Business Roundtable
Security Task Force

A Collaborative Strategy for using National Criminal History Record Checks to Reduce the Insider Terrorist Threat

August 5, 2005

A Collaborative Strategy for Using National Criminal History Record Checks to Reduce the Insider Terrorist Threat

Comments of the Business Roundtable Security Task Force

August 5, 2005

Introduction

The ongoing threat of terrorism requires an unprecedented and sustained commitment from the private sector. Because more that 85 percent of the nation's critical infrastructure - the power grid, financial services, information services, railroads, airlines and others - is owned or operated by the private sector, the business community has important roles and responsibilities in homeland security. The 160 CEO members of the Business Roundtable – with 10 million employees and $4 trillion in annual revenues – recognize and accept this responsibility, and have moved forward to strengthen security at individual companies and to help collectively in our nation's preparedness, disaster response, and recovery programs.

The Roundtable has established a Security Task Force that has spearheaded successful initiatives to enhance preparedness. These include creation of CEO COM LINK^{SM}, a secure telephone communications system to connect businesses and government for the exchange of timely information in the event of a terrorist threat or a crisis; development of two comprehensive guides to assist CEOs and other corporate managers in strengthening homeland security by improving the private sector's preparedness for infrastructure disruptions, natural disasters and terrorist attacks; and authoring two widely disseminated publications: a *Crisis Communications Toolkit* that offers best practices for communicating with employers, customers and neighbors during a crisis, and a white paper entitled *Terrorism: Real threats. Real costs. Joint solutions*, which concludes that the best security solutions will come from government policies that encourage greater business participation and are based on collaborative efforts that favor flexible and focused private-sector initiatives.

Currently, the Business Roundtable Security Task Force is focused on three key initiatives: hardening the Internet by securing cyberspace against attack and taking steps to ensure that essential online business functions are safeguarded so as to ensure safe, secure and survivable communications; enhancing supply chain and port security by working with government and business to bring a greater focus on improving security at points of entry for goods and materials and on developing sound security investment policies to maximize finite financial resources; and addressing the insider terrorist threat through improved applicant screening. This latter initiative is the focus of these comments.

Enhanced Screening of Job Applicants is Critical and Consistent with the National Strategy for Securing Critical Infrastructures

The Business Roundtable believes that there are homeland security, national security and economic security needs for employers to be able to screen prospective employees against a national database in order to reduce the insider terrorist threat to critical industries and infrastructures.

The need to improve security by providing employers with a way to benefit from government criminal history databases for screening of those applying for sensitive positions was identified in the President's *National Strategy for Physical Protection of Critical Infrastructure and Key Assets*. That strategy notes:

> *"Those who have access to and operate our critical infrastructures and key assets are crucial to our national protective scheme. ... Time-efficient, thorough, and periodic background screening of candidate employees, visitors, permanent and temporary staff, and contractors for sensitive positions is an important tool for protecting against the 'insider threat.' Unfortunately, in-depth personnel screening and background checks are often beyond the capabilities of private sector and non-federal government entities. Private employers also lack access to personnel reliability data—often in the possession of the federal government—that could help determine whether employees, contractors, and visitors should be employed at or allowed access to sensitive facilities."*

Working with government to reduce the insider terrorist threat through more effective and efficient screening of potential hires in sensitive industries and facilities against the national criminal history database is a top priority of the Business Roundtable. Key industries already employ extensive background screening for sensitive positions. However, there are inevitable gaps in what employers can accomplish without access to a national database. To meet the homeland security imperative to protect against the insider terrorist threat in the private sector, business and government must work collaboratively to fill those gaps in a comprehensive way, rather than the sector-specific, patchwork approach that has been adopted to date.

The Roundtable is mindful that policies and procedures for providing broader screening against the national database must be efficient, fair, and respectful of legitimate privacy concerns. It will be important to avoid overburdening the already stretched resources of local law enforcement, which is often called upon now to act as intermediary for non-criminal justice records checks. In addition, as with the current processes in place for background screening pursuant to laws like the Right to Financial Privacy Act, criminal records should only be used in hiring decisions where appropriate for the job, and adequate procedures must be in place for applicants or employees who may be treated unfairly or whose records may be inaccurate. Moreover, safeguarding personal information about employees or applicants is a fundamental requirement of corporate security.

