



Cyber Security Export Market: Republic of Korea 2014

Sponsored by the Virginia Economic Development Partnership's (VEDP)
Going Global Defense Initiative

George Mason University (School of Public Policy)

This study was prepared under contract with the Commonwealth of Virginia, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the Commonwealth of Virginia and does not necessarily reflect the views of the Office of Economic Adjustment.

Virginia loves Exports 





CONTENTS

EXECUTIVE SUMMARY	3
CYBER SECURITY MARKET	4
CYBER ATTACKS	4
CYBER SECURITY TRENDS: TECHNOLOGICAL ENVIRONMENT	4
MARKET SECTORS AND OPPORTUNITIES	4
COMMAND STRUCTURE OF THE CYBER SECURITY SECTOR	5
MARKET ACCESS	6
POLITICAL ENVIRONMENT	6
SAFETY AND SECURITY	7
TRADE AGREEMENTS	7
IMPORT AND EXPORT REGULATION	8
GOVERNMENT PROCUREMENT AGREEMENT	8
GOVERNMENT PROCUREMENT	8
DEFENSE PROCUREMENT	9
DOING BUSINESS WITH GOVERNMENT	9
TENDER RISK	9
MARKET SIZE AND GROWTH	10
DEFENSE SPENDING	10
CYBER SECURITY MARKET SIZE	10
COMPETITIVE MARKET LANDSCAPE	10
MARKET ENTRY	11
AGENTS	11
PARTNERS	11
SETTING UP AN OFFICE	11
LEGAL ISSUES	12
INTELLECTUAL PROPERTY RIGHTS	12
TENDER LAWS	12





CONTENTS

ECONOMIC ENVIRONMENT.....	12
SOCIO- CULTURAL ENVIRONMENT	13
PRIVATE SECTOR DEMAND.....	13
APPENDIX 1: USEFUL LINKS	16
APPENDIX 2: KEY CONTACTS IN SOUTH KOREA	17
REFERENCES	18



EXECUTIVE SUMMARY

- » South Korea, also called the Republic of Korea, (ROK), offers United States (US) based cyber security companies many competitive export opportunities. It is a country that leads the world in Internet use and high-speed access but currently lacks the infrastructure to protect it.
- » Recent costly security breaches have created a demand for the deployment of cyber security solutions to protect South Korea's home base of global companies and the government's critical data. South Korea's government and military have developed policies and budgets to combat this complex evolving problem.
- » Its location next to North Korea creates continuous threats, minimized with US commitment of military personnel and financial aid. North Korea is also blamed for most of the cyber-attacks on both the private and public sector.
- » South Korea hosts the eighth largest military defense industry in the world. Focused on establishing a competent force and modernizing infrastructure, [The Ministry of National Defense \(MND\)](#) recently announced a continuation of its plans to procure sophisticated technology for modernization and advancement.¹
- » The South Korean Government has published plans to spend \$8.76 billion by 2017 creating a huge growth market for cyber security.
- » US exporters that produce sophisticated and innovative products are more likely to succeed in the Korean market: for example in bio-recognition systems and internet security. Consulting and training companies also have opportunities in the cyber security area.
- » South Korea is US-friendly and offers open and flexible trade policies. A South Korea- US bilateral trade agreement signed in 2013 provides even more advantages of lower tariffs for US companies.

¹ (Ministry of National Defence, 2010 Defense White Paper, Republic of Korea)

CYBER SECURITY MARKET

CYBER ATTACKS

South Korea is a target for cyber-attacks due to its high network connectedness, advanced use of mobility, significant intellectual property, and economic growth. “Cyber defense capability has emerged as vital to national security due to an increasing number of cyber-attacks against major infrastructures,” said Kim Myung-chul, dean of Korea Advanced Institute of Science and Technology’s Graduate School of Information Security.

From June 25 to July 1 2013, a series of cyber-attacks paralyzed 69 government offices, news outlets and other institutions, including the President’s office website. The hackers stole the personal data of 2.5 million members of the ruling Saenuri Party, 300,000 military personnel and 200,000 registered users of the presidential office’s website.

