

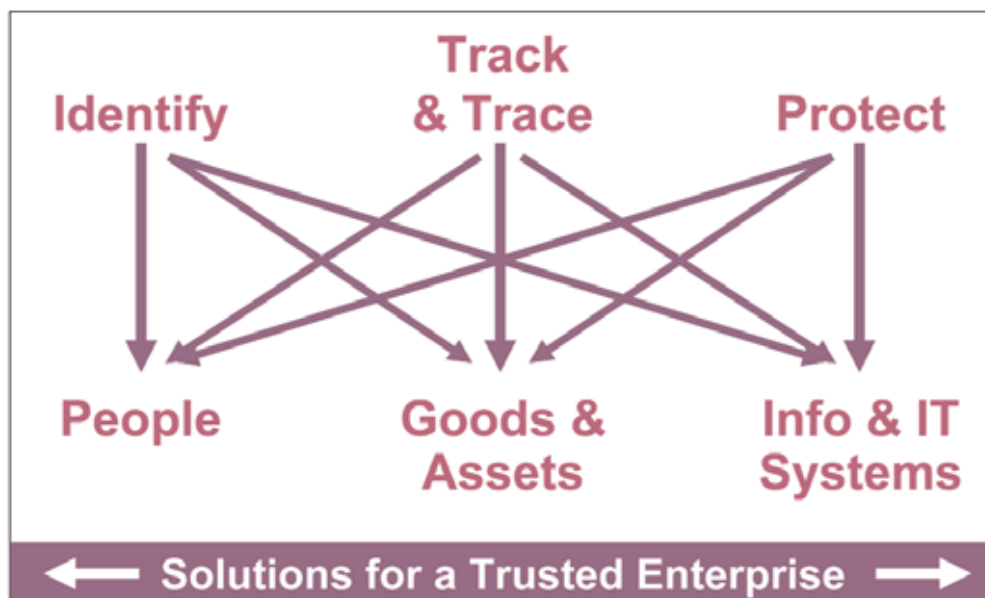


white paper

Secure Business Operations: Redefining Security

trusted

The 'current state' enterprise is unprepared for the security ramifications of global changes and must redefine its security posture via a holistic risk management approach that spans people, goods and assets, and information systems. Redefining security in this manner will provide the future foundation by which to manage risk and develop new ways to conduct business. Unisys has the comprehensive security solution portfolio and the 3D-Visible Enterprise methodology to help clients address these critical needs from strategy to execution.



Executive Summary

A secure business operation is a government or commercial entity with a security posture that meets or exceeds the current threat environment — a security posture that efficiently manages risk and effectively maximizes security investments. In addition to its core mission of ensuring confidentiality, integrity and availability through all its processes, a secure business operation leverages security for competitive advantage by viewing security investments as a business accelerator that delivers opportunities for growth and innovation.

The vision for the secure business operation is clear, yet most organizations today are far from achieving it due to a wide variety of real-world challenges. First, forces of globalization, decentralization, outsourcing and the Internet are requiring nations, governments and businesses to conduct their operations on an ever-growing scale, with corresponding increases in compliance, collaboration, communications, competition and complexity. Second, organizations face the challenge of balancing agility and assurance as they must simultaneously balance the speed and flexibility of their operations with safety and security. Third, today's security environment is faced with escalating, asymmetric threats that can strike at any time, any place and against almost any target.

As evidenced by numerous high-profile events reported by the world media, the 'current state' enterprise is unprepared for the security ramifications of these global challenges and must redefine its security posture via a holistic approach that embraces people, goods and assets, and information systems. Rethinking and redefining security in this manner will provide the foundation to more efficiently manage risk and more effectively develop new ways of conducting business.

This white paper explores the market forces and business challenges affecting the entire spectrum of enterprise security — from identifying people, to tracking and tracing goods and assets, to securing IT systems and data — and discusses how organizations should redefine their security postures to become the secure business operations of tomorrow.

The Secure Business Operation Challenge

Today's security challenges for the typical government and corporate enterprise include external environmental factors, internal factors such as achieving the right balance between agility and assurance, and dynamic factors in terms of maintaining the correct level of preparedness to match ever-changing threat conditions. The first challenge of external market forces stems from conducting global commerce — doing business on the world stage. The second challenge relates to the organization's internal culture and policies in terms of finding the right balance between business convenience and safety. The third challenge relates to the organization's ability to adapt to change and to raise or lower its security posture accordingly. We examine each of these challenges here.