While these comments focus on protecting critical infrastructure from an insider terrorist threat, there are obviously other private sector employers with a legitimate need to carefully screen job applicants for homeland and national security purposes or other reasons. For example, Congress has already determined that child care facilities or other places where volunteers or employees work closely with children should be able to get information from the national database. And most recently, Congress extended access to the database to cover private security officer companies. Broader access, beyond critical infrastructure sectors, may be necessary and appropriate.

The National Security Imperative to Protect Critical Infrastructure

The need to protect critical infrastructures owned or operated by the private sector is beyond dispute. The Department of Homeland Security has identified a number of critical industries with "infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security." Some of the most critical are:

- Civilian nuclear power
- Chemicals and hazardous materials (including oil and natural gas)
- Electricity service
- Food and agriculture
- Water
- Financial Services
- Emergency Services
- Government Operations
- Transportation

Congress also recognizes these sectors as relevant to the national defense. For example, Congress has amended the Defense Production Act of 1950 to explicitly include the critical infrastructures (protection and restoration) as part of the law's parameters. In addition, the Homeland Security Act of 2002 includes provisions to protect from disclosure information submitted by the private sector to the Department of Homeland Security about vulnerabilities and threats to critical infrastructure, much the same way national security information is protected. Most recently, the Intelligence Reform and Terrorism Prevention Act of 2004 included a requirement for the Department of Homeland Security to report to Congress on its assessment of critical infrastructure protection needs and the readiness of the Government to respond to threats against the nation's infrastructure.

Listed below are examples of damage caused by disruptions to elements of the nation's critical infrastructure. While none of these examples were caused by terrorists, it does not require a great deal of imagination to move from these real life examples to envision the damage and economic impact if terrorists gained access to sensitive jobs in critical infrastructure sectors.

- On August 14, 2003, North America experienced the largest blackout in history. It affected eight states in the Midwest and Northeast, and parts of Canada. At its peak over 50 million people were without power and over 100 power plants were immobilized and shut down. The blackout has been estimated to have cost businesses over $6 billion in direct costs and possibly much more in losses in goodwill and brand equity. [i]

- In September of 2002, a dispute between the longshoremen and port operators and shipping lines closed ports from San Diego to Seattle for eleven days. With some economists estimating damage to the economy of $1 billion a day, the lockout caused factories to close, perishable cargo to rot, and retailers to face inventory shortages. [ii]

- In 2000, in Maroochy Shire, Australia, a discontented former employee was able to remotely access the controls of a sewage plant and discharge approximately 264,000 gallons of untreated sewage into the local environment. [iii]

A Shared Security Responsibility Between the Public and Private Sectors

In his cover letter to the *National Strategy for Physical Protection of Critical Infrastructure and Key Assets*, President Bush closed by remarking,

> *As we work to implement this Strategy, it is important to remember that protection of our critical infrastructures and key assets is a shared responsibility. Accordingly, the success of our protective efforts will require close cooperation between government and the private sector at all levels. Each of us has an extremely important role to play in protecting the infrastructures and assets that are the basis for our daily lives and that represent important components of our national power and prestige.*

Private Sector Responsibility

As noted above, approximately 85% of the nation's critical infrastructure is in the private sector. Thus, the private sector is best positioned, and has the responsibility, to undertake many of the necessary steps to ensure the security of that infrastructure. This applies to applicant screening as well as to other security measures. Industry is best able to identify those positions that are most sensitive from an insider threat perspective, for example. Businesses are also best positioned to understand the kind of information they require to adequately screen applicants for sensitive jobs.

Many employers in sensitive industries already conduct extensive screenings, but there are gaps that can only effectively be filled with information from the U.S. government. For example, criminal checks on potential hires currently can only be run against local, rather than national databases and are generally conducted only in locales that the applicant indicates as prior residences. Thus, the thoroughness of this check is dependent upon the accuracy and thoroughness of the application submitted by the prospective employee. Moreover, criminal activity that may have occurred outside the residential area will not be discovered. Access to a national database will fill this critical gap.