The Korea Internet Security Agency, (KISA), said it had recorded 40,000 cases of cyber-attacks from foreign and domestic sources in 2012, up sharply from 24,000 in 2008. KISA’s research shows that 53 percent of hacking sources originated in China with North Korea suspected in many others. In 2012, Panda Labs security reported that South Korea also has the highest percentage of infected personal computers (PC). South Korea’s PC infection rate was 57.3 percent for the second quarter, followed by China with 52 percent and Taiwan at 42 percent. This compares with the global average PC infection rate of 31.6 percent. Clearly, the need for cyber security remains high in the nation.

CYBER SECURITY TRENDS: TECHNOLOGICAL ENVIRONMENT

South Korea is a global leader in technology and global trade. Around 82.5 percent of South Korea's population had Internet access as of June 2012. It experienced a growth in average connection speeds of 25 percent, according to Akamai, a US based information technology (IT) cloud provider. South Korea also leads the world in mobile broadband penetration rates with over 55,049,000 mobile users* in Q4 of 2012. It joins Finland, Sweden, and Australia with more than one mobile subscription per person.²

According to the World Bank, South Korea’s government is investing in research and development in nanotechnology, biotechnology and other IT areas to remain at the forefront of technology. Seoul is creating research parks to create synergy between universities and key industries for greater industry expansion.

While South Korea can boast of the most wired, fastest Internet, and most mobile users, it also has an insecure infrastructure. Both the government and the private sector are concerned with this problem. [KISA](#) (Korea Internet Security Center) states that 73 percent of domestic companies spend no money on data protection because “there’s no immediate return” on their investment.

MARKET SECTORS AND OPPORTUNITIES

South Korea offers a niche market for cyber security products and services. US exporters that produce sophisticated and innovative products are more likely to succeed in the Korean market: for example bio-recognition systems and internet security. Consulting and training companies also have opportunities in the cyber security area.³

² (Top-20-where-to-find-the-worlds-fastest-internet. 2013)

* (These figures include both contract and pre-paid connections.)

³ (US ITA Safety and Security Guide, 2013)

The two industries, which offer the largest cyber security markets within South Korea, include the defense and the financial sectors. South Korea houses the eighth largest military, after China, the US, India, North Korea, and Russia, and is growing faster than the regional average.⁴

South Korea's defense industry is focused on both establishing a competent force and modernizing its infrastructure. [The Ministry of National Defense \(MND\)](#) recently announced that there would be continuation of its plans to procure sophisticated technology for modernization and advancement.⁵

The financial sector, another key cyber market, is currently attempting to further develop and evolve because it has not kept pace with private sector growth. Publicized cyber-attacks further erode future growth making it important to protect the banking infrastructure.⁶

Together, the Defense Ministry and the Financial Services Commission have introduced new policies and regulations to avert cyber-attacks but are having difficulty in getting them implemented. South Korea's recent attempt to set policy and law that would have required on line users to authenticate with national identity was voted unconstitutional days after it was passed due to privacy concerns. South Korea along with all countries is struggling with how to deal with privacy issues.

COMMAND STRUCTURE OF THE CYBER SECURITY SECTOR

A National Security Council (NSC) was established to oversee 15 different agencies that influenced cyber security in the protection of land, sea, and air. It is responsible for setting policy to identify, prevent, and respond to cyber-attacks. NSC works with the private and military sectors to coordinate cyber emergency responses.

⁴ (Korea Defence & Security Report 2013)

⁵ (Ministry of National Defence, 2010 Defense White Paper, Republic of Korea,).

