ISRAEL PRACTICE **NEWSLETTER**

WINTER 2017

TABLE OF CONTENTS

Holland & Knight

www.hklaw.com

Holland & Knight

ISRAEL PRACTICE NEWSLETTER

WINTER 2017

Holland & Knight is a U.S.-based global law firm with a strong commitment to the state of Israel. We focus on providing guidance to Israeli investors and companies interested in doing business or making investments in the United States and Latin America. With more than 1,250 professionals in 27 offices, our lawyers and professionals are highly experienced in all the interdisciplinary areas necessary to guide entrepreneurs, investors, and startup or established companies through the opportunities and challenges that arise throughout the business or investment life cycles.

Areas of legal guidance that are typically provided to our Israel Practice clients include real estate, mergers and acquisitions, private equity, international tax, cross border and customs, Internet privacy and cybersecurity, intellectual property, government lobbying, regulations and compliance, U.S. Foreign Corrupt Practices Act (FCPA), U.S. Foreign Account Tax Compliance Act (FATCA), and litigation and dispute resolution.

We invite you to read our Israel Practice newsletter, in which our authors discuss pertinent American-Israeli topics. As Israel has been a crossroads and a prolific source of new ideas for more than 3,000 years, a natural tradition of inventiveness finds its most recent expression in the creation of a technology startup ecosystem with global impact. This newsletter addresses, among other relevant topics, how the innovative technologies and ideas generated in Israel can be deployed in the United States and globally. We invite you to discuss your thoughts on this issue with our authors listed within the document.

מגזין משפטי ללקוחות ישראלים

Holland & Knight הינה פירמת עורכי דין אמריקאית גלובלית בעלת מחויבות עמוקה לשוק הישראלי. אנו מתמקדים במתן שירותי יעוץ למשקיעים וחברות ישראליות המעוניינים להרחיב פעילות או להשקיע בארצות הברית ובאמריקה הלטינית. פירמת עורכי הדין Holland & Knight מעסיקה למעלה מ-1,250 עורכי דין ואנשי מקצוע ב-27 משרדים. לאנשינו ניסיון רב בכל תחומי הפרקטיקה הנחוצים כדי להנחות יזמים, משקיעים, חברות הזנק וחברות מבוססות.

במסגרת הפרקטיקה הישראלית, אנו מעניקים ללקוחותינו יעוץ משפטי בתחומים שונים, לרבות נדל"ן, מיזוגים ורכישות, קרנות השקעה, מיסוי בינלאומי, מסחר בינלאומי ומכסים, פרטיות ואבטחת מידע, קניין רוחני, ייעוץ לוביסטי ורגולטורי, לרבות FCPA, ו- FATCA, סיוע ביישוב סכסוכים עסקיים וליטיגציה.

אנחנו שמחים להזמין אתכם לקרוא את המגזין המשפטי של הפרקטיקה הישראלית. המגזין עוסק בנושאים בעלי חשיבות למשקיעים וחברות ישראליות הפועלים או המעוניינים להרחיב פעילות בארצות הברית ובאמריקה הלטינית. מעמדה של ישראל כצומת דרכים ומקור בלתי נדלה לחדשנות מזה למעלה מ-3,000 שנה, בא לידי ביטוי ביצירת מערכת פורייה של חברות הזנק טכנולוגיות בעלות השפעה כלל-עולמית. מגזין זה עוסק, בין היתר, באופן שבו ניתן להטמיע בארצות הברית וברחבי העולם טכנולוגיות ורעיונות חדשניים שמקורם בישראל. אנו מזמינים אתכם לפנות בכל שאלה שתעלה בנוגע למידע המתפרסם במגזין זה לכותבים שלנו, ששמותיהם מופיעים לצד המאמרים.

Israel in the Sights of Foreign Corrupt Practices Act Regulators

By Wifredo A. Ferrer and Alec M. Puig


Despite the distance and jurisdictional barriers, U.S. regulators have expanded their global pursuit of Foreign Corrupt Practices Act (FCPA) violators. In recent years, the U.S. Securities and Exchange Committee (SEC) and Department of Justice (DOJ) have ramped up FCPA investigations throughout the world, including within the Israeli economy.

The intensification of this regulatory focus has corresponded with Israel's increasing share of the international marketplace, particularly in the realms of healthcare, technology and natural resource extraction. As recently as December 2016, an Israeli pharmaceutical giant was assessed a $283 million penalty by the DOJ and was required to forfeit $236 million in profits plus interest to the SEC in connection with a subsidiary having pleaded guilty to conspiring to violate the FCPA.

Recent Trends in FCPA Enforcement and Penalties

Penalties for violating the FCPA can be cataclysmic. In September 2017, a Swedish telecommunications corporation settled an enforcement action for $965 million – the largest penalty ever exacted. In the years after the FCPA was amended in 1998, enforcement has risen sharply and has been pursued aggressively. Prior to 2007, there had been only one FCPA claim brought against an Israeli company or individual. Since then, several Israeli companies and individuals have been implicated, including a mining corporation, a large telecommunications enterprise and the former director of a government-owned utilities company. U.S. regulators are capable of bringing claims against Israeli individuals and corporations, primarily because of the exceptionally broad extraterritorial reach of the Act. As described above, violation of the FCPA often comes with steep civil and criminal penalties in addition to significant reputational damage. However, a robust understanding of the FCPA as well as an effective compliance and ethics program can help mitigate one's exposure.

