

Testimony Of

THOMAS PARENTY

**DIRECTOR, DATA AND COMMUNICATIONS
SECURITY**

SYBASE, INC.

On Behalf Of The

**BUSINESS SOFTWARE
ALLIANCE**

**IMMEDIATE NEED FOR RELAXATION OF
EXPORT CONTROLS FOR SOFTWARE AND
HARDWARE WITH ENCRYPTION
CAPABILITIES**

Before The

**COURTS AND INTELLECTUAL PROPERTY
SUBCOMMITTEE**

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

Washington, D.C.

March 4, 1999

**SUMMARY OF STATEMENT OF THOMAS
PARENTY**

**DIRECTOR, DATA AND COMMUNICATIONS
SECURITY, SYBASE, INC.**

BSA strongly supports the Security and Freedom through Encryption ("SAFE") Act (H.R. 850) because it ensures that all Americans may use and sell any encryption domestically and provides badly needed export control relief.

Congress must immediately relax export controls on software and hardware with encryption capabilities. Widespread deployment of American products with encryption capabilities will help to accelerate dramatically the growth of electronic commerce by protecting consumers' privacy and preventing

electronic crime. Export control relief also is vital for protecting America's critical infrastructures and ensuring that American software and hardware companies remain not only internationally competitive but also the market leaders in both software and hardware products.

The Administration took the first step towards developing a sensible long-term encryption policy by permitting exports of select products to select users, but they still have not gone far enough. A successful encryption policy must be based on technological and market realities. It must recognize that:

- The worldwide standard is 128-bit encryption;
- Mass market software and hardware is uncontrollable; and
- It is in America's national and economic security interests to have American designed and manufactured encryption products deployed worldwide.

Without relaxation of export controls, U.S. manufacturers remain at a competitive disadvantage, and foreign consumers will purchase encryption products from foreign suppliers.

Foreign products are comparable in capabilities and quality. When a foreign purchaser cannot obtain an American product they simply purchase it from a foreign supplier. Unfortunately, not only are American companies losing a sale of an encryption item, but they are also losing the sale of the program or hardware such as an Internet server or an application browser that uses the encryption capability. In fact, companies risk losing sales of entire systems because of their inability to provide necessary security features. The only impact of the Administration's export policy is widespread deployment of foreign designed and manufactured software and hardware.

The SAFE Act recognizes that the United States should not try to control uncontrollable exports of mass

market and public domain software and hardware. It also permits exports of 128-bit level custom software and hardware. At the same time, the SAFE Act prohibits the government from mandating the use of key escrow, key recovery or recoverable encryption or requiring Americans to use key escrow, key recovery or recoverable encryption if they want to use an electronic signature. Ultimately, the SAFE Act will help Americans to use encryption to protect privacy, prevent crime and protect our national security.

Introduction

Good Morning. My name is Thomas Parenty, and I am the Director of Data and Communications Security for Sybase, Inc. In this capacity, I am responsible for all security-related product development for one of the ten largest software companies in the world. I have been active in the cryptography and computer security field for over 15 years, including my tenure at the National Security Agency (NSA) in the early to mid-eighties.

While at the NSA, I advised the Director of the NSA on internal NSA computer security issues and worked on the security of global nuclear command and control networks, focusing on the formal verification of cryptographic protocols and internal computer security controls. Because of my specialized security knowledge, I worked on national security-related, compartmentalized programs at other government agencies during my service at the NSA. In addition, I have worked on the security design of operating systems, networks and database management systems for government agencies, including the Central Intelligence Agency, the Defense Intelligence Agency, the Air Force, as well as many U.S. computer vendors. Most recently, I served as an advisor to the President's Commission on Critical Infrastructure Protection, specifically addressing the needs of the telecommunications and banking infrastructures. I am also a member of the National Research Council's panel on information technology.

Headquartered in Emeryville, California, Sybase, Incorporated, is a worldwide leader in distributed, open

computing solutions with revenues in 1998 of over \$ 800 million. We provide customers and partners with the software and services to create business solutions for strategic, competitive advantage. These high-performance, end-to-end solutions encompass client/server, Internet and intranet transaction processing and data mart and data warehousing applications. Sybase's Adaptive Component Architecture™ enables rapid design, development and deployment of distributed multi-tier business applications. Our product lines include Sybase high-performance database servers, EnterpriseConnect™ distributed data access and connectivity products, and Powersoft open business development tools.