⁶(Cha, Baekin, and Choong Y. Ahn. "Financial Sector Restructuring in South Korea")

Figure 1: South Korea's Command Structure for Cyber Security



Source: National Security Council, South Korea

In addition to these agencies, a Cyber War Center was created to increase security to government networks in 2010. In 2012, a cyberwarfare school was chartered to increase the current 400 security experts to 5000 experts by 2017.⁷ This increase in cyber experts is to counter North Korea's approximately 3000 professional hackers as reported by Pyongyang.⁸

MARKET ACCESS

POLITICAL ENVIRONMENT

South Korea today is a well-established democracy with tiered executive, judicial, and legislative branches operating at the national and local levels. As a member of the United Nations Educational, Scientific and Cultural Organization (UNESCO)⁹ and World Trade Organization (WTO), South Korea is open to foreign investment and trade. The US and South Korea have a long history of partnership of working together not only to strengthen financial and trade agreements but also to cooperate against regional and global threats including North Korea. The US is committed to the protection of South Korea. It currently

⁷ (Military spending on cyber 2013)

⁸ (Cyber security is vital for national defense 2009)

⁹ (United Nations Educational, Scientific and Cultural Organization)

provides 28,500 troops and cooperates with South Korea on policies related to North Korea. With recent rising costs and US budget concerns, there is pressure to reduce financial assistance to South Korea.

In a 2013, US Senate Armed Services Committee report that examined the costs associated with American military aiding South Korea; there were critics of the rising costs and the level of South Korean contributions. The US Congress tends to be less critical due to the bidirectional economic ties of Korean /American constituents according to the Congressional Research Service. With the economic rise of China, it is expected that the US will continue to provide similar levels of assistance.¹⁰

South Korea has good relations with the US, China, and Russia, as well as South East Asia. The China - South Korea relationship is two sided. Whereas China was South Korea's largest trading partner in 2012 with over \$134 billion in exports, China's close alliance and support to North Korea provides complexity to this partnership. Nevertheless, the positive relationship between the US and South Korea is a solid foundation for US exporters to access the South Korean market.

- » More details on the US-South Korea political and defense relationship can be accessed from the [Congressional Research Service](#) report.

SAFETY AND SECURITY

The biggest challenge that South Korea faces is its relations with its northern neighbor, North Korea. North Korea's nuclear capability and antagonistic leadership create military tensions and other obvious threats.

The US minimizes these risks with its commitment to protecting South Korea and promises to dispatch 690,000 troops and 2,000 warplanes in the event of war, according to the Korean government. The South Korea government is also heavily invested in its military with over 700,000 in armed forces and a high standard of equipment.¹¹ South Korea's military capability far exceeds that of North Korea. South Korea has an overall security risk rating of 80, which implies that the country is generally regarded as being reasonably secure and stable.¹²

- » For travel to South Korea to make or build business contacts, please refer to the Department of State's travel advisory portal for [South Korea](#).

TRADE AGREEMENTS

The US and South Korea entered into a [Korea-US Free Trade Agreement \(KORUS FTA\)](#), which went into effect in March 2012. The agreement is expected to boost exports by billions of dollars annually for both sides and create new export-related jobs in both South Korea and the United States. Most importantly, the agreement allows US companies easier access to the government procurement market in Korea.

- » Contact information: USTR Office of Korean Affairs (Ph: +1 202-395-5070/
Email: KORUS@ustr.eop.gov).

South Korea is also a member of the World Trade Organization (WTO) and has bilateral trade agreements in place with the US that facilitate, promote, and protect US based companies looking to export products and services to South Korea.

South Korea is a party to the [World Trade Organization's Information Technology Agreement](#) (ITA). Parties to the ITA agree to eliminate duties on several information technology products. Taken together,

¹⁰ (Congressional Research Service)

¹¹ (South Korea Defence & Security Report, 2013)

¹² (Ibid)

DEFENSE PROCUREMENT

The [Defense Acquisition Program Administration \(DAPA\)](#) is the primary agency which manages the procurement process for the Korean Defense Ministry. It has rights to determine offset credits and administer the procurement contracts including prices and schedules, technology transfer and other conditions which are instated by the Korean government for projects valued at over \$10 million. Over half of DAPA procurement in the last few years is comprised of direct commercial sales. However, the Defense Ministry, in an attempt to keep costs low, encourages sales through the Foreign Military Sales program.

A 2010 policy requires DAPA to deal directly with foreign prime contractors for all contracts exceeding \$2 million under a Force Improvement Program (FIP).¹³ FIP “includes purchases, development, upgrades, and associated installations.” This eliminates the use of agents and associated costs of doing business. It is also advisable for US companies to schedule presentations to DAPA to brief them on their products and services. Such presentations provide a strong marketing and networking opportunity for US companies.