The FCPA's Long Jurisdictional Arm

The FCPA's anti-bribery and accounting provisions have broad extraterritorial reach. In addition to U.S. entities, the anti-bribery provisions also apply to non-U.S. "issuers" as well as non-U.S. nationals and corporations, both private and public, that engage in any act in furtherance of a corrupt payment while in the territory of the United States. An "issuer," in practice, is a company that offers a class of securities listed on a national exchange in the U.S., or any company that features a class of securities quoted in the over-the counter market in the U.S. and that is required to file reports to the SEC. Therefore, an entity operating outside of the U.S. may still be categorized as an issuer under the Act even if the entity is not organized under U.S. law.

If a non-U.S. entity does not classify as an issuer, FCPA liability can still be triggered by ordinary day-to-day business conducted inside or outside of the U.S. For example, under the FCPA's extraterritorial provisions, merely placing a phone call, sending an email, text messaging, or faxing to or through the U.S. in furtherance of a corrupt payment is enough to incur liability, regardless of where the conduct originated. Even if an email is not directed to a U.S. recipient, the email is still covered under the Act if it is routed through a U.S. server. Moreover, liability may extend to the parent company if any of its employees, third-party contractors or subsidiaries engage in similar conduct, especially if the subsidiary is a U.S. corporation. As a result, companies looking to shield themselves from liability might consider installing compliance programs among their subsidiaries as well.

Criminal and Civil Penalties

Failure to implement effective anti-bribery programs leaves companies and individuals vulnerable to criminal convictions and civil penalties. For a company, a criminal conviction could carry a fine of up to $2 million per violation as well as restitution. Suspension, debarment or loss of export privileges may follow as well. A criminal conviction for an individual actor is punishable by as much as fines of up to $250,000 per violation, five years in prison, restitution, extradition and asset seizure. Anti-bribery violations by a company or individual are also punishable by civil penalties of up to $16,000 per violation.
As with the anti-bribery provisions, companies and individuals can incur substantial penalties for violating the accounting provisions. For companies, a criminal conviction is punishable by a fine of up to $25 million per violation, and civil violations are subject to a penalty of either the gross amount of the monetary gain to the company or between $75,000 and $725,000. For individuals, a criminal conviction is punishable by a fine of up to $5 million per violation and imprisonment for up to 20 years. A civil violation is subject to a penalty of either the gross amount of the monetary gain to the individual or between $7,500 and $150,000.

Prioritizing Compliance

With FCPA enforcement on the rise, it is advisable that Israeli corporations begin to assess the efficacy of their compliance offices and those of their subsidiaries. The broad extraterritorial reach of the FCPA permits even short meetings, emails, text messages and phone calls to result in severe penalties. However, Israeli corporations can reduce their exposure to FCPA violations by maintaining high ethical standards and proactively reviewing their compliance standards, including enacting vigorous anti-bribery policies, establishing adequate oversight training and resources for both employees and contractors, as well as maintaining routine audits to assure compliance and instituting mechanisms to quickly address FCPA violations when they are discovered.

U.S. Congress Takes the Wheel on Autonomous Vehicles

By Meital Stavinsky

The year 2017 marks the elevation of Israel to global recognition as an advanced transportation technologies hub. It also marks the first notable moves by the U.S. Congress to regulate self-driving vehicles (SDVs). In view of the magnitude of the U.S. transportation industry and its worldwide impact, Israeli companies operating in the innovative transportation sector have much to learn, and also much to gain, by carefully monitoring developments in the legislative and regulatory framework for the U.S. transportation industry.

Startups Disrupt the Transportation Industry

Frost & Sullivan's April 2017 study found that more than 1,700 startups focused on electrification, mobility and connected car technologies are rapidly gaining traction and disrupting the global automotive and mobility industries. Although most North America startups are currently based in California's Silicon Valley, others have been expanding their activity in the Detroit area to attract engineering talent from traditional car manufacturers and engage with original equipment manufacturers (OEMs) in their Detroit-area facilities.

Signs abound that the transportation industry is undergoing a radical transformation, and traditional participants are challenged on all sides by changing technology and new business models. Artificial vision and intelligence-based camera and sensor solutions, SDVs and connected car technologies, the electrification of vehicles and machine learning are but a few of the innovations poised to not only revolutionize the market but even to render much of the conventional transportation industry obsolete. In response, established manufacturers are rolling out new kinds of vehicles and attempting to incorporate innovative features, while leading transportation OEMs are developing in-house or sponsored platforms to incubate promising startups.

Israel: A Hub For Innovation in Transportation Technology

The Frost & Sullivan study highlights regional focal points that have advanced rapidly in specific related fields. Israel is featured prominently in this regard, with more than 300 startups focusing on cybersecurity, smart mobility, artificial intelligence, smart cities and alternative fuels.

