

Oracle PROTECT: Solutions for Homeland Security

*An Oracle Business White Paper
June 2005*

Oracle PROTECT: Solutions for Homeland Security

INTRODUCTION

The events of September 11, 2001 have changed our country and our lives forever. Today, we remain in the midst of a global war – a war on crime and terrorism. It is also a “4th Generation War,” one in which the enemy does not operate from geopolitical boundaries, but rather through a network of “cells,” both within our homeland and abroad. It is, in many respects, a global insurgency.

At Oracle, we believe that information sharing can be a primary deterrent to all forms of terrorism. Just as the 9/11 Commission recommended that the President coordinate a “trusted information network,” we are taking preventative measures to exploit all forms of data to produce timely and accurate intelligence. Intelligence sharing is the means to provide for the safety and security of our community and our national interests to:

- Reduce the incidence and fear of crime;
- Prevent terrorism;
- Safeguard assets; and
- Improve health.

The need for a trusted information network that unifies thousands of types of disparate data sources and facilitates the genuine sharing of information and intelligence among agencies across the nation has driven us to create Oracle PROTECT Solutions for Homeland Security.

“The President should lead the government side effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a ‘trusted information network’.”

- *The 9/11 Commission Report,*
July 2004

ORACLE PROTECT: SOLUTIONS FOR HOMELAND SECURITY

Oracle takes proactive action to affect positive change in our world by focusing on problem solving as opposed to consequence management. Oracle PROTECT Solutions leverage Oracle's people, products and corporate assets to improve both quality of life and functions vital to society.

A set of solutions based upon Oracle's core technology, applications, professional services, and partner solutions, PROTECT Solutions assist in preventing, preparing for, and responding to crimes and terrorist attacks on the homeland by providing a flexible and adaptable architecture upon which a decentralized information sharing network can be built. Moreover, PROTECT fully integrates disparate systems, leverages resources, and shares data in an efficient, seamless, and interoperable manner.

The goal of PROTECT Solutions is to provide the capability for a fully integrated system in which public and private entities across the United States can share information in a trusted and secure manner. Oracle's PROTECT Solutions for Homeland Security are based on a "Trusted Information Sharing" approach that:

- Promotes actionable, timely and accurate intelligence;
- Defends our global interests, economy and commerce;
- Safeguards our health, food and water;
- Secures our data, key assets and infrastructures; and
- Maintains continuity of operations of our business enterprises.

Oracle PROTECT is comprised of a portfolio of over twenty separate business solutions. These are integrated offerings of Oracle products and services which are often complemented by Oracle Partner offerings. These solutions address key business requirements – those that impact the safety and security of our country and our environment – in the following five market areas:

- PROTECT for National Security
- PROTECT for Net-Centric Operations and Warfighting
- PROTECT for Justice and Public Safety
- PROTECT for Healthcare
- PROTECT for Critical Infrastructures

The foundation of Oracle PROTECT is Oracle's technology and applications products, which include: Oracle Database 10g, Oracle Fusion Middleware (consisting of the family of products in Oracle Application Server 10g, Oracle Developer Suite, Business Process Management and Activity Monitoring, Oracle Data Hubs and Oracle Collaboration Suite), and Oracle E-Business Suite.

Reducing crime and terrorism... "begins with timely, accurate intelligence."

- **William Bratton, Chief LAPD, PERF Conference, April 2005**

Oracle's Trusted Information Sharing approach provides an innovative, modular, scalable and secure information architecture that integrates all of these products and supports the information management and sharing requirements of each of the PROTECT market areas.

PROTECT FOR NATIONAL SECURITY

Through the use of foreign and domestic intelligence, the national security community performs its critical mission of protecting the nation—a daunting obligation. Sifting through large volumes of data, tracking down leads, coordinating with military intelligence and local law enforcement, and sharing and pooling knowledge all present both cultural and technical challenges, challenges that must be met in order to successfully fight a nimble enemy like the modern terrorist.