Challenge #1: Market Forces — The Five Forces of Globalization

In the global economy, a perfect storm that threatens to disrupt the day-to-day operations and future prosperity of nations, governments and commercial enterprises is on the horizon. Unlike the localized forces of nature that once endangered maritime crossings and the regional exchange of goods and assets, these new influences include truly complex global forces of compliance, collaboration, communications and competition.

Globalization has opened up the free flow of trade, capital, people and knowledge across both developed and emerging markets. Businesses have access to global markets to source their goods and services and export their finished products, enabling revenue growth, cost reduction and performance improvement. The world stage provides the opportunity to gain economies of scale, competitive advantage and the differentiation needed for steady, incremental growth required by capital markets.

The price of admission to do business on this world stage, however, is exposure to the myriad of market forces mentioned above. In recent years, all of these forces have opened up the enterprise to a rising tide of security threats and vulnerabilities. Thus, the enterprise must act to mitigate the risk.

Forces of Compliance

The increasing regulatory environment includes governance, privacy, standards and industry requirements, and varies widely from country to country. For example, in the U.S. certain public and private organizations may be required to comply with regulations, mandates or guidelines such as Sarbanes-Oxley (Sox), the Health Insurance Portability and Accountability Act (HIPAA), ISO 17799 or FISMA, the Customs-Trade Partnership Against Terrorism (C-TPAT), Homeland Security Presidential Directive 12 (HSPD-12), the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) and the Federal Financial Institutions Examination Council (FFIEC) guidance — to name just a few. In other countries, organizations must comply with measures such as the Basel II and the European Data Privacy Directive in Europe, the Canadian Privacy Act, and the Hong Kong Personal Data Privacy Act.

Within the U.S. Government, one mandate is Homeland Security Presidential Directive (HSPD) 12. HSPD-12 was issued in 2005 with the aim of establishing a government-wide, standardized credential for personal identity verification (PIV) for government employees and contractors for both physical and logical access. This means that agencies must issue a single credential to employees and contractors that can support both physical access to government buildings as well as logical access to government IT systems. For government agencies, such mandates will require broad changes to current processes and IT systems, including the ability to produce, issue and read interoperable smartcards and, most importantly, develop fraud-proof technology and processes to bind both the user and the issuer to the smartcard.

Government mandates are necessitating sweeping changes in the commercial environment as well. A typical supplier importing from overseas may have to deal with Sox, C-TPAT and possibly the U.S. Department of Defense and various retailer mandates related to Radio Frequency Identification (RFID). Section 404 of Sox requires companies to implement controls that protect against

adverse, preventable events that could affect their value, including events within their supply chains. C-TPAT, which requires companies to take responsibility for the security of their own supply chains, is voluntary, but the consensus is that it may soon be mandatory.

In the financial services industry, the Gramm-Leach-Bliley Act of 1999 requires that financial institutions protect the security and confidentiality of customer personal information against “reasonably foreseeable” internal or external threats. Due to recent FFIEC guidance, starting in January 2007, financial institutions will be required to provide consumers of online financial services with the same authentication levels that they experience offline. Thus, online transactions will require two-factor authentication rather than the single-factor authentication of username and password that is predominantly utilized today.

Forces of Collaboration

In terms of collaboration, enterprises now have more partners in their ecosystems than ever before. As major organizations consolidate their procurements, there has been a decline in the average number of suppliers. However, the complexity of these relationships has skyrocketed, with increased interaction and levels of systems integration. The extensive collaboration and data sharing required means organizations must now be even more vigilant — not only about their own security posture, but that of their partners as well. For example, counterfeiting costs pharmaceutical manufacturers \$30 billion annually and poses a significant threat to consumers worldwide. In response, state and Federal authorities are enacting regulations that require pharmaceutical organizations to secure their supply chains. Purdue Pharma worked with Unisys to implement an ePedigree system for self-authenticating medicines, complying with state regulations and for sales tracking in high-value, high-risk supply chains. Clearly, corporate security is only as strong as that of its strategic partners.