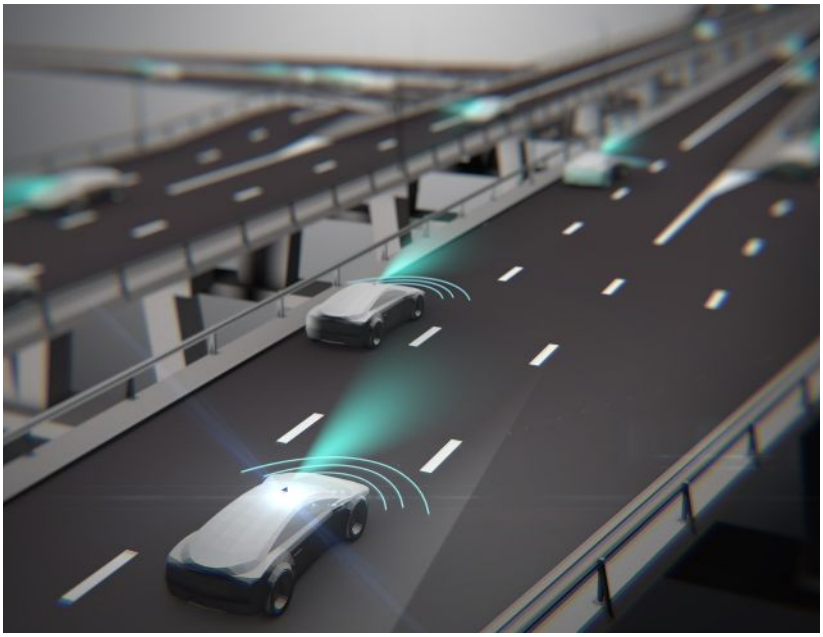
The State of Israel's commitment to advancing related technologies is clear. Israel's Fuel Choices and Smart Mobility Initiative, a national program for alternative fuels and transportation, was established in 2011. In January 2017, the government of Israel approved NIS 250 million (approximately $71.4 million) to be spread over five years as part of the national plan for smart mobility. This program has two main objectives: 1) to strengthen Israel as a center of knowledge on smart mobility and 2) to promote innovative solutions for transportation within Israel (which, if successful, will be deployed abroad). The national plan for smart mobility complements the national plan for alternative fuels.

In March 2017, Israel's Mobileye, a company that develops vision-based, advanced driver-assistance systems, was acquired for $15 billion by Intel. The importance of this acquisition goes far beyond the immediate effect on Israel's advanced transportation technologies industry, and suggests a broader pattern in which Israel is considered a prime source of fundamental advances in useful technologies. Long before the Mobileye acquisition, the industry in Israel had been targeted by leading car manufacturers and venture capitalists, and there is every reason to believe this will continue and accelerate.

The range of technologies related to evolving SDV deployment and infrastructure includes many technology sectors where Israel has been a leading player for decades. SDVs and connected vehicles, for example, require robust data communication between vehicles, the cloud and an infrastructure. SDV solutions developed in Israel have led to a number of "byproducts" instrumental for the development of a new transportation environment, including, among others, new ideas for the collection of data and processing, mapping, vehicle cybersecurity, artificial intelligence and sensors to measure the comfort and health of drivers. Moreover, a number of new electrification technologies are being developed in Israel and are positioned to have a tremendous impact as well: superfast charging of next-generation electric vehicle batteries, wireless charging of electric buses and kinetic storage for electric vehicles, among others. Private and public traffic management is also a key objective, and companies in Israel are already providing real-time scheduling solutions for public transportation and "smart" traffic light sensors to reduce congestion.

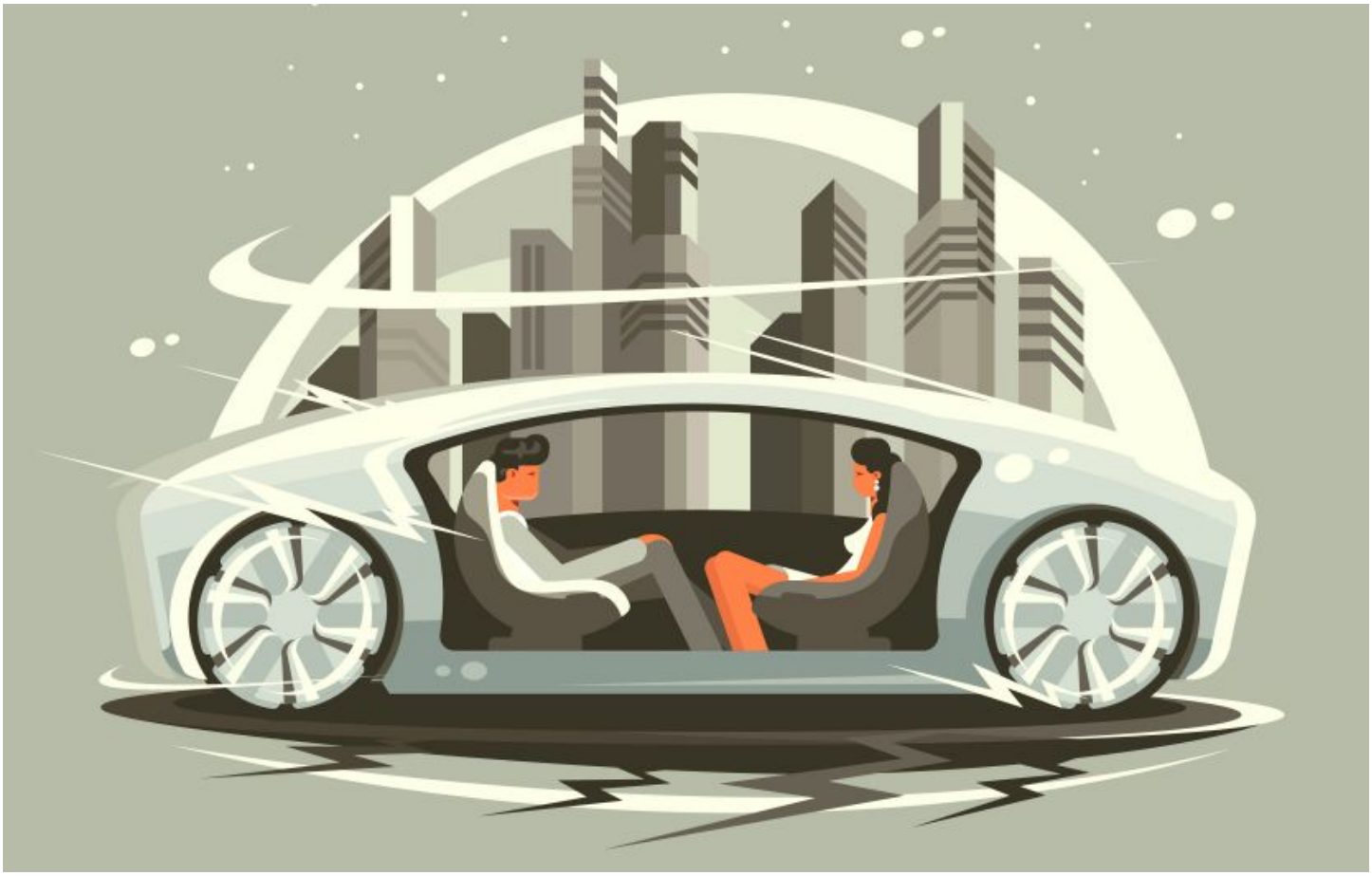
Paving the Way for Deployment of SDVs in the U.S.