Business Problems in National Security

Securing our nation requires detailed cooperation and near flawless execution.

National security challenges continue to increase, and the public is aware of many of them because of the publicity those challenges receive.

These challenges include:

- Mining vast amounts of data.
- Protecting sources and methods while sharing intelligence.
- Sharing terrorism intelligence with local law enforcement as well as national customers across different security domains.
- Managing a large number of key assets and critical infrastructure and protecting them from threats.
- Maintaining a skilled workforce and maximizing their utilization across agencies.
- Collaborating across the community and performing joint analytic work.
- Pursuing innovative methods of gleaning intelligence from new sources.



“Communication, collaboration, and sharing across the gaps between and among [the appropriate actors] are critical to countering terrorism because we cannot predict where the first sign of a potential terrorist threat will come from—a communications intercept from the National Security Agency (NSA), a human source of the CIA or the FBI, an investigation by a local police department, or an observation by an alert private security guard or emergency room nurse.”

- ***Creating a Trusted Information Network for National Security,***
The Markle Foundation

Oracle PROTECT for National Security offers solutions specifically designed to meet the most demanding challenges facing the national security space.

Business Solutions Provided for National Security

Oracle PROTECT for National Security offers solutions specifically designed to meet the most demanding challenges facing the national security community. These solutions are securely architected with enterprise scalability and manageability to facilitate information sharing, National Security Agency accreditation for multi-level secure information sharing (NSA Protection Level Four (PL-4)), collaborative analysis, enterprise information discovery, and selectivity and targeting.

Oracle PROTECT for National Security includes the following ten business solutions:

- Selectivity and Targeting
- Collaborative Analysis
- Case Management
- Cross-Domain Information Sharing
- National Asset Management and Protection
- Enterprise Information Discovery
- National Security Data Hub
- Human Capital Management
- Biometrics Management
- Sensor and Location-Based Services

PROTECT FOR NCO AND WARFIGHTING

Secretary of Defense Donald Rumsfeld has been driving the United States military to transform itself from a post-Cold War fighting force to one that is capable of addressing emerging 21st century challenges. A key part of this transformation is leveraging “network-centric operations,” or the synergies derived from interoperable, connected information systems.

Oracle PROTECT for Net-Centric Operations (NCO) and Warfighting is a series of capabilities based on Oracle’s technology platform that addresses secure information sharing, mobile connectivity, high-end analytics, legacy system integration, and geospatial representation.

Business Problems in NCO and Warfighting

Maintaining security in a networked, information-intensive world is taxing the budget plans and programs instituted during the industrial-based Cold War. As a result, the military recognizes that it must change the way it operates. The following list provides a glimpse of the complex, difficult problems facing America’s defense community today:

- Inability to support dynamic coalition warfighting operations

Oracle’s PROTECT Solution for Net-Centric Operations and Warfighting is a series of capabilities based on Oracle’s technology platform that addresses secure information sharing, mobile connectivity, high-end analytics, legacy systems integration and geospatial representation.

- Limited program funding
- Enemy forces generating comparable battlefield effects for far less money
- Many disparate legacy systems
- Fragmented data stores
- Inefficient business processes
- Lack of secure and seamless data distribution to participants
- Inadequate means to provide accurate and timely “machine-to-machine” data transfer
- Increased competition for talented technical people



Source: U.S. Navy

As America’s military proceeds with its transformation to a 21st century information-based fighting force, it must develop an enterprise-class information infrastructure to handle intense, short-lived, rapid-response operations in a global battlespace.

Business Solutions Provided for NCO and Warfighting

By conforming to the latest SOA standards, Oracle PROTECT allows for a robust environment of modular web services or business process components that can be consumed or configured based on the evolving operational situation.