Forces of Communications

Recent years have brought about a broad array of new technologies for improving how information is captured, stored and exchanged among computer systems, individuals and organizations. In just a decade, organizations have moved from primarily localized and mostly secure computing infrastructures to the open computer networks — wired and wireless — in use today. This pace of change and degree of openness continues unabated with the regular introduction of new portable storage media, mobile devices and communications protocols. For example, the recent commercial introduction of WiMAX will further increase the power of wireless broadband networks linking computers several miles apart and providing high-speed Internet access for end users. This transition to highly connected computing, wireless technologies and portable storage has brought about powerful capabilities and business benefits with anytime, anywhere access to information and transactions — but it has also brought considerable data security risks.

Nowhere is this risk more critical than with proprietary or classified information. As technologies proliferate and improve the way we conduct business and how we collect, exchange and store information, we should examine these emerging technologies to close the security loopholes they introduce. For consumers, low-cost devices such as removable flash drives can be fast and valuable data transfer and backup solutions — but in the wrong hands, when proprietary or classified data is involved, these devices can represent a significant threat to corporate or national security. Consider the recent and well publicized incident at the U.S. Department of Energy, when operations were temporarily suspended for several days due to misplacement of classified removable electronic media.

Forces of Competition

The need to do more with less has increased the threat level for most companies. Razor thin margins in retail, for example, mean that supply chains must be highly optimized and security investments directed only at the most high-risk areas. Forces of competition also increase the internal threat of employees leaking confidential information outside the corporation to competitors or fraudsters, and boost the external threat of corporate espionage.

Forces of Complexity

The four forces described above have increased the complexity of business operations. The intricacy of today's global supply chains, for example, is daunting. A typical supply chain often involves shipments crossing up to 25 hands between the first and last mile, 75 days of transit time and masses of documentation. Extensive communications are required as information and transactions move beyond the four walls of the corporation and out into the field to support the needs of customers, partners and employees. All this complexity makes it even more difficult for security professionals to effectively ensure the confidentiality, integrity and availability of information and transactions throughout the enterprise and among customers and business partners.

Challenge #2: Responding to Asymmetric Threats

In considering its security posture, private enterprise can learn a great deal from the history of global conflict. Over hundreds of years, military organizations around the globe have had to continually transform themselves to obtain superiority and preparedness against a wide variety of threats. Transformation has been a basic operating principle of warfare since the ages of the bow and arrow. Some of the major transformational developments over history have included the first “iron-clad” ships, the rifle, jet engine, aircraft carriers, stealth fighters, unmanned aerial vehicles, precision-guided munitions, the Internet and network-centric warfare. Each of these technological advances has transformed the way that wars have been fought and provided their inventors with a decided advantage of overwhelming force or capability. In some cases, they have also opened new vulnerabilities that can be exploited via asymmetric warfare.

Today's enterprise is faced with its own version of asymmetric warfare due to threats such as identity theft, phishing, product counterfeiting, data theft, hacking, viruses, denial of service attacks and other forms of assault. An asymmetric threat can attack an organization at any time or place and be directed at its people, its goods or assets, or its technology infrastructure. Like the military, the enterprise must respond and adapt to new threats, continually transforming itself as it moves from a

well-known adversary to attacks that can occur almost randomly at any time and any place, against any target.

In essence, the game has changed, yet we are still fighting the last war. Today's government and commercial organizations need to redefine their security postures to mitigate these risks and ensure business continuity for their global operations. The fragility of global business and its critical infrastructures is often only exposed when business disruptions, lapses in security, natural disasters or acts of terrorism reveal the weakest links. Here are a few recent examples:

Business Disruptions — Recent world events such as the Dubai Port controversy have served to highlight some of the unique challenges related to global trade. Port ownership is just one aspect of the container security issue, and organizations must consider the full end-to-end journey and the people, processes and technology involved because any disruption to global trade can be devastating. In a war game scenario conducted by the U.S. Government, it was estimated that closing the nation's ports for as few as 12 days would lead to a 60-day container backlog and a cost to the U.S. economy of approximately \$58 billion.

Lapses in Security — Government and corporate lapses in security process have also been highly profiled in the media. These lapses include misplaced backup tapes, laptops, documents and electronic media containing sensitive personal data or even information related to national security. According to Information Week, as many as 53 million people — including consumers, employees, students and patients — have had personal data exposed or stolen over the past 13 months.

Acts of Nature — According to the Milken Institute, insurance payouts for Katrina are expected to cost from \$20 billion to \$45 billion — the most for any hurricane cleanup in U.S. history. The final cost to the federal government could reach \$150 billion.