Approximately 250 million vehicles are currently registered in the U.S., 10 million of which are freight vehicles (two-plus axles, six-plus tires). A 2014 study by the U.S. National Highway Traffic Safety Administration (NHTSA) found that the economic and societal harm from the increasing number of motor vehicle collisions in the U.S. totals $871 billion annually. A 2015 NHTSA study found that 94 percent of collisions were due to human error.



By contributing to a decrease in accidents caused by human error, SDVs are likely to save many thousands of lives a year in the U.S., reduce injuries, and deliver life-changing freedom and independence to seniors and people with disabilities, as well as providing sustainability benefits.

The U.S. Congress recognizes that some regulatory limits must be set, in an attempt to balance safety and innovation. Among other intiatives, bipartisan U.S. SDV legislation – such as House Bill H.R. 3388 (SELF DRIVE Act) and Senate Bill S.1885 (AV START Act) – would limit the role of the states in regulating certain aspects of SDVs and allow for certain exemptions from U.S. Federal Motor Vehicle Safety Standards. Although the legislation provides tools to expedite passenger SDV deployment in the U.S., it seems, as of the time of publication, that autonomous commercial vehicles (ACVs) exceeding 10,000 pounds and carrying more than 10 occupants would be left out. The main concern expressed by proponents of the exclusion of trucks is that the legislation would otherwise result in the elimination of approximately 3 million truck drivers' jobs in the U.S. In 2012, there were 300,000 collisions involving trucks in the U.S., so it may be expected that, ultimately, safety considerations will bring the issue of ACVs to the forefront as well.



In addition to efforts in Congress, on Sept. 12, 2017, the NHTSA released voluntary guidance with respect to the development and regulation of SDVs. The new NHTSA guidance, "Automated Driving Systems: a Vision for Safety 2.0," replaces the September 2016 NHTSA guidance issued by the Obama Administration. The updated document offers voluntary guidance to car manufacturers and emphasizes the primary regulatory role of the federal government. The guidance has been criticized by some as being too accommodating to the industry. In any event, the guidance is likely to be further revised as more information becomes available next year.

The Fall 2017 issue of the online magazine *Resources*, in an article titled "Is the Future Now? Autonomous Vehicle Technology and Consumer Demand," discusses a study published in March 2017 that found the average household is willing to pay a significant amount for autonomous transportation features: about $3,500 for partial automation and $4,900 for full automation. It took decades for the transportation industry, U.S. Congress and the federal government to adopt such life-saving technologies as seatbelts and airbags. The arrival of SDVs, however, seems to be approaching much faster in drivers' rearview mirrors.

About Our Transportation Team

Companies across the transport industry are working to develop today's vision into tomorrow's reality – from intercity transportation to global transport. To exploit emerging opportunities, the world's leading transportation companies and service providers are turning to Holland & Knight because of our extensive experience, our deep knowledge and our prompt responsiveness.

With a long history of representing clients in transportation matters, we advise clients at nearly every point in the supply and distribution chains and deal with the myriad issues that have emerged in the industry, including self-driving vehicles. (See Holland & Knight's alerts, "Autonomous Vehicles Continue to Move Forward," Nov. 6, 2017; "Autonomous Commercial Vehicles Closer to Hitting the Road After New Developments," Sept. 25, 2017; "Buckle Up: Autonomous Commercial Vehicles are Coming to a Road Near You," July 24, 2017; and "Are You Ready for Self-Driving Vehicles?", Jan. 11, 2017.)

Treasury Report Highlights Changing Environment for Real Estate Finance Online

By David P. Sofge

A report on ways to boost capital markets released by the U.S. Department of the Treasury in October highlights the expanding options for real estate financing online. The report reviews progress to date under the Jumpstart Our Business Startups (JOBS) Act of 2012, which was intended to promote capital formation and job growth generally but also has proven to be unexpectedly useful in private placement transactions for real estate investment.