I greatly appreciate the opportunity to appear today before this Committee on behalf of Sybase and the Business Software Alliance (BSA). Since 1988, BSA has been the voice of the world's leading software developers before governments and with consumers in the international marketplace. BSA promotes the continued growth of the software industry through its international public policy, education and enforcement program in 65 countries throughout North America, Europe, Asia and Latin America. Its members represent the fastest growing industry in the world. BSA worldwide members include Adobe, Attachmate, Autodesk, Bentley Systems, Corel Corporation, Lotus Development, Microsoft, Network Associates, Novell, Symantec and Visio. Additional members of BSA's Policy Council include Apple Computer, Compaq, Intel, Intuit and my company, Sybase. BSA websites: www.bsa.org; www.nopiracy.com.

But we really are here today to speak on behalf of the tens of millions of users of American software and hardware products. The American software and hardware industries have succeeded because we have listened and responded to the needs of computer users worldwide. We develop and sell products that users want and for which they are willing to pay.

One of the most important features computer users are demanding is the ability to protect their electronic information and to interact securely worldwide. American companies have innovative products which

can meet this demand and compete internationally. But there is one thing in our way — the continued application of overbroad, unilateral, export controls by the U.S. Government.

The Security and Freedom through Encryption (SAFE) Act, H.R. 850, modernizes U.S. export laws regarding software and hardware with encryption capabilities to permit American companies to compete on a level international playing field and to provide computer users with their choice of adequate protection for their confidential information and critical infrastructures.

For these reasons, BSA strongly supports the SAFE Act. We urge the Committee to report the SAFE Act unamended and look forward to its passage by the House early this year.

We want to pay tribute to the tremendous efforts of Representatives Goodlatte and Lofgren in championing this legislation, as well as thank both you, Mr. Chairman, and Mr. Frank and the other Subcommittee members who were among the 205 original cosponsors of the SAFE Act.

This morning I want to make three points:

- Widespread deployment of encryption is not only desirable, it is critical;
- America's export policy should promote widespread deployment of products with encryption capabilities in the worldwide market; and
- BSA strongly supports the SAFE Act because it provides freedom for Americans to use and sell any encryption domestically and provides greatly needed export control relief.

Widespread Deployment Of Encryption Is Not Only Desirable, It Is Critical

Confidential Information And Secure Networks In The Internet Age

Are The Key To Privacy And

Commerce

American individuals and companies are rapidly becoming networked together through private local area networks (LANs), wide area networks (WANs) and public networks such as the Internet. Combined, these private and public networks are the economic engine driving electronic commerce, transactions and communications. This engine is being choked by the lack of availability of strong encryption products.

Traffic on the Internet doubles every 100 days. Predictions of business-to-business Internet commerce for the year 2000 range from \$66 billion to \$171 billion, and by 2002, electronic commerce between businesses is expected to reach \$300 billion. During 1997, one leading manufacturer of computer software and hardware sold \$3 million per day online for a total of \$1.1 billion for the year.

More and more individual consumers also are going on line and spending. More than 10 million people in North America alone have purchased something over the Internet and at least 40 million have obtained product and price information on the Internet only to make the final purchase off-line. Imagine the boost in volume of e-commerce if all of these consumers had enough confidence in the security of the Internet to purchase on-line.

Yet in 1996 the Computer Security Institute/FBI Computer Crime Survey indicated that our worldwide corporations will be increasingly under siege: over half from within the corporation, and nearly half from outside of their internal networks.

Network users must have confidence that their communications and data — whether personal letters, financial transactions or sensitive business information — are secure and private. Electronic commerce is transforming the marketplace — eliminating geographic boundaries and opening the world to buyers and sellers. Companies, governments and individuals now realize that they can no longer protect data and communications from others by relying on limiting physical access to computers and maintaining

stand-alone centralized mainframes. Instead, users expect to be able to pick up their e-mail or modify a document from any computer anywhere in the world simply by using their Internet browsers. Thus, consumers worldwide are demanding to be able to protect their electronic information and interact securely worldwide, and access to products with strong encryption capabilities has become critical to providing them with confidence that they will have this ability.

