YIGAL ARNON & CO.

LAW FIRM

LEGAL UPDATE – JANUARY 2016
PROPOSED REGULATIONS ON CYBERSECURITY EXPORTS

The Israeli Defense Export Controls Agency ("**DECA**") has proposed new regulations concerning the export of cybersecurity products. The proposed regulations put forward an export control regime that is substantially more comprehensive and extensive than the 2013 amendments to the Wassenaar Arrangement. For example, the proposed regulations include express restrictions on the cross-border disclosure of vulnerabilities and the export of software designed to locate vulnerabilities, as well as restrictions on software that provides cyberdefense and forensic capabilities. DECA is accepting comments on the proposed regulations until February 7, 2016.

The proposed cybersecurity regulations are detailed. This legal update generally describes the proposed categories of controlled products, but does not include all details. An unofficial English translation of the proposed control list is available upon request.

Background

The Wassenaar Arrangement is an international export control regime. Countries that are members of the Wassenaar Arrangement coordinate regarding the imposition of national export restrictions on conventional arms and dual-use goods and technologies. In 2013, the Wassenaar Arrangement was amended to include controls for certain cybersecurity-related technologies – specifically software and technology that are directed at "intrusion software" and "IP network communications surveillance systems."

Israel is not a member of the Wassenaar Arrangement. At the same time, Israel generally updates its national export controls to reflect the requirements of the Wassenaar Arrangement pursuant to the Israeli Import-Export Order (Regulation of the Export of Dual-Use Goods and Services) (the "**Wassenaar Order**"). Under the Israeli Wassenaar Order, all exports of controlled dual-use technologies require an export license. Requests for export licenses are directed to the Ministry of Defense, in the case of exports for military or defense uses, or the Ministry of the Economy, in the case of exports for civilian use. Procedures for obtaining export licenses are not addressed in this update.

On January 7, 2016, DECA published proposed regulations covering cybersecurity exports. The regulation propose export controls on the following three categories:

1. **Systems, Equipment & Components**: This category follows the Wassenaar Arrangement by controlling "Intrusion Software" and "systems, equipment and components specially designed or modified for generation, operation or delivery of, or communication with Intrusion Software" on the proposed control list. The category, however, goes substantially farther than the Wassenaar Arrangement in also proposing controls on software for the simulation of intrusions, cyberdefense products for military defense equipment, and products for digital forensics. The proposed category also includes proposed export controls on systems for the monitoring of national-grade communication backbones, a class of technology that is similar to but substantially broader than the Wassenaar controls on "IP network communication surveillance systems".
2. **Software**: This proposed category includes proposed export controls on software that performs functionality similar to the proposed category of Systems, Equipment & Components.

3. **Technology & Know-How**: This proposed category includes software vulnerabilities as well as technology and know-how for the development of "Intrusion Software". The proposed regulations include several exceptions to the controls on the cross-border disclosure of vulnerabilities. These exceptions include the disclosure of vulnerabilities exclusively to the developer of the affected software, the disclosure of vulnerabilities that are already in the public domain and the disclosure of vulnerabilities that are intended for use in the "defense products" of the company. The category also includes software for the automatic detection of software vulnerabilities.

Analysis

The proposed regulations set forth an export control regime that has the potential to significantly affect cybersecurity research and the cybersecurity industry in Israel. Some of the proposed additions to the control list reflect the language of the Wassenaar Arrangement. Other proposed additions, however, go substantially farther than the Wassenaar controls, such as the proposed controls on systems, equipment, components and software for the "monitoring of national grade communication backbones".

In particular, companies active in cybersecurity should note the proposed regime for the control of the cross-border disclosure of software vulnerabilities. While the proposal does include some exceptions to this proposed addition to the control list, it is not clear if these exceptions are sufficiently broad to cover academic security research, malware detection, situations of security vulnerabilities in open source software (such as with the Heartbleed bug) or other circumstances in which the correction of security vulnerabilities requires the cross-border cooperation of a number of firms and governments.

DECA is accepting comments on the proposed regulations until February 7, 2016.

Contact Details

Eli Greenbaum, Partner
Email: elig@arnon.co.il
Phone: +972-2-623-9200