- » Upcoming schedules can be accessed [here](#).

DOING BUSINESS WITH GOVERNMENT

Government agencies are the primary buyers for leading edge foreign technology products, systems integration, and services. US companies are encouraged to monitor government procurement plans and establish partnerships with prime Korean contractors. Government buying is influenced by past performance history, timely provision of parts and post sales service. Usually, at least two years warranty service period for security systems is necessary. Today, US companies dominate the top end product market while the Europeans have a larger share of the mid quality products. US based products have a great reputation for excellent quality and reliability.¹⁴

- » Tenders for projects in South Korea by category can be found [here](#). Also, see the appendix for tenders listing as of November 2012.

TENDER RISK

Defense Offset agreements are sometimes used in South Korea to balance trade in aerospace and military exports and gain advantages. Offsets examples include requiring security solutions to use South Korean parts or services within the program or sale. This adds additional risk and cost when bidding on government and defense programs and needs to be accounted for when responding to defense tenders and programs. Potential exporters should be aware of issues surrounding offsets including inconsistency and lack of transparency leading to a reduction in revenue.

¹³ (FIP “includes purchases, development, upgrades, and associated installations” according to US Commercial Service 2013)

¹⁴ (US ITA Guide to Security Exports, 2013)

MARKET SIZE AND GROWTH

DEFENSE SPENDING

South Korea's Defense Ministry announced that the defense budget for 2013 would be expanded from the current \$30.5 billion to slightly more than \$30.7 billion, an increase of .07 percent to meet the ongoing North Korea threat and fight cyber war.¹⁵ Within this budget is the plan to double the size of domestic information security market to 10 trillion won, (\$8.76 billion) by 2017 according to the Ministry of Science, ICT and Future Planning.

The Ministry of Defense outlined goals to protect its Defense information Network in a [2010 Defense White Paper](#). It outlines policy, budget and departments to fulfill this mission in a comprehensive national cyber security plan.

CYBER SECURITY MARKET SIZE

South Korean Defense Minister Kim Kwan-jin expects the country's information technology (IT) market to double to \$8.7 billion in 2017 from the current \$4.2 billion. Furthermore, demand for cyber security products and services from the private sector, defense and non-defense sectors will add to the overall market size and also drive market growth in the future.

COMPETITIVE MARKET LANDSCAPE

There is a growing number of South Korean and US companies providing security solutions in South Korea. AhnLab, founded in 1995, is Korea's largest security software company with considerable market share and over 500 worldwide distributors.¹⁶ AhnLab sells software that includes antivirus applications, online security, network security appliances, firewalls, IPS, UTM, and security software for online gaming and the mobile Web.

Ahnlab is joined by other South Korean security based companies; for example Penta Security, which offers web application security, database security, and public key infrastructure (PKI) solutions. American IT companies and government integrators also have a presence in South Korea. For example, the top two integrators, [Lockheed Martin](#) and [Northrup Grumman](#) have Seoul based entities. Many of the top, global IT companies have also selected Seoul as a location for business.

While these firms can be viewed as competitors, they are also possible partners for small sized exporters. Teaming up with other product vendors is a common strategy used by companies to fill gaps in technology in order to meet program requirements. Security solutions include a number of products to meet the wide range of cyber needs. These include authentication, identity management, encryption, network intrusion analysis, firewalls to name a few solutions.

US firms have a significant presence in the Korean government procurement market. The close defense relationship between the two countries is partly responsible for US companies being primary suppliers to the Korean government. In the year 2010, 66 percent of Korean defense imports were from the US through various programs.¹⁷ However, firms from the United Kingdom, Germany and other European

¹⁵ (Raghavan, Sneha, Joachim Hofbauer, and Priscilla Hermann. "Asian Defense Spending." CSIS, Oct. 2012)

¹⁶ (Security: The Last Hope for IT Growth? 2013).

¹⁷ (US Commercial Service, 2013)

countries are fast becoming rivals in this market place. In spite of this competition, American standards and quality of products are viewed favorably in South Korea and the demand for US services is expected to continue.