***Full Deployment Of Strong Encryption
Is Vital For Protecting***

America's Critical Infrastructures

Governments also are recognizing that without encryption, the electronic networks that control such critical functions as airline flights, health care functions, electrical power and financial markets remain highly vulnerable. The U.S. General Accounting Office in its report issued in May of 1996 entitled *"Information Security: Computer Attacks at Department of Defense Pose Increasing Risks"* found that computer attacks are an increasing threat, particularly through connections on the Internet, such attacks are costly and damaging, and such attacks on Defense and other U.S. computer systems pose a serious threat to national security.

As the President said on January 22, 1999, before the National Academy of Sciences, "[w]e must be ready — ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services — or military assets. More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption."

The President has been so concerned that he established a Commission on Critical Infrastructure Protection to provide him with guidance and issued two Presidential Directives based on the Commission's recommendations.

In the Report of the President's Commission on Critical Infrastructure Protection entitled *Critical Foundations: Protecting America's Infrastructures* (October 1997), the Commission emphasized that "Strong encryption is an essential element for the security of the information on which critical infrastructures depend." In fact "[p]rotection of the information our critical infrastructures are increasingly dependent upon is in the national interest and essential to their evolution and full use. A secure infrastructure requires the following:

- Secure and reliable telecommunications networks.
- Effective means for protecting the information systems attached to those networks. . . .
- Effective means of protecting data against unauthorized use or disclosure.
- Well-trained users who understand how to protect their systems and data."

An earlier blue ribbon National Research Council (NRC) Committee similarly concluded in its (May 1996) CRISIS Report ("Cryptography's Role in Securing the Information Society") that encryption promotes the national security of the United States by protecting "nationally critical information systems and networks against unauthorized penetration."

Thus, the NRC Committee found that on balance the advantages of widespread encryption use outweighed the disadvantages and that the U.S. Government has "an important stake in assuring that its important and sensitive . . . information . . . is protected from foreign government or other parties whose interests are hostile to those of the United States."

Information security is critical to the integrity, stability and health of individuals, corporations and governments. While cryptography is but one element

of security, it is the keystone of secure, distributed systems. Frankly, there is no substitute for good, widespread, strong cryptography when attempting to prevent crime and sabotage through these networks. The security of any network, however, is only as good as its weakest link. America's infrastructures cannot be protected if they are networked with foreign infrastructures using weak encryption.

U.S. unilateral export controls have also had a significant impact on the availability of strong American encryption domestically, which is ultimately harming the American consumer. The U.S. software and hardware industry makes at least one-half of its revenues through exports. For this reason and due to the significant difficulties companies encounter selling foreign purchasers a weaker version of an encryption product, some software companies have offered products with the same encryption capabilities both domestically and abroad. Therefore, the American consumer has fewer strong American encryption products to choose from than they would without U.S. export controls. The American consumer is ultimately left with an unfortunate choice: they may either buy strong encryption which they cannot use internationally, or they may simply purchase strong foreign encryption products that are not subject to U.S. export controls. Neither choice is the best for protecting America's critical infrastructures.

In the long-term, we believe it is in America's best interest to have America's critical infrastructures and national security be protected by widespread reliance on strong American encryption products both here and abroad.

***Relaxed Export Controls On
Encryption Products Is Vital For
Ensuring***

America's Global Competitiveness

American companies do have exciting and innovative products that can meet the demand for 128-bit encryption and compete internationally. But unless the current unilateral U.S. export restrictions are changed

to allow the use of strong encryption, American individuals and businesses will not be active participants in this new networked world of commerce — let alone continue to be the leaders in its development. Furthermore, American companies will no longer be providing the world, and its critical infrastructures, with the answers to their security problems. Instead foreign companies will. It is unclear how U.S. national security or law enforcement will be aided or how our critical infrastructures will be secure when foreign encryption products dominate the world market.

The computer software and hardware industries are American success stories, but they are being threatened. America's software and hardware industries are important contributors to U.S. economic security — now and in the future. Information technology industries are now directly responsible for over one-third of real growth of the U.S. economy. Between 1980 and 1992, the computing and software industry grew at an annual rate of over 28%, while overall domestic growth was less than 3%. From 1990 through 1996, the software industry grew at a rate of 12.5%, nearly 2.5 times faster than the overall U.S. economy.

