics is gaining tremendous importance as a means of identifying individuals, particularly in the government vertical. Governments in Asia Pacific have allocated around $100 million for facial recognition biometrics and another $120 million for fingerprinting biometrics. Governments' projects are predominantly pilot studies and evaluations as against large scale deployments and the allocations for biometric projects are expected to increase significantly during 2006-2008, when the technologies stabilize. Automated fingerprint identification system (AFIS) and non-AFIS were the largest revenue generators, accounting for market shares of 40.4 percent and 35.9 percent respectively in 2005. Segments such as voice verification and signature verification are likely to record impressive growth and being in the early growth stage, voice verification promise to be a lucrative segment for investors. Additionally, the facial recognition segment experienced strong uptake between 2003 and 2005 and the largest current demand for facial recognition biometrics is in Australia, Singapore, and Thailand. In future, China and India are expected to be the most promising markets for face recognition biometrics between 2006 and 2008.

The primary reason why biometrics volume expectations are very high in the Asia Pacific market is that the technologies are targeted more toward the mass-consumer market than large-scale government applications. This trend, though expected to continue for some time, is likely to change over the next 2-3 years because of the greater number of projects being undertaken by the various Asia Pacific governments. With respect to investment opportunities, multimodal biometrics, which is expected to see a growth rate of over 52 percent during the 2005-2010 period, promises better returns on investments for venture capitalists (VCs) than conventional single technologies. We do agree with Frost & Sullivan, however, that growth for voice is faster outside of Asia Pacific.

Related News

New Jersey Supreme Court Upholds Use of DNA Evidence

The highest court of the state of New Jersey issued two decisions that strongly support the capture of DNA from adults and children convicted of crimes and for including that DNA in a database. The court's decision also rejected the imposition of time limits on the use of the captured DNA and supported the transfer of the information to other suitable authorities.

POTENTIAL IMPACT: These two decisions overwhelmingly ratify the capture and use of DNA from convicted adults and children - both for use in solving other crimes in the past and the future.

and for use forever into the future, as well as for transfer to other appropriated authorities and jurisdictions. These two decisions are the final word, as far as the New Jersey Constitution is concerned. It is subject to review by the Federal Courts as far as the United States Constitution is concerned, if the prisoners choose to bring the matter to the Federal Courts.

DETAILS: The capture of DNA from convicted offenders is mandated by the New Jersey DNA Database and Databank Act of 1994. The DNA test results are to be used for the following purposes:

a. for law enforcement identification purposes;
b. for development of a population database;
c. to support identification research and protocol development of forensic DNA analysis methods
d. to assist in the recovery or identification of human remains from mass disasters or for other humanitarian purposes;
e. for research, administrative and quality control purposes;
f. for judicial proceedings, by order of the court, if otherwise admissible pursuant to applicable statutes or rules;
g. for criminal defense purposes, on behalf of a defendant, who shall have access to relevant samples and analyses performed in connection with the case in which the defendant is charged; and
h. for such other purposes as may be required under federal law as a condition for obtaining federal funding. [N.J.S.A. 53:1-20.21.]

The Act declares that DNA samples and the test results are to be kept confidential. N.J.S.A. 53:1-20.27.Further, the disclosure of "individually identifiable DNA information" in "any manner to any person or agency not entitled to receive it" is a disorderly persons offense. N.J.S.A. 53:1-20.26. In addition to establishing a state DNA database, the Act requires the DNA information to be forwarded to the Federal Bureau of Investigation (FBI) for inclusion in the Combined DNA Index System (CODIS),

The cases:

People v O'Hagen – In 2002, John O'Hagen was indicted for third-degree possession of a controlled dangerous substance. He entered into a plea agreement and pled guilty. The court sentenced O'Hagen to a prison term and required O'Hagen to supply a biological sample for DNA testing and storage pursuant to the Act. O'Hagen objected to the collection and testing of his DNA and appealed, claiming that the Act was unconstitutional under both the Federal and State Constitutions as an unreasonable search and seizure without a warrant, as well as a violation of equal protection.

"AA" v New Jersey - The case consolidated one case involving a minor (pseudonym "AA") with another involving an adult that questioned whether a DNA collection statute can

be applied retroactively to persons previously convicted. The AA case also presented the issue of the application of the statute to minors.

The adult case involved Jamaal W. Allah who pled guilty to second-degree possession of a controlled dangerous substance with intent to distribute and third-degree possession of a controlled dangerous substance with intent to distribute. The court imposed a prison sentence. AA, the minor (age fourteen) pled guilty to an act akin to aggravated assault. AA received probation. In 2003, an amendment to the Act extended DNA sampling to convicted adults and delinquent juveniles whose crimes or delinquent acts preceded the original enactment date if the person was still serving a sentence of imprisonment, detention, confinement, probation, parole, or other form of supervision. Both offenders fell into those categories and were required to submit to DNA testing. Both contended that the constitutionality of DNA collecting, testing, and creating a DNA database violated the Fourth and Fourteenth Amendments of the US Constitution other provisions of the New Jersey Constitution.

The Court determined that the capture of DNA from convicted adults and children violates neither the Constitution of the State of New Jersey nor the Constitution of the United States. It also found that there is no need to place a limit on how long the captured samples can be held and used for investigations of past and future crimes. The court found no difference between the capture of DNA from convicts and the taking of fingerprints or photographs of convicts.