Oracle PROTECT for NCO and Warfighting provides a robust, high-performance, secure information infrastructure that helps today’s front-line military forces obtain relevant, timely information to make effective combat decisions. By conforming to the latest Service Oriented Architecture (SOA) standards, Oracle PROTECT enables a robust environment of modular web services or business process components that can be consumed or configured based on the evolving operational situation.

Oracle’s Protect for NCO and Warfighting solution includes the following seven business solutions:

- Cross-Domain Information Sharing
- Collaborative Operations Planning and Execution
- RFID-Enabled Logistics
- Geospatial Battlespace Awareness
- High-Performance Tactical Grid
- Secure Data Auditing
- Disconnected Operations

PROTECT FOR JUSTICE AND PUBLIC SAFETY

Law enforcement is on the front lines of dealing with terrorism, both in terms of prevention and response. But police must also address the day-to-day problem of fighting crime. To make matters worse, both missions must be accomplished with increasingly limited resources.

Combining emerging technologies with Oracle technology, applications, and consulting services as well as Oracle Partner applications, PROTECT for Justice and Public Safety aims to solve real-world business problems. The PROTECT architecture—a SOA—integrates disparate legacy systems, thereby leveraging existing user investments while seamlessly adding emerging applications. Further, PROTECT enables agencies to share critical information in real time.

Business Problems in Justice and Public Safety

Law enforcement and public safety agencies have encountered many disadvantages in their new mission tasking of detecting, deterring, and preventing crime and terrorism before they occur. Today, these agencies cannot:

- Securely share criminal and terrorism intelligence regionally (which is critical to investigations and analysis);
- Track crime regionally and in real time;
- Efficiently execute incident management;
- Refer to a virtual library of crime fighting best practices;
- Identify, quantify, assess, validate, manage, or provide analysis on a large number of critical infrastructure assets;
- Analyze data to identify trouble spots and pre-incident indicators, focus resources, and help solve crimes; or
- Efficiently ensure relentless follow up to reduce crime, the fear of crime, and potential terrorist pre-incident and incident activities.



“With terrorism, prevention is the whole point...The best—and the essential—prevention weapon is information.”

- **Dr. David Harris, author of *Good Cops: The Case for Prevention Policy*, PERF Conference, April 2005**

Law enforcement is further challenged by the growth of gangs, the need to serve as counter-insurgency ‘soldiers’ in the war on terrorism, and the need to work outside traditional jurisdictional boundaries that are often exploited by both criminals and terrorists. Moreover, law enforcement agencies must contend with numerous complex demographic, political, and cultural factors that impede crime fighting and counterterrorism at the city, county, regional, and state levels.

PROTECT allows a law enforcement agency the option and the ability to securely share information with federal, state and local, and commercial systems.

Business Solutions Provided for Justice and Public Safety

The Oracle PROTECT for Justice and Public Safety solution focuses on the early detection, deterrence, and prevention of criminal and terrorist activity. PROTECT uses an integrated approach to develop regional crime fighting and counterterrorism intelligence sharing capabilities. Further, PROTECT allows a law enforcement agency the option and the ability to securely share information with federal, state and local, and commercial agencies.

The Oracle PROTECT for Justice and Public Safety solution encompasses two principal business solutions that fully address the business challenges, goals, and key business requirements of state and local law enforcement agencies:

- Regional Crime Fighting; and
- Regional Counterterrorism.

PROTECT FOR HEALTHCARE

Today, public health agencies find themselves in a new environment. Typically underfunded, public health organizations have traditionally struggled to just maintain current technology in order to support the most vital program areas within their purview (e.g., immunization registries or environmental health tracking). Nowadays, public health organizations are expected to become more enabling—relying upon health-related data from public and private sources to better assess health threats and to help achieve better health outcomes for the citizens, businesses, and health organizations within the community.