Below is a quick look at how some of the major channels for real estate financing are being affected by new rules under the JOBS Act and advancing technology.

Regulation D, Rule 506(b): The traditional private placement exemption for offers and sale to investors where there is a substantive pre-existing relationship (that is, where the relationship does not result from any general solicitation). Still the most common and largest by volume for private placements of realty interests. Changes here have been due to the appearance of a vast number of new technology-based service providers facilitating information flows.

In addition, 506(b) offers were boosted by a 2015 no-action letter from the U.S. Securities and Exchange Commission (SEC) saying that a "substantive" relationship may be established without the passage of any particular time period. (It previously had been assumed, based on earlier SEC guidance, that at an acquaintance of at least 30 days was required before an offer could be made.) The required relationship can now be created and developed on a website and possibly a few follow-up calls. Said the SEC: "We agree that the quality of the relationship between an issuer (or its agent) and an investor is the most important factor in determining whether a "substantive" relationship exists." It's the quality time that counts.

Regulation D, Rule 506(c) (JOBS Act Title II): Newly created under the JOBS Act and allowing general solicitation, including on the web, so long as reasonable steps are taken to verify that all purchasers are accredited investors. Although the big excitement and an explosion of new intermediary platforms are here, 506(c) still accounts for only about 3 percent of the capital raised under Regulation D through 2016: $107.7 billion, compared to $2.2 trillion under 506(b). As a related point, a vast new ecosystem of companies has sprung up to provide verifications of accredited investor status as well as "Know Your Customer" (KYC), anti-money laundering (AML), and other regulatory compliance functions for 506(c) and the entire range of permissible online investment activity.

Regulation CF (JOBS Act Title III): The long-awaited "true equity crowdfunding" accessible by non-accredited investors became effective in March 2016 to great acclaim, but it has gotten off to a slow start. Most blame the cost and complexity compared with private placements (filing and reporting requirements apply), as well as the offering limit (maximum $1.07 million per issuer in one year), making it unusable for most commercial real estate deals. Changes including an increase in the offering limits are under discussion in Congress.

Regulation A+ (JOBS Act Title IV): A surprise success. The long-moribund Regulation A sector for "mini-public offerings" was overhauled and streamlined by the JOBS Act, with two tiers now available: $20 million and $50 million. Contrary to many predictions, Reg A+ (an unofficial name now in general use) has gained traction. The Treasury Department report shows 147 Reg A+ offerings in the year after implementation, up from 27 in the preceding four years under the old Reg A. The average size of the post-JOBS offerings was approximately $18 million, for an aggregate of $2.6 billion. This is still far below the levels for Reg D offerings, but Reg A+ offerings show an upward trajectory, particularly for larger commercial real estate projects.

Not discussed in the Treasury report but looming on the horizon is the possible use of "initial coin offerings" (ICOs) for offerings of tokens representing or backed by interests in real estate. An early attempt at this was quickly shut down by the SEC as a fraud, but the idea has momentum. It is expected that other offerings – including some with legitimate business plans and compliant offering structures – will appear soon.

As a final note, the Treasury report is a snapshot of an industry in a period of rapid development, with U.S. (and other) regulators actively seeking to apply the twin principles of their mandate – supporting the effectiveness of capital markets and assuring investor protection – to an expanding, technology-based ecosystem for real estate transactions.

Digital Health: FDA's New Genetic Testing Policy Continues Streamlined Approach

By Michael J. Werner

In another example of the U.S. Food and Drug Administration's (FDA) revision of regulatory policies for digital health products, Commissioner Scott Gottlieb announced on Nov. 6, 2017, that the agency is extending its precertification model to low-risk, direct-to-consumer genetic risk tests.

Under the new policy, genetic health risk (GHR) tests will be exempt from premarket review under certain conditions. If and when the policy is finalized, manufacturers of these types of tests would receive a one-time review to ensure that they meet the FDA's requirements, after which manufacturers may enter the market with new GHR tests without further review. In a separate order, the agency also established special controls for these tests that outline requirements for assuring the tests' accuracy, reliability and clinical relevance as well as describe the type of studies and data required to demonstrate performance of certain types of genetic tests.

In a statement announcing the new policy, Gottlieb noted the importance of GHR tests to help people gain insight into their predisposition to certain illnesses or diseases. He also pointed out that more and more of these tests are being developed and marketed to consumers directly. While this can provide consumers access to more information, he said, FDA regulation is needed to ensure the quality of the tests. Gottlieb said that, with the new policy, "FDA seeks to strike a balance that provides for an efficient pathway to bring these tests to consumers, without sacrificing the assurances offered by FDA oversight."

In addition, Gottlieb announced that FDA has classified certain tests to evaluate vitamin D levels in class II, subject to special controls, and announced its intent to exempt these tests from premarket review. The FDA also issued a final order exempting genetic carrier screening tests from premarket review.

Continuation of a Trend

This regulatory approach continues the FDA's efforts to streamline and in some cases reduce regulation for digital health technologies. Since early this year, the agency has taken several steps to streamline regulation of these technologies. These actions came on the heels of the 21st Century Cures Act, legislation enacted in late 2016 that codified FDA rules governing digital health technologies, including clinical support programs.

The approach proposed by Gottlieb for GHR tests is similar to the proposed manufacturer-based, pre-certification model developed for other digital health technologies launched by FDA earlier this year. Under that program, the developers of medical software receive FDA certification of fitness and not the products themselves. Gottlieb said that the FDA will keep looking for ways to use this regulatory model for new tests and novel technologies.