More than 7 million people work in IT industries. In 1996, the software industry provided a total of over 619,000 direct jobs and \$7.2 billion in tax revenues for the U.S. economy. The software industry is expected to create an average of 45,700 new jobs each year through 2005. If piracy were to be eliminated in the United States, the number of new software jobs created would double to an average of 93,000 a year.

Moreover, the computer software industry has achieved tremendous success in the international marketplace with global sales of packaged (*i.e.*, non-custom) software reaching over \$118.4 billion in 1996, and rising to \$135.4 billion in 1997. American produced software accounts for 70% of the world market, with exports of U.S. programs constituting half of the industry's output.

The incredible growth of the industry and its exporting

success benefits America through the creation of jobs here in the United States. Many of these jobs are in highly skilled and highly paid areas such as research and development, manufacturing and production, sales, marketing, professional services, custom programming, technical support and administrative functions. In the U.S. software industry, workers enjoy more than twice the average level of wages across the entire economy — \$57,319 versus \$27,845 per person.

All of these revenues and jobs are dependent upon American software and hardware producers remaining the market leaders around the world, especially as the major growth markets continue to be outside the United States. Strong export controls on products with encryption capabilities are crippling the ability of these companies to compete with foreign providers.

**America's Export Policy Should Promote
Widespread Deployment Of American Products
with Encryption Capabilities In The Worldwide
Market**

As embodied in the SAFE Act, the most successful encryption policy will ensure that Americans can use and sell any encryption that they want domestically, prohibit both Federal and State governments from imposing encryption standards or techniques, and relax export controls on products with encryption capabilities in a manner that is based on technological and market realities. Just because law enforcement and national security interests wish that they could turn back the clock and limit consumers access to strong encryption approved by the government, it will not happen, especially on a worldwide basis. This is especially true for mass market software and hardware, which by its inherent nature is uncontrollable.

***The Administration Took The First
Step Towards Developing A Sensible
Long-Term Encryption Policy, But
They Still Have Not Gone Far Enough***

The BSA members welcomed the Administration's

efforts to relax export controls on select products used by select users. However, the Administration's actions are merely a first step. A truly successful, sensible encryption policy would be based on technological and market realities, and would not create winners and losers in the encryption marketplace on a sector-by-sector basis. It would recognize that:

- The worldwide encryption standard is 128-bit encryption;
- Mass market software and hardware is inherently uncontrollable; and
- It is in America's national and economic security interests to have American designed and manufactured encryption products deployed worldwide.

Moreover, we believe it is preferable for Congress to put encryption policy on a statutory basis — sending a strong message around the world that encryption is important for a strong defense, for protecting the privacy of citizens and for preventing crime.

Unilateral U.S. Export Controls Harm American Interests

Currently, there are no restrictions on the use of cryptography within the United States. However, the U.S. Government maintains strict *unilateral* export controls on computer products that offer strong encryption capabilities.

American companies are forced to limit the strength of their encryption to the 56-bit key length level set late in 1998. The recently announced regulations will also permit companies to export stronger encryption on a sector-by-sector, user-by-user basis. However, this policy ignores the fact that:

- The minimum strength now required by new Internet

applications is 128-bit encryption;

- The most widely used encryption program, PGP, with over two million users worldwide, uses the Swiss developed IDEA encryption algorithm, with a 128-bit key;
- American companies cannot export encryption products to a vast majority of non-U.S. commercial entities. Foreign manufacturers provide 128-bit encryption alternatives and add-ons — filling the market void created by U.S. export controls;
- Providing sector-by-sector relief is unworkable for mass market products and does not reflect commercial realities for sales of custom products; and
- 56 bit encryption has been demonstrated to be vulnerable to commercial let alone governmental attack. (In the beginning of this year at the RSA Encryption Conference, a 56-bit DES encoded message was broken by private companies and individuals working together in 22 hours and 15 minutes — imagine what a hostile government with serious resources could do.)