As such, the real problem for public health organizations is how to gain access to all of the needed health data without controlling the source systems that hold that data. Certainly, data integration is a daunting issue as there are many different technologies, systems, and even health terminologies that a public health organization must consolidate. The challenge, therefore, is to establish a platform that can store all of this data in a secure, private manner in order to provide analysts, epidemiologists, doctors, and other stakeholders appropriate, real time access to review and act on integrated up-to-date health-related information.

Oracle has created a unifying, central healthcare data repository based upon healthcare industry standards that enables the consolidation and integration of health data. Together with an integration engine that allows data to be transferred from system to system, these technologies enable data sharing, thereby facilitating the establishment of a truly integrated healthcare community. This solution is known as Oracle PROTECT for Healthcare.

Business Problems in Healthcare

The challenges that the healthcare industry faces are shared amongst the public and private communities. While both have different perspectives on the issues, a central issue that needs to be addressed is healthcare interoperability.

“...the nation’s largest industry in terms of gross national product—data sharing—is not readily available because of proprietary standards in healthcare IT.”

**- Dr. David Brailer,
National Coordinator for Health
Information Technology,
February 2005**

PHIN will have dual functionality—it will provide a foundation for routine public health activities and it will enhance bioterrorism detection and response.

Interoperability

The ability to share health-related data, both clinical and non-clinical, is critical to the future of healthcare. Proper information sharing provides near real time data access for those who treat patients, and it provides the ability to assess potential public health disasters. Within the public health realm, the Centers for Disease Control and Prevention (CDC) has endorsed the establishment of a secure information sharing network that enables public health agencies to exchange health data from many systems, including both clinical and traditional public health data (e.g., immunizations and disease surveillance). This network is known as the Public Health Information Network (PHIN). The overall vision for PHIN is an information network that integrates public health partners across the nation. PHIN will have dual functionality—it will both provide a foundation for routine public health activities as well as enhance bioterrorism detection and response.

The other initiative that pertains to interoperability is the Electronic Health Record (EHR). The EHR concept supports a community-based system of healthcare, focusing on the citizen of the community rather than the individual healthcare delivery providers. Its design presents a fluid stream of healthcare information available at all potential patient touch points. This rectifies the silo-based, partial view of patient health records that exists today.



These two interoperability initiatives have many attributes in common. As such, Oracle has created a technology footprint that addresses both

PHIN and EHR, based upon Oracle's core technology products.

Public health organizations need to be able to access and analyze various data that are leading indicators of potential health incidents.

Homeland Security and Bioterrorism

Besides the need for health data interoperability, healthcare professionals are also acutely aware of the need to be able to detect and respond to bioterrorism events. Specifically, public and private healthcare organizations need to work together to share information pertinent to the incident detection. While specific situations may differ, public health organizations need to be able to access and analyze various data sources that are proven indicators of potential health incidents, such as student absenteeism and over-the-counter pharmaceutical sales.

Business Solutions Provided for Healthcare



The Oracle PROTECT for Healthcare solution is an infrastructure that provides public and private health organizations with the ability to create a near real time messaging network comprised of member organizations or systems from both inside and outside the health organization.

At the center of this network is a public health data repository. The purpose of this is to make available public health data for central access without the need to query multiple systems. PROTECT for Healthcare follows the requirements and standards as set by CDC, the Centers for Medicare and Medicaid Services (CMS), and HIPAA. Together with specific solution partners for subjects like disease surveillance, Oracle delivers a full-function solution for healthcare that focuses on both individual programs as well as the more global view of public health within the community.

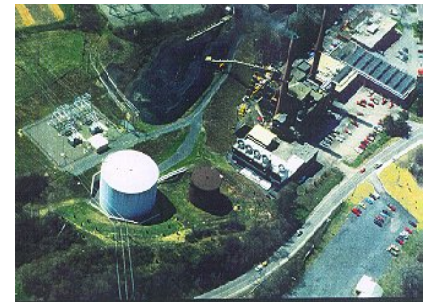
In general, the Oracle PROTECT for Healthcare solution portfolio is focused upon the integration of systems and people by leveraging Oracle technology to apply effective business rules to all healthcare data regardless of where it is currently stored. Oracle offers the following three healthcare related business solutions:

- Oracle Public Health Information Network (PHIN);
- Oracle Electronic Health Record (EHR); and
- Oracle Health Alert Network.