U.S. Focus on Strengthening Cybersecurity Provides Opportunity for Israeli Firms

By Norma M. Krayem

Cybersecurity is a critical issue for the U.S. and Israel. The two countries have collaborated for many years on ways to manage cybersecurity risks, and Israeli companies are well known for their cybersecurity skill sets. The recent cybersecurity Executive Order (EO), described below, lays out key U.S. priorities for cybersecurity that govern the direction the U.S. government will go in managing its own risk, with a comprehensive cybersecurity plan for the U.S. coming shortly. U.S. owners and operators of critical infrastructure are working to manage their risk every day as well. This presents opportunities for Israeli firms to work collaboratively with the U.S. government and the private sector to find new solutions to managing cyber risk. Each sector is regulated in different ways for cybersecurity and the U.S. government has specific contracting requirements, all of which Holland & Knight can help companies understand and navigate.

Earlier this year, President Donald Trump signed a long-anticipated cybersecurity Executive Order (EO) entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The White House and the U.S. Department of Homeland Security (DHS) are now working on a comprehensive cybersecurity plan which is expected to be rolled out later this year and early in 2018.

The EO represents President Trump's first major cybersecurity policy, which aims to strengthen the security of the federal government's information technology (IT) infrastructure, increase cybersecurity protection measures for critical infrastructure (CI) and train a new generation of cybersecurity workforce. The Executive Order is broken down into three sections: 1) Cybersecurity of Federal Networks, 2) Cybersecurity of Critical Infrastructure and 3) Cybersecurity for the Nation. Notably, Homeland Security Advisor Tom Bossert said when announcing the signing of the EO: "I think the trend is going in the wrong direction in cyberspace, and it's time to stop that trend and reverse it on behalf of the American people."

The following is a quick overview of the EO. Implementation by the White House – with many federal agencies involved as they work directly with companies – will be a lengthy but important process in which some of Israel's top cybersecurity firms may be able to usefully engage.

Section 1: Cybersecurity of Federal Networks

Section 1 reinforces the need to "build and maintain a modern, secure, and more resilient executive branch IT architecture." Specifically, the EO requires each Executive Branch agency to use the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and successor documents, to manage each agency's own cybersecurity risk. Previously, the focus for use of the NIST Framework had been on the private sector.

The order also tasks Chris Liddell, named to the newly created position of Director of the American Technology Council, to work with DHS, the Office of Management and Budget (OMB) and the General Services Administration (GSA) to submit a report to the President with recommendations on a plan to modernize Federal IT.

Section 2: Cybersecurity of Critical Infrastructure

Section 2 represents one of the most-awaited areas of the new cybersecurity EO, focusing on the cyber risks that Critical Infrastructure faces and continuing the policies established in the Obama Administration's 2013 EO 13636 ("Improving Critical Infrastructure Cybersecurity"). Section 2 similarly requires sweeping reviews of private sector cybersecurity initiatives in order to identify areas of improvement needed to support CI's ability to manage and sustain itself against cyberattacks, as well as calling on the Executive Branch to provide "Support to Critical Infrastructure at Greatest Risk."

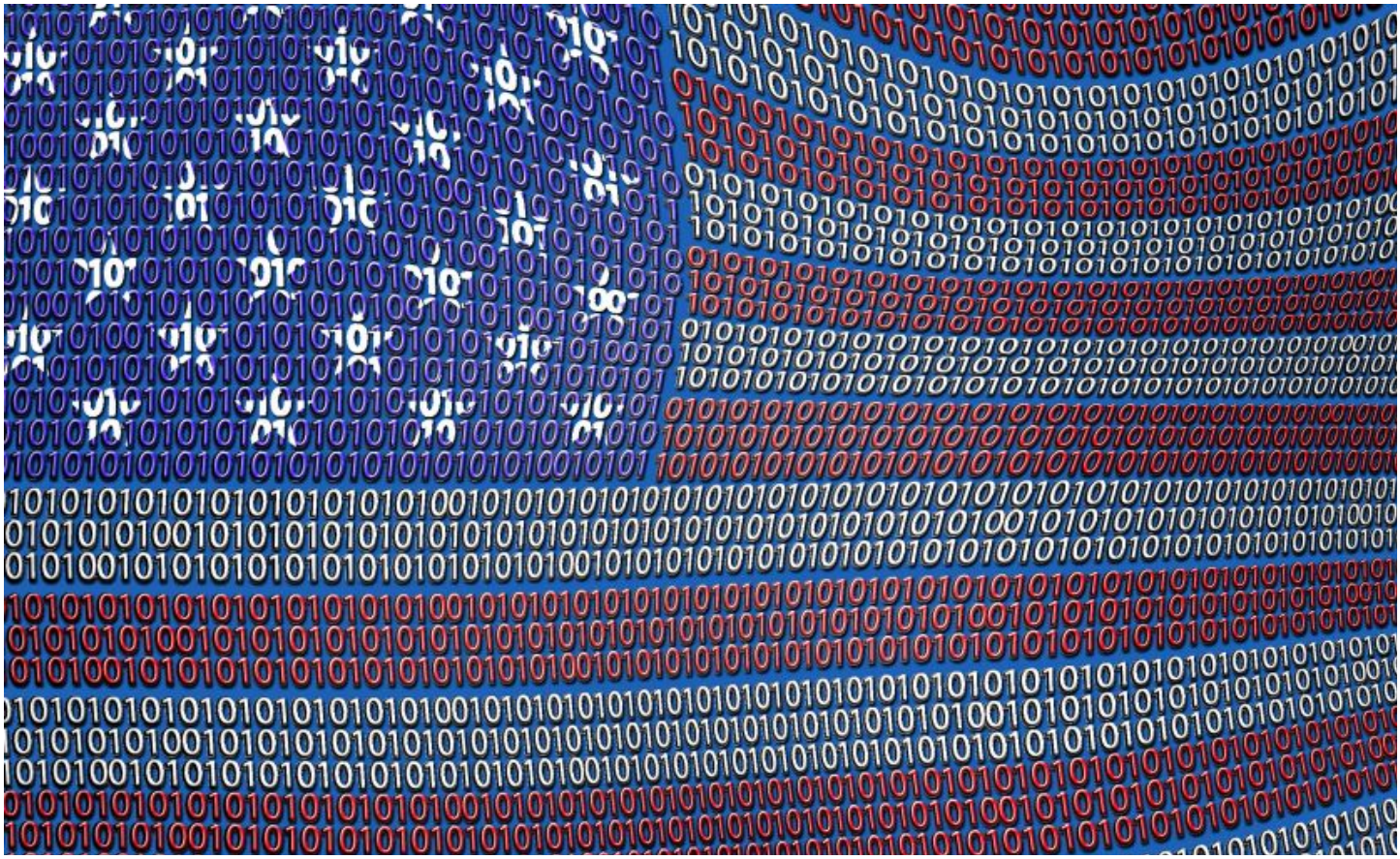
President Trump's EO directs DHS, in coordination with the U.S. Department of Defense (DOD), the Attorney General, the Director of National Intelligence, the Director of the FBI and the heads of appropriate sector-specific agencies to work with the private sector to address cyber risks to CI companies and sets out actions the agencies should take to support the companies' risk management efforts.