MARKET ENTRY

There are a few alternatives for entering the South Korean market to work on government contracts. These options include the use of agents and distributors, finding partners or setting up offices and branches for companies looking to have a longer presence in the country. Regardless of the method of entry selected, it is important to have legal counsel in South Korea to ensure that the contracts are solid, have acceptable termination clauses and as per local requirements.

AGENTS

Given the cultural and language differences between the US and South Korea, hiring an agent is often advisable especially for first time exporters. Doing so entails entering a contractual relationship with a commercial agent also known as an 'offer agent' in South Korea. Individual agents might operate on a small scale in many cases. It is crucial to find out if the agent has experience or contacts that might help with government contracts. In some cases, agents might not be exclusive and US exporters should weight the risks of working with agents before making the decision. As of 2010, defense contracts through DAPA forbid the engagement of an agent for Force Improvement Programs worth more than \$2 million. In these cases, DAPA signs contracts directly with foreign prime contractors.

US exporters might also hire a trading company instead of an individual as an agent. Registered trading companies can help with the importing process. South Korean culture is relationship-based which makes it imperative for US companies to work at getting to know their potential agents or partners and maintain regular interaction throughout the period of the contract.

PARTNERS

Instead of seeking agents, some companies might find it suitable to work with local partner companies in South Korea. Government contracts often prefer local suppliers, which increases the need for US exporters to work through a partnership model in order to win contracts. This can be a difficult route to take in South Korea in the case of some products because domestic companies are fairly technologically sophisticated and might not be keen on partnering with a foreign company. However, for cyber security consulting and other services, innovative American companies might find it easier to find partners in South Korea. Partnerships might also take the form of participation in consortia with local companies especially when the project requires local component or methods.

- » The [Gold Key service](#) offered by the US Commercial Service can help US exporters find suitable partners. Taking advantage of this service removes at least some part of the search costs and risks involved in finding partners.

SETTING UP AN OFFICE

Firms seeking to establish a long-term presence in South Korea can consider setting up a liaison office or branch. [Invest Korea](#), which also has offices in the US, provides information on these procedures. Foreign investors can establish subsidiaries for a more permanent presence. While most small exporters are unlikely to select this method of entry, companies, which do so, should familiarize themselves with the [tax considerations](#). The [Korean Commercial Arbitration Board](#) can be consulted while drawing up investment contracts.

LEGAL ISSUES

INTELLECTUAL PROPERTY RIGHTS

South Korea has favorable laws and policies for foreign investments. Laws include the protection of intellectual property, and strong enforcement provisions to ensure that American rights are efficiently and effectively protected. Other key protections surround Copyright, Penalties for Piracy, Counterfeiting and patent protection, all key considerations when exporting cyber security products.¹⁸

South Korea follows a patent and trademark system based on 'first-in-time, first-in-right'. US firms should register their intellectual property in South Korea. Doing so is even more important when working with a South Korean partner or trading company.

- » [Korea Intellectual Property Office \(KIPO\)](#)

TENDER LAWS

According to DAPA, offsets are used with FMS and Research and Development, (R&D) projects equal to or exceeding \$10 million. However, DAPA also reserves the right to place offsets on a case-by-case basis. Because these rules are written broadly, offset rules should be verified with the US Department of [Commerce](#) and the [Bureau of Industry and Security](#) (BIS) before exporting cyber security solutions. BIS's role is to protect US security when exporting technology and is tasked with overseeing US defense offset agreements with foreign nations.

- » More information is available through South Korea's [DAPA site](#) which lists the 2012 Offset guidelines.

ECONOMIC ENVIRONMENT

South Korea is a high growth, industrialized economy. As the 12th largest economy in the world, a gross domestic product (GDP) of \$1.64 trillion, (2012) and a growth rate of 2 percent, (2012)¹⁹, there is great opportunity for trade and investment. Ironically, some of the growth challenges South Korea faces include its reliance on exports, which comprise 50 percent of its GDP.

Today, South Korea is home to 13 of the Fortune 500 global companies including Samsung, LG, and Hyundai Heavy Industries Co., Ltd., which produce everything from mobile phones to ships.²⁰ While it continues to grow its technology sector, investment and growth in biotechnology is also on the rise. South Korea's highly educated workforce, with educational standards among the highest in the world aids its firms in high-end product development.