PROTECT FOR CRITICAL INFRASTRUCTURES

PROTECT for Critical Infrastructure Protection is an interactive, web-based planning, decision support, and collaboration solution to track, assess and manage threats and vulnerabilities to infrastructure and key assets.

Threats once identified as being primarily overseas are now facing us in our homeland. The American people and our infrastructure are vulnerable to potentially debilitating attacks that threaten our national security, economic viability and societal well being. PROTECT for Critical Infrastructures is an interactive, web-based planning, decision support, and collaboration solution that tracks, assesses and manages threats and vulnerabilities to infrastructure and key assets.



The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* defines critical infrastructures and key assets as “a highly complex, heterogeneous, and independent mix of facilities, systems, and functions that are vulnerable to a wide variety of threats.” Accordingly, it is incumbent on leaders of both public and private enterprises to take prudent action to protect their physical assets, their electronic data, and other intangible assets.

PROTECT for Critical Infrastructures provides both the public and private sectors with the ability to:

- Identify the assets entering an enterprise;
- Track, control, and manage those assets;
- Identify the assets leaving an enterprise; and
- Survey and secure the enterprise at all times.

ORACLE'S PRODUCT SUITE: THE FOUNDATION FOR PROTECT

The Oracle PROTECT portfolio of solutions is built on database tools, development tools, professional services, and a suite of existing applications that integrate and extend a variety of business functions to meet the needs of the homeland security, intelligence, law enforcement, healthcare and Defense communities. The basic lineup of products is as follows:

- **Oracle Database.** The foundation of Oracle's product line is the powerful and secure Oracle Database 10g. Oracle Database 10g is the industry's first database designed for Grid computing. Low entry-level pricing makes Oracle the best choice for large enterprises and small to medium-sized businesses alike.
- **Oracle Enterprise Manager.** Oracle Enterprise Manager 10g with Oracle Grid Control provides a single, integrated interface for administering and monitoring applications and systems based on the Oracle technology stack. Enterprise Manager includes complete monitoring, performance management, distributed database and application server administration, enhanced diagnostics, automated tuning, and an architecture that allows administrators to manage from anywhere.
- **Oracle Fusion Middleware.** Oracle Fusion Middleware is the newly created brand for Oracle's family of existing, world-class middleware products, including all of the products needed to integrate a number of diverse business applications. These products include the family of products in Oracle Application Server 10g: Application Development Tools and J2EE Application Server; Web Services infrastructure; Enterprise Service Busses and Integration; Business Process Management and Activity Monitoring; Business Intelligence Tools; Security and Identity management; Enterprise Portals and Mobile, Oracle Data Hubs, and Oracle Collaboration Suite. The products are available today and are currently being used by thousands of customers and partners throughout the world.



Oracle Fusion Middleware provides a comprehensive, open, standards-based approach for deploying SOA.

As part of the company's initiative to make application integration easier for customers, Oracle Fusion Middleware provides a comprehensive, open, standards-based approach for deploying SOA. Using Web Services, an Enterprise Service Bus and Oracle BPEL Process Manager to implement SOA, customers can easily integrate heterogeneous business applications and automate business processes. Oracle's middleware is used to support the Oracle E-Business Suite as well as other enterprise applications and thousands of Independent Software Vendors that use it as the basis to build their own custom applications.