Supporting Transparency in the Marketplace: The EO cites potential issues with the cybersecurity efforts of publicly traded CI companies, calling for a report to be submitted to the President within 90 days, led by DHS and the Department of Commerce (DOC), to "examine the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities."

Resilience Against Botnets and Other Automated, Distributed Threats: Botnets and other similar threats bring shared risk across all CI ecosystems. DOC and DHS are directed to "lead an open and transparent process to identify and promote action by appropriate stakeholders to better collaborate and protect against botnets." The report must be publicly available in 240 days from the EO, with a final report within one year.

Assessment of Electricity Disruption Incident Response Capabilities: The EO specifically cites to risks in the electricity sector and directs the U.S. Department of Energy (DOE) and DHS, in consultation with the Director of National Intelligence and along with state and local governments, to look at "the potential scope and duration of a prolonged power outage associated with a significant cyber incident as defined in Presidential Policy Directive 41 against the electricity sector; the readiness of the United States to manage the consequences of such an incident; and any gaps or shortcomings in assets or capabilities to mitigate the consequences of such an incident."

Department of Defense Warfighting Capabilities and Industrial Base: Interestingly, the Defense Industrial Base (DIB) was also cited separately in the EO based on "cybersecurity risks facing the defense industrial base, its supply chain, and U.S. military platforms, systems, networks and capabilities." DOD, DHS and the FBI, in coordination with the Director of National Intelligence, had 90 days to provide a report to the President on both the risks and recommendations for addressing them.



Section 3: Cybersecurity for the Nation

Section 3 outlines a number of other key items that the Administration is concerned about, including the needs to:

- create an improved cyber deterrence policy focusing on "strategic options for deterring adversaries and better protecting the American people from cyber threats"

- focus on international cooperation and priorities, including the need to maintain a "globally secure and resilient internet," working with our allies around the world on "attribution, cyber threat information sharing, response, capacity building, and cooperation"

- prioritize cybersecurity workforce development, focusing on the need to find, educate and create the next generation of cybersecurity workforce to better meet the needs of the public and private sectors.

Cybersecurity ultimately represents a national and economic security threat to the United States. What is important about this Executive Order, the work of the Executive Branch and Congress on cybersecurity is the awareness that more needs to be done to address the challenges both within the U.S. government, with the U.S. private sector and around the world. The EO lays out a road map to better understand how the U.S. looks at the threat and where the future may go on policy, regulatory and legal issues — establishing a structure to provide solutions for a variety of sectors, including autonomous vehicles, health and medical devices, banking and financial services, defense and beyond.

About Our Israel Practice

With an intimate understanding of the Israeli economic, political and social environment, members of Holland & Knight's Israel Practice Team provide a wide array of legal services to both Israeli clients operating abroad and companies and investors doing business in Israel.

Areas of legal guidance typically provided to our Israel Practice clients include real estate, mergers and acquisitions, private equity, international tax, cross border and customs, internet privacy and cybersecurity, intellectual property, government lobbying, regulations and compliance, U.S. Foreign Corrupt Practices Act (FCPA), U.S. Foreign Account Tax Compliance Act (FATCA), and litigation and dispute resolution.

Our lawyers have extensive experience with outbound projects and regularly represent clients from the region. A core value of Holland & Knight is our dedication to delivering the highest quality of legal services and providing responsive and cost-effective counsel to every client. This core value of the firm – coupled with our business acumen, legal experience and solid commitment to the Israeli marketplace – enables us to successfully assist our Israeli clients operating in the United States, as well as companies and investors doing business in Israel.