The US is South Korea's second largest export partner and third largest country for imports. Top imports include machinery, electronics and electronic equipment, oil, steel, transport equipment, organic chemicals, and plastics.

¹⁸ (Intellectual Property Rights in the US-South Korea Trade Agreement.- Office of the United States Trade Representative.)

¹⁹ (Estimate from Central Intelligence Agency." The World Factbook. 2013)

²⁰(Fortune Magazine)

South Korea's currency, the Won is mostly stable. The Won saw dramatic depreciation with the global financial crisis in late 2008, the sinking of a South Korean ship by a North Korean submarine and the subsequent artillery barrage on a southern island in 2011. Since then the won has gradually appreciated, strengthening past the 1,100/USD level.

SOCIO- CULTURAL ENVIRONMENT

While Korea is becoming more “Westernized” in doing business, there are many cultural differences that are important to know. Considerations include the concept of how a contract differs between the US and Korea. While the US places great importance on the specific and words in a contract, Koreans view a contract as more broadly defined, leaving room for flexibility and adjustment later. It is important that both parties to contracts have understanding of terms agreed upon.

In the area of business relationships Koreans value personal relationships when doing business so Americans should be ready to mix business with social life. Seniors in age are given the highest of respect and women are now entering into management roles as well.

While laws and institutions are in place to protect intellectual property, there are reported problems of corruption, which undermines these laws and creates risk when needing legal assistance, according to the Heritage Foundation.²¹ This claim is substantiated by the [Transparency International Corruption Index](#) placing South Korea at 56 out of 100, whereby scores range from 0 (highly corrupt) to 100 (very clean).²² This compares with the United States score of 73.²³

PRIVATE SECTOR DEMAND

South Korea has a large group of multinational companies that are working to remain competitive in the global market place. These companies are required to build new information technology (IT) infrastructure to accommodate mobility and cloud services for greater efficiencies and cost savings.

During the 2008 – 2012 time period, many of the major South Korean Companies were hacked to expose valuable customer data. These companies include SK Communications, a large Korea Internet Service Provider; Hyundai Capital, a major consumer finance company; Nexon, Korea's biggest gaming company with 13 million users; Operator KT, Korea's largest internet provider with 9 million users and Cyworld, a Facebook competitor with an estimated 35 million records.²⁴

Global market projections for the commercial cyber security marketplace have predicted growth rates between 8 and 10 percent from a base of over \$30 billion, for the foreseeable future, according to IDC.²⁵ South Korea will be no exception to this forecast. With the government projected to train 5000 cyber security experts by 2017, its labor force will be primed to implement and innovate in the cyber security area. Although today, the private sector is lagging in investment, the recent high profile attacks with estimated costs as high as \$7.5 million necessitate cyber security investment in the future.

²¹ (<http://www.heritage.org/index/country/southkorea>)

²² (Scores range from 0 (highly corrupt) to 100 (very clean)).

²³ (<http://www.transparency.org/cpi2012/results>)

²⁴ (Hackings in Korea have compromised more than 100 million user accounts since 2008, 2013)

²⁵ (Information Age/IDC, 2012)

Table 1: South Korea Cyber Security Market at a Glance

Strengths

- Strong political and defense relationship with the US
- Large military budget
- Open market access
- Member of WTO's Government Procurement Agreement

Opportunities

- Increased spending on cyber security
- Free trade agreement with the US
- High regard for US defense and security products

Weaknesses

- Cultural differences and issues which create challenges for foreign firms doing business

Threats

- Significant competition from other domestic and foreign companies
- Existence of technologically sophisticated domestic companies
- North Korea

Table 2: Examples of Available Tenders Related to Cyber Security²⁶

Industry	Project details	Due date
Information Technology	Maintaining and supporting of National Spatial Information Center systems	16 Dec 2013
Transportation - Airports & Aviation , Infrastructure - Roads and Highways , Information Technology (IT)	Smart Highway Project (IT)	n.a.
Information Technology	Maintaining and supporting of the 2014 Korea Land Information Systems(KLIS)	16 Dec 2013
Telecommunications	Telemetry system	6 Dec 2013

SOURCE: Information obtained from www.globaltenders.com/republicofkorea.