- **Oracle Collaboration Suite.** Oracle Collaboration Suite brings together the essential components of collaborative productivity: web conferencing, content management, email, messaging, voicemail, fax, an integrated calendar, and wireless connectivity.
- **Oracle Developer Suite.** Oracle offers a complete and integrated set of application development and business intelligence tools that supports any development approach, any technology platform, and any operating system.
- **Oracle Data Hub.** With Oracle's Data Hub products, organizations can synchronize information centrally, from all systems throughout the enterprise, to get an accurate, consistent 360-degree view of the agency's data, whether from packaged, legacy, or custom applications.
- **Oracle's Information-Age Applications.** This complete set of integrated applications collects, processes, and shares information from all public and private sector areas, automates processes so that information is shared across agencies instantly, and can be used out of the box or customized depending on local needs. Oracle applications (Oracle E-Business Suite) automate, streamline, and simplify business processes and put all of an organization's business information in one place so that the enterprise can share high-quality, consistent data in real time.
- **Oracle Services.** In addition to databases, applications, programming, engineering tools, and systems integration services, Oracle provides special consulting, application development, and training.

TRUSTED INFORMATION SHARING

Oracle Trusted Information Sharing provides an innovative, modular, scaleable, and secure architecture that supports the information management and sharing requirements of defense, emergency management and intelligence communities. Trusted Information Sharing provides a nationwide, and in some cases worldwide, content management system consisting of interconnected, decentralized networks that enable the sharing of critical information in real time—in effect, an interactive “network of networks.” Importantly, this approach to the management of mission

Trusted Information Sharing defines a nationwide content management system consisting of interconnected, decentralized networks; these networks will enable the sharing of critical emergency information in real time to create a “network of networks.”

critical information enables coordinated responses while providing seamless data security and respecting individual privacy.

Oracle's Trusted Information Sharing solution defines and provides the architecture for sharing sensitive and classified data within and between organizations by virtually splitting the networks into sensitivity zones. Ensuring the authenticity of the information flowing between emergency responders and/or incident commanders, this system effectively provides a multi-layered defense framework. Based upon modular technologies, this layered framework can be administered and monitored independent of the applications deployed on the networks.



Further, the architecture includes a commercial software based system for sharing information between isolated classified networks. This approach to the National Security Agency Protection Level Four or Five (PL4 or PL5) requirements of the military and intelligence communities greatly facilitates the secure management and sharing of information.

There are generally two aspects of Trusted Information Sharing:

- Within an organization; or
- Between organizations.

These are enabled by three new Oracle technology products: Data Vault, Audit Vault, and Trusted Information Gateway.

Within an Organization

The PROTECT business solution referred to as Cross-Domain Information Sharing extends Oracle security in order to control not only who is accessing the data, but also how, where, and when the data is accessed. For example, Data Vault—an Oracle technology solution within the Cross-Domain Information Sharing solution—can block requests for Secret data from a wireless network without biometric authentication at 3:00 A.M. It can also restrict access to data based upon the user's network. This approach can be used to provide the protection levels mandated by Director of Central Intelligence Directive (DCID) 6/3 for military and intelligence systems. For example, auditing at the data element level will ensure that if a Top Secret cleared user is accessing a PROTECT application from a Secret level network, then that user will have access to, at most, Secret level data. If the same user needs access to the Top Secret data in the same system, the user will have to connect via a Top Secret network to obtain that data.

PROTECT can extend Oracle's robust security to achieve even higher levels of accreditation, such as DCID 6/3 PL4.

Between Organizations

The PROTECT architecture supports federated-based identity management. For example, an agent from one organization could login to System A of his organization, and then the user could connect to System B of another organization without the need to re-login. Under the covers, System B will have checked, via a central authentication server, that the agent has already been authenticated.

A Trusted Information Gateway establishes the concept that specific groups and systems within an agency are the 'Data Owners.' These 'Data Owners' effectively control what information can be shared and with whom the information can be shared. Trusted Information Gateway also establishes 'Data Users' who are authorized to access the data. 'Data Users' can be either users or applications. Thus, a local agency has complete control of what information (and at what security classification) is shared to which agencies and when this sharing occurs. This local level of control not only enables best of breed data security, but also maintains crucial data privacy.