About This Newsletter

Information contained in this newsletter is for the general education and knowledge of our readers. It is not designed to be, and should not be used as, the sole source of information when analyzing and resolving a legal problem. Moreover, the laws of each jurisdiction are different and are constantly changing. If you have specific questions regarding a particular fact situation, we urge you to consult competent legal counsel. Holland & Knight lawyers are available to make presentations on a wide variety of Israel-related issues.

For inquiries regarding this newsletter, you may contact:

Ronald J. Klein
Co-Chair, Israel Practice
Fort Lauderdale | +1.954.468.7874
Washington, D.C. | +1.202.469.5152
ron.klein@hklaw.com

Meital Stavinsky
Co-Chair, Israel Practice
Miami | +1.305.789.7710
Washington, D.C. | +1.202.828.5004
meital.stavinsky@hklaw.com

Wifredo A. Ferrer
Partner, Litigation
Miami | +1.305.789.7780
wifredo.ferrer@hklaw.com

David P. Sofge
Partner, Corporate
Fort Lauderdale | +1.954.468.7884
david.sofge@hklaw.com

Norma M. Krayem
Senior Policy Advisor,
Public Policy and Regulation
Washington, D.C. | +1.202.469.5195
norma.krayem@hklaw.com

Michael J. Werner
Partner,
Public Policy and Regulation
Washington, D.C. | +1.202.419.2515
michael.werner@hklaw.com

Alec M. Puig
Associate, Litigation
Miami | +1.305.789.7558
alec.puig@hklaw.com

About the Authors

Wifredo A. Ferrer, the former United States Attorney for the Southern District of Florida, is a Miami litigation attorney who is the Chair of Holland & Knight's Global Compliance and Investigations Team. Mr. Ferrer focuses his practice primarily on internal corporate investigations, corporate compliance and training, and white collar criminal defense with special attention to matters arising from or connected to Latin America. Prior to joining Holland & Knight, Mr. Ferrer served nearly seven years as the U.S. Attorney for the Southern District of Florida.

Alec M. Puig is a Miami attorney in Holland & Knight's Litigation and Dispute Resolution Practice. Mr. Puig is experienced in matters involving general commercial and corporate litigation, representing both international and domestic clients.

Meital Stavinsky is a Miami and Washington D.C. attorney, member of Holland & Knight's Public Policy & Regulation Group and co-chair of the firm's Israel Practice. She focuses her practice on business and government relations, with a particular emphasis on Israeli emerging and advanced technologies companies. Ms. Stavinsky assists Israeli companies seeking to enter the U.S. market and expand their operations in the United States. She has successfully matched Israeli companies with strategic partners, potential joint ventures and other business-to-business connections.

David P. Sofge is an attorney in Holland & Knight's Fort Lauderdale office. He represents public and private companies in corporate and financing transactions and regulatory compliance.

Michael J. Werner is a Washington, D.C., public policy and regulatory attorney and a co-leader of Holland & Knight's Healthcare & Life Sciences Team. Mr. Werner has almost three decades of healthcare law, lobbying, regulatory and reimbursement experience in Washington.

Norma M. Krayem is a senior policy advisor in Holland & Knight's Washington, D.C., office and co-chair of the firm's Cybersecurity and Privacy Team, as well as a member of the Public Policy & Regulation Group. Ms. Krayem provides strategic advice on key issues in a range of areas, including homeland security, transportation, defense, international trade and environmental, as well as appropriations issues for all aspects of critical infrastructure. She also focuses on the impacts of cyber and privacy issues on the banking and financial services, energy, communications, health, transportation and other critical sectors.

Contact Our Israel Practice Attorneys


David B. Allswang | Chicago
+1.312.578.6677 | david.allswang@hklaw.com


Adam J. August | Tysons
+1.703.720.8059 | adam.august@hklaw.com


Stephen J. Double | New York
+1.212.513.3528 | stephen.double@hklaw.com


Marjorie F. Gannett | Washington, D.C.
+1 202.469.5187 | marjorie.gannett@hklaw.com


Jessica H. Hoch | Miami
+1.407.244.1138 | jessica.hoch@hklaw.com


Ronald J. Klein | Fort Lauderdale
+1.954.468.7874 | ron.klein@hklaw.com


James T. Mayer | Chicago
+1.312.715.5841 | james.mayer@hklaw.com


Barton W. Morrison | Orlando
+1.407.244.1131 | barton.morrison@hklaw.com


Doug A. Praw | Los Angeles
+1.213.896.2588 | doug.praw@hklaw.com


Stuart M. Saft | New York
+1.212.513.3308 | stuart.saft@hklaw.com


Janis B. Schiff | Washington, D.C.
+1.202.862.5994 | janis.schiff@hklaw.com


William B. Sherman | Fort Lauderdale
+1.954.468.7902 | bill.sherman@hklaw.com


David P. Sofge | Fort Lauderdale
+1.954.468.7884 | david.sofge@hklaw.com


Meital Stavinsky | Miami
+1.305.789.7710 | meital.stavinsky@hklaw.com


Erez I. Tucner | New York
+1.212.513.3417 | erez.tucner@hklaw.com


Michael J. Werner | Washington, D.C.
+1.202.419.2515 | michael.werner@hklaw.com


Jose V. Zapata | Bogotá
+57.1.745.5940 | jose.zapata@hklaw.com