Virginia
ExportVirginia.org
BUSINESS WITHOUT BORDERS

Saudi Arabia

Cyber Security Market

Saudi Arabia's Cyber Security Market

EXECUTIVE SUMMARY

- Offers ripe market for cyber security exports, which is expected to increase 30 percent to $37.5 billion by 2016.
- Foreign firms need to navigate certain cultural considerations; however, the kingdom offers a stable political and economic environment.
- Strong need for surveillance technology, communication systems, detection equipment, cyber attack alarms, and cyber intrusion prevention technology.
- Saudi Arabia devotes considerable resources to defense spending and recognizes cyber security as a key area for future investment.
- US has coordinated cyber security policies with Saudi Arabia and organized trade missions, making it easier for US defense firms to engage the government.
- Private sector demand in the energy, banking, IT and communications industries.

Saudi Arabia's Cyber Security Market

POLITICAL & ECONOMIC ENVIRONMENT

- Saudi Arabia offers a stable political environment under the monarchy.
- Although relatively secure, terrorist groups pose some security threats.
- Saudi Arabia's economy is prospering and competitive, with the highest GDP in the Middle East.
- GDP has increased at an average annual rate of six percent.
- Trade has historically accounted for more than 90 percent of GDP.
- Government spending has also led economic growth, boding well for US defense firms.

Saudi Arabia's Cyber Security Market

CYBER SECURITY MARKET

- All levels of government have begun to focus on cyber security. National Information Security Strategy proposed in 2011, attempts to establish a national cyber security agenda, but still open for comments.
- Cyber attacks on government websites have elevated demand. The Ministry of Finance, Interior and Labor as well as SEO Aramco have been victims of attack.
- ITA identified immediate need for surveillance technology, communication systems, detection systems, and cyber intrusion prevention.
- US maintains Technical Cooperation Agreement for security-related issues.
- A handful of US firms already occupy some of the market space.
- Market entrants could target eGovernment initiatives and efforts to enhance protection of energy systems and e-commerce.

Saudi Arabia's Cyber Security Market

MARKET ACCESS, SIZE & GROWTH

•Last year, military expenditures reached $53 billion. In 2013, public and private cyber security spending reached $6 billion and is expected to expand exponentially. The King, Crown Prince, Council of Ministers and relevant ministries oversee military spending and programs.

•Party to the WTO GPA. Most government contracts are published publically and subject to standardized requirements.

•Although import burdens are comparatively minimal, GCC countries maintain a competitive advantage over foreign firms from other countries.

•Saudi Arabia maintains trade agreements with the US, and several other countries including the MEFTA.

•US has helped shaped cyber security agenda and led trade missions to connect US defense firms with opportunities.

Saudi Arabia's Cyber Security Market

MARKET ENTRY STRATEGY

- Foreign firms not required to partner with nationals or employ a commercial agent, however it is advisable.
- Foreign firms looking to establish local presence can either form an LLC or joint stock company.
- To register a business, foreign firms must engage SAGIA, obtain an Investment Licenses, and complete a Commercial Registration.

Saudi Arabia's Cyber Security Market

PRACTICAL CONSIDERATIONS

•Saudi Arabia has reinforced cyber security regulatory and legislative framework with four new IP laws and a new cyber security law.

•Saudi Arabia's corporate tax system is highly regarded for its simplicity and clarity.

•Socio-cultural issues include:

- Gender inequality
- Censorship
- Piracy
- *Shari'ah* Law

Saudi Arabia's Cyber Security Market

PRIVATE SECTOR DEMAND

- Role for private sector cyber security exports.
- US trade missions already identified private sector opportunities.
- Private sector opportunities include:
  - Energy
  - Financial services
  - Technology firms
  - Communications