Export controls also have made American companies less competitive and opened the door for foreign software and hardware developers to gain significant market share —decreasing our national and economic

security.

I want to take one minute to discuss the Wassenaar Arrangement at this point. Please do not be fooled by any claims from the Administration that the Wassenaar Arrangement is the multilateral agreement on encryption that they have been touting was just around the corner for the past several years.

The Wassenaar Arrangement was an agreement among only 30 countries, and it actually decontrolled encryption products. Many countries, such as Israel and South Africa, who export strong encryption are not signatories to the Arrangement. The Wassenaar Arrangement eliminated controls of any sort on 56-bit encryption and permits exports of up to 64-bit encryption in mass-market software and hardware. It also removed any reporting requirements — the sole official means for actually monitoring what countries are doing. Although the Arrangement left open the possibility that countries might individually control 128-bit encryption, we are skeptical that they will do so. There is no penalty for failing to control 128-bit encryption, and most countries are actually moving towards encouraging the use of stronger encryption. Finally, a country could technically comply with the Arrangement, while still permitting easy exports of strong encryption.

Even France, traditionally the country which placed the greatest restrictions on its own citizens by limiting them to the easily broken 40-bit level of encryption, has recognized that technology has progressed. Near the end of 1998, France relaxed controls on the domestic use of encryption and is now permitting, and in fact encouraging, the use of 128-bit encryption by its citizens.

Without Export Relief, Foreign Consumers Will Purchase Their Products From Foreign Suppliers, Keeping U.S. Manufacturers At A Competitive Disadvantage

As a result of U.S. unilateral export controls, encryption expertise is being developed off-shore by

foreign manufacturers who now provide hundreds of encryption alternatives and add-ons. The Administration's export controls are in no way preventing foreigners, let alone those with criminal intent, from obtaining access to encryption products. In fact, foreign software and hardware manufacturers have seized the opportunity to create sophisticated encryption products and to capture sales.

As long ago as 1995, the General Accounting Office confirmed that sophisticated encryption software is widely available to foreign users on foreign Internet sites. In 1996, a Department of Commerce study again confirmed the widespread availability of foreign manufactured encryption programs and products. An on-going industry study by Trusted Information Systems (TIS Study) highlights the ever-increasing availability of foreign developed and manufactured products as it discovered there were 656 foreign programs and products available from 29 countries as of December 1997.

Further demonstrating the worldwide availability, use and sophistication of encryption abroad is the Department of Commerce's National Institute of Standards and Technology (NIST) efforts to work with the private sector to develop an Advanced Encryption Standard (AES). Individuals and companies from eleven different countries proposed 10 out of the 15 candidate algorithms submitted to NIST: Australia's LOKI97; Belgium's RIJNDAEL; Canada's CAST-256 and DEAL; Costa Rica's FROG; France's DFC; Germany's MAGENTA; Japan's E2; Korea's CRYPTON; and the United Kingdom, Israel and Norway's SERPENT algorithms. Only 5 out of the 15 candidate algorithms were submitted by U.S.-based individuals or companies.

The impact of lost sales is enormous. If an encryption product is combined with other applications such as Internet browsers and application servers, U.S. companies will generally lose both sales. In fact, companies risk losing sales of entire systems because of inability to provide necessary security features. This permits foreign manufacturers to gain entry into companies as well as gain credibility — providing the

foreign manufacturers with further opportunity to take away future sales in the same and other product lines.

I would like to mention a few specific examples with respect to foreign availability of encryption products. The Apache Group, based in the U.K., announced in April 1997 that its Apache Unix Internet Server software with very strong encryption had a 29% market share of Web server software. Today the Apache web server serves over half — 50% — of the domains on the Internet.

Companies such as Brokat Informationssysteme, a German company, are developing products that are more than simply add-ons to American products. Brokat's modular e-services platform, Twister, which companies use to offer their customers secure and simple electronic services via various electronic channels, such as the Internet or mobile communications networks, is already being used by more than 1,500 companies worldwide. Brokat's sales outside of Germany, including to the United States, have now increased to be 56 percent of the company's total sales. The American market research institute Meridien Research described BROKAT as the leading company worldwide for Internet banking solutions.

