KIRKLAND & ELLIS LLP

KIRKLAND ALERT

September 2010

$42 Million Blackwater Settlement Demonstrates ITAR Enforcement on the Rise

On August 23, 2010, the State Department's Directorate of Defense Trade Controls (DDTC) published its $42 million Consent Agreement with the private security firm formerly known as Blackwater Worldwide ("Blackwater"; n/k/a Xe Services LLC), settling claims for hundreds of International Traffic in Arms Regulations (ITAR) violations. This highly-anticipated civil settlement followed the State Department's December 2008 imposition of a "presumption of denial" for all new applications for export licenses or other forms of authorization submitted by Blackwater, with limited exceptions for applications "in direct support of a U.S. Government contract."[1] The Blackwater Consent Agreement set a new high-water mark for ITAR settlements, surpassing the Hughes Electronics/Boeing Satellite settlement of 2003 and the ITT Corporation settlement of 2007. As discussed below, this settlement embodies the recent trend of increasing penalties for ITAR violations.

ITAR Enforcement: A Brief Overview

Although controlling the export of defense articles has always been an enforcement priority, post-9/11 terrorism threats have led to increased efforts to halt the illegal trade of defense articles and services. The ITAR, which implement the Arms Export Control Act (AECA), govern the temporary import and temporary and permanent export of defense articles and services that appear on the United States Munitions List (USML).

The DDTC may impose civil penalties for ITAR violations. Generally, such penalties include fines of up to $500,000 per violation, a portion of which the DDTC may offset for remedial compliance expenditures. Settlements often result in Consent Agreements that specify onerous compliance measures that must be undertaken as part of the settlement. The compliance measures may include:

- Appointment of an internal or external Special Compliance Officer (SCO), in some cases subject to DDTC approval
- Law Department oversight of consent-decree implementation and monitoring
- Debarment
- License Revocation
- Comprehensive audits
- On-site reviews by the DDTC with minimum advance notice
- Institution of a "cradle-to-grave" automated export tracking system

In addition, U.S. Immigrations and Customs Enforcement (ICE) and the Federal Bureau of Investigation (FBI) have authority to investigate violations of ITAR for possible criminal prosecution. Subjects of civil and criminal enforcement for ITAR violations range broadly from those who deliberately violate U.S. law for profit, to major defense contractors who run afoul of highly technical regulations either through an outdated compliance

regime[2] or through an acquisition of an entity with such a deficiency in their export controls.[3]

Recent Trend: Rising Penalties

Because defense trade control is so integral to national security, the DDTC expects strict compliance, and applies stiff fines and penalties when violations are discovered. In recent years, penalty amounts have increased substantially.

In 1998, the first double-digit penalty in the millions was issued for ITAR violations. Penalty amounts increased incrementally over the next several years, culminating in a notably high settlement in February 2003, with a $25 million civil penalty pertaining to unlicensed exports of defense-related hardware and technical data to Pakistan. That penalty was eclipsed just days later with a $32 million fine against another company for furnishing to China defense services related to a space launch vehicle without the required licenses.

In more recent years, significant civil penalties have remained a fixture in ITAR enforcement. In 2007, ITT Corporation, the leading manufacturer of military night vision equipment for the U.S. Armed Forces, became the first major defense contractor to be criminally convicted for violations of ITAR after admitting to sending sensitive night vision technology to China, Singapore, and the United Kingdom without the requisite State Department licenses. As a result, the DDTC levied a $28 million fine against ITT Corporation. The DDTC also imposed a statutory debarment against ITT Corporation's Night Vision Value Center unit; revoked eighty-eight licenses previously approved for the ITT Night Vision Division; and ordered ITT Corporation to retain and pay for an external monitor to serve as a Special Compliance Official. The next year, the DDTC imposed a $25 million fine on photonics manufacturer Qioptiq (formerly Thales) for unauthorized exports of ITAR-controlled technical data and defense articles.

Blackwater: New High-Water Mark

As demonstrated by the recent Blackwater settlement, ITAR enforcement is on the rise. The $42 million civil penalty—which surpasses the Hughes settlement by $10 million—settles charges that Blackwater committed an array of ITAR violations, including:

- violations of provisos of a license governing firearms exported to Iraq;
- unauthorized proposals to train armed forces in the Sudan, a proscribed country;
- unauthorized exports of technical data and provision of defense services involving military training to foreign persons, including dual-national persons from Afghanistan, Iran, and Pakistan; and
- unauthorized exports of defense articles, including Significant Military Equipment (SME), to Afghanistan and Iraq.

In addition, the DDTC alleged that Blackwater failed to maintain records involving ITAR-controlled transactions and made false statements, misrepresentations, and omissions of material facts. Altogether, DDTC charged Blackwater with 288 AECA and ITAR violations.

The Consent Agreement, which settles and disposes of all the violations in DDTC's Proposed Charging Letter to Blackwater, is effective for four years and contains a hefty list of requirements to which Blackwater must adhere. To begin, Blackwater must pay a $42 million civil penalty, of which only $12 million may be used to defray the costs of remedial compliance measures. Blackwater is also required to appoint a DDTC-approved external Special Compliance Official (SCO) who will (1) monitor Blackwater's ITAR compliance program, policies, and procedures; (2) oversee a variety of compliance activities at Blackwater, including internal ITAR audits; and (3) track, evaluate, and report to DDTC the status of Blackwater's compliance with the Consent Agreement, including any findings or recommendations necessary to ensure strict compliance with the ITAR. The external SCO must perform these duties for the first three years of the Consent Agreement term. During the fourth and final year of the term, Blackwater may appoint an internal SCO (ISCO) to assume the SCO's duties.