Acts of Terrorism — A study by the New York City Partnership and Chamber of Commerce revealed that the September 11th attacks on the World Trade Center buildings resulted in both direct and indirect costs of approximately \$83 billion (in 2001 dollars) in total losses. In addition to the macro-economic impacts, many industries including securities, retail, restaurants and banking were directly affected.

To ignore these risks and imperatives, or to remain unprepared after these threats have proven to be real, is too costly for both governments and corporations. The impact on a company can be as devastating as the impact on a nation. As the senior executive of a Fortune 50 company has stated: "...if an act of terrorism were committed using one of our containers, we believe it would be a company-ending event."

Challenge #3: Balancing Agility and Assurance

Navigating the delicate balance between the agility necessary for competitive advantage and the assurance of safe, secure operations is a key challenge for governments and businesses worldwide — one that is made even more pressing due to increasing business complexity, multiple regulations and the escalating level of asymmetric threats.

Globalization, decentralization, outsourcing and the Internet have, in effect, created a divide between agility and assurance. Organizations are operating with increased agility, yet their security mechanisms are outdated. Too often, security has been an afterthought layered on top of new and existing applications while processes have been incorrectly applied or not applied at all. Internet and wireless security are just two examples. The ease with which user information has been fraudulently acquired through relatively unsophisticated "phishing" schemes illustrates the challenge of implementing secure business operations in an agile online world.

The type and magnitude of threats to the global supply chain have also changed. Today's supply chains face the possibility of disruptive threats such as terrorism, theft, extreme acts of nature (e.g., Katrina), diversion, counterfeiting, unpredictable acts of governments and even the human factor of supply chain personnel (for example, port operators).

The World Health Organization estimates that five to ten percent of world pharmaceuticals are counterfeit, costing pharmaceutical manufacturers \$30 billion annually and posing a significant threat to consumers worldwide. Product counterfeiting across all global trade now accounts for five to ten percent, or approximately \$350 billion. Theft and diversions affect one to three percent of all goods in the supply chain.

The Secure Business Operation Current State

Today, governments and businesses are challenged to operate efficiently and effectively in harsh environments while trying to maintain a balance between “assured” and “agile” commerce. With threats to business continuity, the need for disaster preparedness and the need for strong risk mitigation and management, it is critical that organizations redefine their security posture if they hope to survive and continue to grow. The challenges within today’s typical enterprise are many:

Disparate security systems

Security solutions have typically grown organically to meet specific needs and often create silos of functionality that are difficult to manage across the enterprise. Often, there are several different solutions implemented even within a specific functional area such as physical access control. End users may need many different credentials to support physical access to facilities and logical access to IT systems. Perimeter security for IT systems is often fragmented across point solutions for anti-virus, firewall and intrusion detection — but a holistic approach is required for effective security information and event management.

Lack of business preparedness across “prevention, detection and reaction”

Enterprises have typically focused on security in terms of installing intrusion detection systems and, more recently, intrusion prevention systems to guard their IT assets. However, the level of preparedness across the continuum of prevention, detection and reaction and across the security pillars of people, goods and assets, and information systems is often varied and uncoordinated. According to the Wall Street Journal, laptop theft is the root cause of many recent identity data exposure incidents. Clearly, this is a serious vulnerability that bypasses standard sophisticated security controls and exposes huge gaps in security policy management and enforcement.

Lack of visibility

Enterprises that cannot track shipments along every step of the distribution chain and proactively identify threats and emerging problems are finding themselves — as well as their brands and customers — at great risk. Lack of visibility, flexibility and security within the supply chain accounts for 8 percent out-of-stock rates on retail shelves; logistics and transportation costs account for 9.5 percent of the U.S. Gross Domestic Product; and lead time from one supply chain node to another varies from 40 percent (by sea) to 95 percent (by air).

Limited public/private collaboration

There is often duplication of effort and expense related to security initiatives because of limited public and private collaboration within and across organizational boundaries. Common concerns include improving the security of national borders, securing and accurately tracking cargo, and protecting the personal data of individuals.

Purely reactive focus on compliance

Most compliance requirements are viewed as a cost of doing business, with organizations adopting a minimal approach. Many vendors use a “slap and ship” approach to retailer and defense-related RFID mandates, tagging shipments for compliance but not leveraging the data for internal supply chain visibility.