²⁶ (Information obtained from www.globaltenders.com/republicofkorea)

APPENDIX 1: USEFUL LINKS

US Export Controls

- » [International Traffic in Arms Regulations \(ITAR\) – U.S. Department of State](#)
- » [Export Administration Regulations \(EAR\) – U.S. Department of Commerce](#)
- » [Exporting from Virginia](#)
- » [Export Licenses](#)
- » [KORUS Free Trade Agreement](#)

US Laws Governing International Business

- » [US Anti-corruption guide](#)
- » [Corruption Map](#)

US-South Korea Political Relationship

- » [US-South Korea Political Relations](#)
- » [Congressional Research Service](#)

Country Information

- » [Country Information](#)
- » [Country Fact Sheet](#)
- » [Culture](#)

Doing Business in South Korea

- » [US Commercial Service](#)
- » [Exporting to South Korea](#)
- » [US Embassy in South Korea](#)

APPENDIX 2: KEY CONTACTS IN SOUTH KOREA

[US Embassy, South Korea](#)

US Embassy in Seoul, Korea
188 Sejong-daero, Jongno-gu,
Seoul, Korea
1 82-2-397-4114 10-710

[American Chamber of Commerce in Korea](#)

#4501 TradeTower 159
Samsung-Dong, Seoul, 135-729
Tel: (82-2) 564-2040 Fax: (82-2) 564-2050
amchamrsvp@amchamkorea.org

[Korea Customs Service \(KCS\)](#)

Address: Building 1, Government Complex-Daejeon, 920 Dunsan-dong, Seo-gu, Daejeon, Korea / Postal code: 302-701
Main line: 1577 - 8577

[Korea Chamber of Commerce and Industry\(KCCI\)](#)

39, Sejong-daero, Jung-gu, Seoul
Tel:82-2-6050-3114
email: webmaster@korcham.net

[Korea Trade Investment Promotion Agency \(KOTRA\)](#)

Address : (137-749) 13 Heonreung-ro, Seocho-gu, Seoul (Former: 300-9 Yeomgok-dong, Seocho-gu, Seoul)
TEL : (02) 3460-7114
FAX : (02) 3460-7777

[Korea International Trade Association \(KITA\)](#)

General inquiry regarding KITA, please contact
Trade Call Center : 82-1566-5114
e-Mail : kitainfo@kita.net
For DC office:
1660 L ST NW Suite 401, Washington DC 20036
Tel : 202-828-9282 / Fax : 202-828-9287

Information Technology Industry

[Korea Information Technology Service Industry Association](#)
[Korea Internet and Security Agency](#)
[Korea Software Enterprise Association](#)
[Korea Software Industry Association](#)
[Korea Software Property-Right Council](#)
[Korea Software Technology Association](#)

REFERENCES

As Internet Gets Faster, Hong Kong & South Korea Lead the Broadband Speed Derby — Tech News and Analysis. *Gigaom.com*, 22 Apr. 2012. Web. Retrieved 10 Nov. 2013 from <http://gigaom.com/2013/04/22/as-internet-gets-faster-hong-kong-south-korea-lead-the-broadband-speed-derby/>.

Central Intelligence Agency.(2013) *The World Factbook*. N.p., n.d. Web. Retrieved 03 Nov, 2013 from <https://www.cia.gov/library/publications/the-world-factbook/geos/ks.html>

Cha, Baekin, and Choong Y. Ahn.(2004) Financial Sector Restructuring in South Korea: Accomplishments and Unfinished Agenda -.Vol. 3(1): 1-21.

Country Intelligence Report.(2013). Sept 5, 2013. *IHS Global*.