In addition, the Consent Agreement requires Blackwater to implement an automated export compliance system that is capable of tracking exported defense articles and identifying technical data and assistance to

be disclosed to foreign persons. Blackwater must also develop within its email system a means of alerting users to ITAR requirements on electronic transmissions of ITAR technical data. Moreover, external consultants must audit Blackwater's compliance with the Consent Agreement and the overall effectiveness of Blackwater's ITAR compliance programs twice under the supervision of the SCO or ISCO.

Notably, as each of the 288 charges brought against Blackwater carried a maximum $500,000 civil penalty, the $42 million Blackwater fine—while significant—could have been much higher. Thus the Blackwater Consent Agreement highlights the importance of considering voluntary disclosure of ITAR violations. Indeed, the DDTC's Proposed Charging Letter noted that in the absence of certain mitigating factors—including Blackwater's voluntary disclosures and cooperation with the DDTC's investigation—the charges and penalties would likely have been even more severe.

In the wake of the 2007 ITT settlement, the 2008 Qioptic settlement, and the Blackwater Consent Agreement published last month, defense contractors and others involved in this industry are on notice that the DDTC has raised the bar on liability for these violations. Such increased exposure is particularly troublesome given the vulnerability created by emerging issues such as: (1) DDTC scrutiny of dual-citizen employees; (2) so-called deemed exports to foreign nationals employed in the U.S.; and (3) email and electronic vulnerabilities with respect to transfers of technical data. We will continue to update our clients regarding these specific issues.

---

1 For full text, see Public Notice 6458, 73 Fed. Reg. 77099 (Dec. 18, 2008).

2 *See, e.g.*, ITT Corporation Consent Agreement and Order, dated December 21, 2007, available on the State Department DDTC website at www.pmddtc.state.gov/compliance/consent_agreements.html.

3 *See, e.g.*, General Motors Corporation and General Dynamics Corporation Consent Agreement and Order, dated November 1, 2004, available on the State Department DDTC website at www.pmddtc.state.gov/compliance/consent_agreements.html.

If you have any questions about the matters addressed in this *Kirkland Alert*, please contact the following Kirkland authors or your regular Kirkland contact.

Michael J. Garcia
Kirkland & Ellis LLP - New York
www.kirkland.com/mgarcia
+1 (212) 446-4810

Michael J. Garcia was the Assistant Secretary of Homeland Security for Immigration and Customs Enforcement ("ICE") from 2003 to 2005, and from 2001 to 2002 was the Assistant Secretary of Commerce for Export Enforcement. As head of ICE, he led an agency of 6000 investigators charged with enforcing the Arms Export Control Act and the International Traffic in Arms Regulations ("ITAR"). As Assistant Secretary of Commerce he was the nation's top enforcer of U.S. restrictions on the export of sensitive dual-use technology. Mr. Garcia also served as United States Attorney for the Southern District of New York, from 2005 to 2008, and in that role he created an export enforcement task force later used as a model by the Department of Justice for a nationwide initiative.

Henry J. DePippo
Kirkland & Ellis LLP - New York
www.kirkland.com/hdepippo
+1 (212) 446-4780

Henry J. DePippo was the Deputy Chief of the Criminal Division in the United States Attorney's Office for the Southern District of New York from 1993 to 1994, where he served as one of the lead prosecutors in the successful trial involving the 1993 terrorist bombing of the World Trade Center. He also has extensive private practice experience defending corporations and leading internal investigations, including in matters related to potential export control violations. Among those matters, he is leading a multinational investigation into potential diversion of controlled products in connection with an energy project in Iran.

Mark R. Filip
Kirkland & Ellis LLP - Chicago
www.kirkland.com/mfilip
+1 (312) 862-2192

Mark Filip was second-in-command of the Justice Department as the Deputy Attorney General of the United States, charged with overseeing all of the Department's criminal, civil, and regulatory enforcement efforts. As Deputy Attorney General, Mr. Filip also represented the Department in interactions with Congress, the White House, and other cabinet-level Departments, as well as with numerous foreign governments throughout Europe, the Middle East, and South America. Mr. Filip also served as Acting Attorney General for the new administration after January 20, 2009, until Attorney General of the United States Eric Holder was confirmed. Prior to serving as Deputy Attorney General, Mr. Filip spent four years presiding over a full docket of federal civil and criminal cases as a federal judge in the U.S. District Court for the Northern District of Illinois.

John A. Eisenberg
Kirkland & Ellis LLP - Washington
www.kirkland.com/jeisenberg
+1 (202) 879-5902

John Eisenberg served at the Department of Justice from 2004 to 2009 in various capacities, with a focus on national security, including intelligence and counterterrorism issues. Both as a Deputy Assistant Attorney General in the Office of Legal Counsel and as an Associate Deputy Attorney General, Mr. Eisenberg advised the Attorney General, the Deputy Attorney General, the Counsel to the President, the Legal Advisor to the National Security Council, the General Counsel of the Department of Defense, and various general counsels in the Intelligence Community on complicated national security matters.