Outdated technology infrastructures and applications with limited integration and data exchange

While the threat level has changed, current technologies within the typical enterprise are often outdated and residing in silos. These disparate technologies inhibit ease of integration between systems and impede data exchange. Legacy architectures such as client-server systems operate in their own stove pipes, resulting in fragmented identity and access management solutions. Much of IT innovation has migrated to the edges of the network in terms of new devices and form factors to support information and transactions in the field. Yet, for applications such as sales force automation and field service, the security of those systems is often insufficient or inappropriately applied.

The Secure Business Operation Imperative

Given today's market challenges and the current state of enterprise security, the following secure business operation imperatives are clear.

Security must be holistic

Enterprise security should no longer be defined as simply IT security plus guards, guns and gates. It must be considered holistically across the entire enterprise, from identifying people to tracking and tracing goods and assets, to securing IT systems. People, process and technology must be secured in a coordinated manner driven by a visible, transparent risk management approach that mitigates identified risk across the full spectrum of business operations. In addition, security must be implemented by design from the ground up — not treated as an afterthought layered on top of insecure processes. In the global supply chain, security must address the entire journey from first mile to last mile, across all modes of transportation and between all participants.

Create strategies and operational plans for prevention, detection and reaction

It is not a question of if, but when the typical enterprise will be confronted with a disruptive event. Organizations must plan not just for prevention, but for detection and reaction as well to minimize adverse events and maintain business continuity. Disaster recovery and business continuity planning are critical to a secure business operation.

Visibility is critical

Visibility into enterprise processes can enable both “assured” and “agile” commerce. An enterprise cannot secure what it cannot see or what it doesn't know. For the supply chain, visibility means having a real-time view of the entire supply chain operation to recognize and respond to business events as they occur. Leveraging visibility can lead to significant gains in efficiency, productivity, flexibility and security. Unisys experience shows benefits such as:

- Supply variability reductions of up to 25%
- Lead-time reductions of up to 15%

- Supply chain partner performance improvements of up to 20%
- Increased asset utilization of up to 25%
- Reduced expedited cost by more than 20% up to 80%

Enhance Public/Private Collaboration

To protect against rising threat levels, greater public/private collaboration and greater internal collaboration are necessary. C-TPAT and the Container Security Initiative are successful models of how business and government can work together to support homeland security. With more than 7,000 members, C-TPAT now works with the trade industry to emphasize a seamless security-conscious environment throughout the entire commercial process. It is the federal government's largest public/private partnership in U.S. history. Enterprises need to establish such levels of collaboration as well. It is essential that organizations introduce processes to share data among their security, purchasing and supply chain departments to gain a clear understanding of the most vulnerable aspects of their operations.

Take a proactive stance and look beyond compliance for competitive advantage

Compliance requirements are viewed as a cost of doing business, and organizations consequently adopt a minimal approach. Initiatives to support compliance should also be evaluated for opportunities to leverage the investment for innovation and growth. Rapidly mastering compliance guidelines or recommendations before they become mandates can help organizations focus on their core business while their competition struggles to comply. A proactive approach can also help identify security and privacy concerns before they occur. In addition, an investment in compliance can often be leveraged for improved visibility and operational efficiency. RFID is an excellent example. RFID tags for smart containers can improve container security — but they can also deliver economic benefits for importers, improve supply chain efficiency and increase the potential for streamlined clearances at customs.

Leverage emerging technologies and new business models for secure business operations

New technologies and business models can be valuable enablers for redefining an organization's security posture and improving business operations. Emerging technologies such as RFID, GPS, Satellite and GIS can enhance visibility into global supply chains and improve security. Real-time infrastructures can facilitate total information awareness, support government reporting and ensure compliance with mandates. Outsourcing of non-core competencies such as security information and event monitoring functions to managed security service providers can free organizations to focus on their core business. Emerging identity federation standards will allow higher levels of secure access control between business and government partners, as evidenced by the successful standards-based approach to federated security that Boeing and Southwest Airlines have implemented.

Redefining your security posture by applying these business operation imperatives can help you mitigate your risk to exposure while leveraging security for business growth and innovation.

The Unisys Value Proposition

Enterprises today need a holistic approach to security — one that combines management and process expertise based on industry standards with technological skill and operational excellence.