The merger of two foreign companies, Zergo Holdings (U.K.) and Baltimore Technologies (Ireland), into a new company called Baltimore only further illustrates that foreign companies are flourishing solely because there is no U.S. competition. According to the Gartner Group in a Research Note dated January 28, 1999, the new company is "a competitive participant in providing e-commerce and enterprise security, with 11 international offices and a global partner network . . . with customers in 40 countries."

***U.S. Encryption Export Controls Hurt
American Companies***

***Without Helping Law Enforcement Or
National Security***

U.S. export controls have had the effect of creating an encryption expertise outside the United States that is

gathering momentum. Unfortunately, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies lose. We believe that continuing down this path will be ultimately more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

In fact, as long ago as 1996, the NRC Committee concluded that as demand for products with encryption capabilities grows worldwide, foreign competition could emerge at levels significant enough to damage the present U.S. world leadership in information technology products. The Committee felt it was important to ensure the continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including American computer, software and communications companies. Correspondingly, the Committee called for an immediate and easy exportability of products meeting general commercial requirements — which is currently 128-bit level encryption!

To summarize:

- Foreign competitors not subject to outdated U.S. export controls are ready to take sales and customers from U.S. companies today.
- Complex and cumbersome U.S. export controls make American companies less competitive. They significantly increase the costs of developing, marketing and selling products with encryption capabilities, delay the introduction of new products or features, and encourage foreign customers to purchase

- from foreign suppliers due to the uncertainty and delay in obtaining a comparable American product.
- Current export controls do not keep strong encryption out of the hands of foreign customers; they just keep U.S. products out of their hands.

BSA Strongly Supports The SAFE Act Because It Provides Freedom For Americans

To Use And Sell Any Encryption Domestically And Provides Greatly Needed

Export Control Relief

The SAFE Act Preserves Americans' Domestic Encryption Freedom

The SAFE Act ensures that Americans may use and sell whatever kind of encryption they want domestically. It ensures that the U.S. government may not require or provide other incentives for Americans to use encryption products "approved" by the government or meeting certain standards. Also, the Act does not permit the government to link electronic signatures to the use of certain types of encryption products.

The SAFE Act Provides Law Enforcement With Important Safeguards

Importantly, the SAFE Act does permit the Secretary of Commerce to continue preventing exports to countries of terrorist concern or other embargoed countries pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act.

The bills also contain safeguards when relaxing export controls for strong encryption products — the Secretary of Commerce is not required to permit such

exports if there is substantial evidence that the software or hardware will be diverted or modified for military or terrorist use or re-exported without requisite U.S. authorization.

The SAFE Act Recognizes That Mass Market Products Are Uncontrollable And Should Be Exportable

U.S. export controls still ignore the realities of mass-market software and hardware distribution. Mass-market hardware manufacturers and software publishers sell products through multiple distribution channels such as OEMs (*i.e.*, hardware manufacturers that pre-load software onto computers), value-added resellers, retail stores and the emerging channel of on-line distribution. Thus, mass market products are available to the general public from a variety of sources.

The mass-market distribution model presupposes that hardware manufacturers and software publishers will take full advantage of these multiple channels to ship identical or substantially similar products worldwide (allowing only for differences resulting from localization) irrespective of specific customer location or characteristics.

Uncontrollable products at 56-bits cannot suddenly become controllable products at 128-bits. The SAFE Act recognizes as a fundamental proposition that the United States should not try to control the export of something that is, by its very nature, uncontrollable. Trying to control the uncontrollable squanders the limited resources of companies trying to comply with unrealistic export controls as well as the resources of the government as it tries to enforce unenforceable export controls, undermining the credibility of the entire system of export controls.

The SAFE Act Permits Exports Of Custom Hardware And Software

The SAFE Act ensures that if strong encryption products have been permitted to be exported to foreign banks, then custom software and hardware

with comparable encryption capabilities should be exportable to other foreign commercial purchasers in that country. The U.S. should not control exports of competitive custom products embodying world encryption standards. Note that the type of software and hardware we are talking about here is a "custom" product (if it were generally available it would not need an individual license under the bill's other provisions).

The Time For Action Is Now

To keep American vendors on a level international playing field and American computer users adequately protected, U.S. export controls must be immediately updated to reflect technological and international market realities.

Thank you.