Screening applicants against a comprehensive, national criminal history database will not necessarily identify suspected terrorists. However, experts have found that terrorists often finance themselves through criminal activity. Moreover, applicants who lie about their criminal history have a vulnerability that could be exploited by terrorists.

A fingerprint check can also assist critical industries to verify the identity of prospective hires in sensitive positions. Key to an effective personnel screening program is the ability to ensure that the applicant is not misrepresenting their identity. While programs like those prescribed in the REAL ID Act will go a long way toward addressing this problem, they will take some time to implement. Unfortunately, as we saw with the recent bombings in London, we cannot assume that time is on our side.

U.S. Government Responsibility

Addressing the insider threat is ultimately part of a general risk management strategy. As with any risk management plan, this requires mapping threat information against vulnerabilities. As noted above, industry is best positioned to identify vulnerabilities, including with regard to applicant screening. However, the federal government is the repository of the only truly national

criminal history database, which is key to identifying potential threats. Only the federal government can work with all 50 states to ensure that all local criminal records can be appropriately accessed at a national level in a way that is efficient, accurate, and safeguards legitimate privacy interests.

Need for Strategy to Strengthen Public-Private Partnership

The Roundtable believes that private industry and the federal government should work collaboratively to develop mechanisms for providing employers with appropriate information from the national database based on a partnership with government. The federal government and industry representatives should also consult on ways to safeguard an applicant's privacy and afford applicants adequate due process. Existing procedures and requirements for safeguarding applicant rights in the context of criminal history checks can inform policies for these national record checks.

This work would build on existing policies that already permit such screening. For example, in recognition of the homeland security value of screening employees against the national database, Congress has already enacted laws requiring such screening for some highly sensitive jobs, including airline employees and hazardous cargo truck drivers. For example, the Transportation Worker Identification Credential (TWIC) program creates a nationwide credential system, including national criminal history checks for key employees, designed to enhance security at U.S. transportation facilities, including seaports, airports, railway, pipeline, trucking and mass transit facilities. Rather than these patchwork, industry-specific, mandatory laws, however, the Business Roundtable believes that a voluntary, across-the-board initiative is a more effective approach. As noted earlier, the private sector is in the best position to identify sensitive jobs for which this level of screening is needed.

An example of this kind of voluntary screening is the recent Private Security Officer Employment Authorization Act of 2004, which authorized employers to screen individuals applying to be private security officers against the national database at the employers discretion. Similarly, the Volunteers for Children Act, enacted in 1998, allows entities that involve contact with children to choose to request fingerprint-based national criminal history record checks of employees and volunteers. This has led to the development of innovative collaborative mechanisms between the private sector, state law enforcement agencies, and the federal government to enhance screening and, hence, the safety of children. These could serve as useful models.

Conclusion

The Roundtable understands that the private sector must share the heavy lifting as our nation prepares for the possibility of future domestic attacks by terrorists, and companies have taken action to improve security for our employees, their communities, and our companies. Working in partnership with the government to mitigate the insider terrorist threat by improving the voluntary screening process for sensitive jobs in industry is a priority of the Roundtable's Security Task Force. We applaud Congress for recognizing the need for a review of current laws and policies on non-criminal justice access to the national database and are grateful for this opportunity to provide our input into the review being undertaken by the Department of Justice. We look forward to working with Congress and the executive branch to develop an effective and appropriate way to provide employers with essential information from the national criminal history database.

[i] "The 2003 Blackout: Economy Won't Likely Be Derailed --- Cost Could Hit $6 Billion As Major Sectors Are Hurt; A Few Reaped Benefits," by Jon E. Hilsenrath, *The Wall Street Journal*, A6, August 18, 2003. **"**Record blackout over for most; Officials still in dark over failure of grid," by Jerry Seper, *The Washington Times*, A01, August 16, 2003.

[ii] "Both Sides See Gains in Deal To End Port Labor Dispute," by Steven Greenhouse, *The New York Times*, Page 14, Column 5, November 25, 2002.

[iii] "Critical Infrastructure: Control Systems and the Terrorist Threat," by Dana Shea, *CRS Report for Congress,* received through CRS web, updated July 14, 2003, citing National Infrastructure Protection Center, *Highlights*, 2-03, June 15, 2002.