An approach that views security policies, procedures and technology as more than just a way to protect against the occurrence of unwanted events, but also as a means of reducing organizational costs, improving operations, and enabling new business opportunities.

An approach that focuses on creating the visibility required to be proactive rather than reactive.

We call this approach Secure Business Operations. It's based on the seemingly simple premise that you can't secure what you can't see. Yet it requires an in-depth understanding of the many facets of security, the industry in which you operate, and the methodologies and tools that can provide the visibility you need to make the right security investment decisions.

Whether you are protecting physical and IT infrastructures; addressing concerns about privacy and identity theft; controlling access to government benefits, physical or logical resources; participating in e-business initiatives; complying with governmental regulations; tracking goods and assets; securing your supply chain — or all of the above — **you need visibility to effectively manage your security risk.**

This is the critical difference between delivering security and ensuring secure business operations — the ability to visualize the different elements of your environment, understand the causal relationships and take the appropriate steps to maximize your security investments.

In both the public and private sector, organizations around the globe need to focus their attention on operational efficiency and planned profitable growth — rather than constantly worrying about the continuity, integrity and security of their operations. They need the knowledge gained from visibility that enables them to focus on their core activities. **After all, how can you secure what you can't see? Or expand your business without worrying about the security implications?**

Unisys Secure Business Operations encompasses a comprehensive approach to security that leverages our investment in 3D Visible Enterprise (3D-VE) — a methodology for uncovering even the deepest, most remote cause-and-effect relationships throughout an organization. 3D-VE shows decision makers the correct paths forward and — equally important — the critical gaps that can block effective execution.

Secure Business Operations also incorporates our deep security expertise across a broad range of disciplines, industries and enterprises, large and small. At Unisys, our global security operations centers handle more than 300 million security events per day, and we are rated the #1 systems integrator in Gartner's latest Managed Security Services Provider Magic Quadrant based on our ability to execute — including our expertise in security event management. We are delivering global visibility with the world's largest RFID network supporting the U.S. Army warfighter. We've also designed and implemented multiple national identification programs, including the Malaysia MyKad multi-purpose smart card and the South African

Home Affairs National Identification System (HANIS), which includes one of the largest civilian fingerprint databases ever built. Our Identification and Credentialing practice professionals are considered leading experts in the areas of identity repositories; authentication and access control; and provisioning and credential management. And our secure supply chain experience includes the U.S. Army and the Operation Safe Commerce initiative. Unisys areas of security focus include:

Identification of People and Systems

At Unisys, we implement traditional computer security services such as complex directory services, automated provisioning systems, single sign-on, role-based access controls or federated environments. We also implement national identification and voter registration solutions for citizens; registered traveler systems for frequent commuters; and advanced access management solutions for employers.

Track and Trace Goods and Assets

At Unisys, we don't just operate and maintain the U.S. Army's secure supply chain, ensuring deployment of cargo and equipment to the U.S. warfighter in austere and dangerous environments. We also manage a system to track containers through global ports, providing an anti-counterfeiting solution to a pharmaceutical company. And we track goods and assets as mundane as computer tapes and currency.

Secure Data and Infrastructure

At Unisys, we don't just implement technologies to thwart cyber attacks against enterprise networks and applications. We also make business sense out of the attack information to help you manage risk and address regulatory compliance.

Interoperate Voice and Data

At Unisys, we didn't just provide secure wireless communications to U.S. Government agencies on the ground during the 9/11 attacks. We also provided secure communications hubs to the City of New Orleans after Hurricane Katrina.

The Secure Business

From government organizations as large as the U.S. Department of Homeland Security to small local banks, businesses around the world seek out Unisys for our security know-how.

Only Unisys combines extensive systems integration, outsourcing and security consulting, design, implementation, monitoring and management expertise with 3D-VE to ensure secure business operations.

About Unisys

Unisys is a worldwide technology services and solutions company. Our consultants apply Unisys expertise in consulting, systems integration, outsourcing, infrastructure and server technology to help our clients achieve secure business operations. We build more secure organizations by creating visibility into clients' business operations. Leveraging Unisys 3D Visible Enterprise, we make visible the impact of their decisions — ahead of investments, opportunities and risks. For more information, visit www.unisys.com/systems/security.

For more information, please visit our Website at:
www.unisys.com/public_sector

Specifications are subject to change without notice.

© 2006 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