ORACLE PARTNERS

Oracle currently partners with more than 150 companies to develop new ideas and create and test cross-functional products. To support critical homeland security missions, the PROTECT solution portfolio encompasses the best products from this cooperative community. Examples of partner solutions that fulfill key requirements within the homeland security, intelligence, law enforcement, healthcare, and defense communities are as follows:

- **Biometrics and identity management**, including fingerprints, iris scans, and facial recognition systems, are key components used for physical access to facilities, access to IT systems and applications, and authentication of identity.
- **Incident management/command and control applications** help streamline the process of dealing with a disaster or emergency situation.
- **Document authentication and version control** facilitate application development management, content management, and compliance.
- **Radio frequency identification (RFID) and sensor-based computing** enable organizations to track inventory, ensuring, for example, cargo security, and acceptable levels for pollutants or toxins in the environment.
- **“Spatially enabling” the enterprise** provides geographic reference information to existing data as well as real time asset tracking and resource management.
- **Turning data into actionable intelligence** by providing a common taxonomy and context in order to make the information relevant to the situation and needs of the participants.

- **Physical security of people or infrastructure** via monitored access and staff identification systems.

ORACLE PROTECT: VALUE PROPOSITION

Oracle, as a major information management solution provider, and working with its partners:

- Provides a secure technology infrastructure, including:
 - Integration and collaboration;
 - Consolidation;
 - Decision support and business intelligence; and
 - Workflow, alerts, and notifications.
- Which will enable:
 - Accurate and timely intelligence;
 - Effective military and police tactics;
 - Rapid deployment of personnel and resources to critical incidents; and
 - Relentless follow-up, pursuit and assessment.
- And, will result in:
 - Improved response to critical disasters;
 - Reduction of crime; and
 - Deterred acts of terrorism.

Agencies, departments, and governments of all sizes benefit by implementing a PROTECT solution that supports not only homeland security needs and critical missions, but also supports basic business requirements such as safe data storage, secure communications, more efficient workflow processes, and easier policy administration. Additionally, the PROTECT solution sets enable easier implementation of all-important cyber-security features that ensure critical computer systems remain up and running.

Oracle has more than 25 years of experience supporting federal defense and civilian agencies as well as state, local, and municipal governments. Oracle's installed solutions form the foundation of America's critical information infrastructure today. Our database, architecture, and application offerings power government agencies, financial institutions, utilities, hospitals, and educational institutions. We understand the scope and depth of the Homeland Security challenge: there is no quick-fix solution. However, Oracle is committed to bringing together our leading technology infrastructure, applications, and domain expertise to deliver secure, cohesive, relevant, and flexible solutions.

Oracle has more than 25 years of experience supporting federal defense and civilian agencies as well as state, local, and municipal governments.

CONCLUSION

To achieve “Unity of Effort in Sharing Information,” an overarching decentralized framework must be built. As a Markle Foundation report states, “...without an overall framework that links regional or local networks with one another and with federal entities, the full potential of state and local governments will never be realized.”

A decentralized network model will not only encourage communication, collaboration, and sharing between federal, state, and local agencies, but it will also promote a “need-to-share” culture of integration. Sharing information horizontally, as the 9/11 Commission recommends, will reduce existing information gaps and unify the nation’s efforts to fight terrorism.

Oracle PROTECT Solutions for Homeland Security focus on applying technology to solve mission critical homeland security problems to meet national and local requirements. PROTECT addresses the challenges and fulfills the recommendations outlined in *The 9/11 Commission Report*. Integrated across the federal, state and local, and commercial markets via a common architecture and approach, the PROTECT portfolio is a “system of systems” leveraging Oracle’s industry-leading technology.



Oracle PROTECT

June 2005

Authors: Stan Defilippi, Greg Gardner, Julie Greenspoon,

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Copyright © 2005, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.