Intellectual Property Rights in the US-South Korea Trade Agreement.(2013) *Office of the United States Trade Representative*. Web. Retrieved 03 Nov. 2013 from <http://www.ustr.gov/uskoreaFTA/IPR>

Cyber Security Is Vital for National Defense.(2009) , *Chosunilbo*, 2 November 2009, Web. <http://english.chosun.com/>

Development Progress in Korea. (2013). *Korea*. World Bank, 10 Nov. 2013. Web. <http://www.worldbank.org/en/country/korea>

Doing Business with South Korea.(2013) *PKF.com/media*, 2012. Web. Retrieved 20 Oct. 2013. From <http://www.pkf.com/publications/doing-business-in/doing-business-in-south-korea>

Hackings in Korea Have Compromised More than 100 Million User Accounts since 2008. (2013). *TNW Network All Stories RSS*. The Next Web.com/Asia, 21 July 2013. Web. 20 Oct. 2013. from <http://thenextweb.com/asia/2013/07/21/koreas-internet-explorer-dependency-blamed-for-hacking-of-over-100m-user-records-since-2008/>

Information Age. (2012). Analytics software market hits \$30 billion. July 11, 2010. Retrieved November 12, 2013 from [http://www.information-age.com/technology/information-management/2112153/analytics-software-market-hits-\\$30-billion](http://www.information-age.com/technology/information-management/2112153/analytics-software-market-hits-$30-billion)

List of Internet Security Companies Worldwide. (2013). Bloomberg, Web. Retrieved 10 Nov. 2013 from <http://www.bloomberg.com/markets/companies/internet-security/>.

Military Spending on Cyber. (2013). *Phys.org*. 18 Mar. 2013. Web. 10 Nov. 2013. Military spending on Cyber - <http://phys.org/news/2013-03-south-korea-gun-cyber-warriors.html>.

Ministry of National Defence, Republic of Korea. (2010). *Defense White Paper*, Print. pp. 8–10.

News. Attack on South Korean Targets Part of a Larger Cyber-espionage Campaign. (2013). *Infosecurity Magazine.com*, 08 July 2013. Web. Retrieved 10 Nov. 2013 from <http://www.infosecurity-magazine.com/view/33341/attack-on-south-korean-targets-part-of-a-larger-cyberespionage-campaign/>.

News. South-Korea-Leads-Nations-in-pc-infections. (2013). *Infosecurity Magazine.com*., 08 Aug. 2012. Web. Retrieved 10 Nov. 2013 from <http://www.infosecurity-magazine.com/view/27487/south-korea-leads-nations-in-pc-infections/>

Ponemon Institute© Research Report,(2012). *Cost of Cyber Crime Study* Web. Retrieved 10 Nov. 2013 from http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

Raghavan, Sneha, Hofbauer , Joachim, and Hermann , Priscilla. (2012). Asian defense spending. CSIS, Oct. 2012. Web. http://csis.org/files/publication/121005_Berteau_AsianDefenseSpending_Web.pdf

Security: The Last Hope for IT Growth? (2014). *Home*. Sept. 2004. Web. Retrieved 10 Nov. 2013 from <http://www.koreaitimes.com/story/1634/security-last-hope-it-growth>.

South Korea Confronts Uphill Battle against Hackers. (2013). *South Korea Confronts Uphill Battle against Hackers*. Korea Herald, 19 July 2013. Web. Retrieved 15 Oct. 2013 from <http://www.koreaherald.com/view.php?ud=20130719000707>.

South Korea Cyber Security-Concerns Go Far Beyond Financial Industry.(2013) E27.co, 22 July 2013. Web. <http://e27.co/south-korea-cyber-security-concerns-go-far-beyond-financial-industry/>

South Korea Defence & Security Report.(2013) Q3. Published by Business Monitor International ISSN 1749-1665

Top-20-where-to-find-the-world-s-fastest-internet (2013). *Bloomberg.com*, 23 July 2013. Web. 20 Oct. 2013. <http://www.bloomberg.com/slideshow/2013-07-23/top-20-where-to-find-the-world-s-fastest-internet.html>

US International Trade Administration. (2013). Global safety and security resource guide. 2013-2014 Edition. Available from www.buyinfousa.net

US - Korea Free Trade Agreement.(2013). Web. Retrieved 30 Oct. 2013 from <http://www.ustr.gov/uskoreaFTA>.