Client Alert.

February 22, 2013

White House Announces the Administration Strategy on Mitigating the Theft of U.S. Trade Secrets

By Daniel P. Westman and Jessica N. Childress

On February 20, 2013, the White House released the Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (the "Strategy"), which "recognizes the crucial role of trade secrets in the U.S. economy and sets out a means for improved coordination within the U.S. government to protect them."[1] The Strategy articulates a five-pronged approach including (1) diplomatic efforts to protect trade secrets overseas, (2) promotion of voluntary best practices by private industry to protect trade secrets, (3) enhancement of domestic law enforcement, (4) improvement of domestic legislation, and (5) public awareness and stakeholder outreach. Emphasizing its importance, the Strategy was announced jointly by U.S. Attorney General Eric Holder, U.S. Intellectual Property Enforcement Coordinator Victoria Espinel, and U.S. Department of Commerce Deputy Secretary Rebecca Blank.

The announcement of the Strategy culminates an intense sixty-day period of federal activity with respect to trade secret protection that includes the enactment of the Theft of Trade Secrets Clarification Act ("Clarification Act") and the Foreign and Economic Espionage Penalty Enhancement Act of 2012 ("Enhancement Act"). The Strategy suggests that additional federal legislation may be appropriate. After an overview of the Strategy, this Alert discusses the Clarification Act, the Enhancement Act, a proposed amendment that would create a private civil right of action under the federal Economic Espionage Act of 1996 ("EEA"), and practical steps companies may take in light of the Strategy.

A. Overview of the Strategy

The Strategy quotes a note of urgency sounded by President Obama in his State of the Union address: "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[2] The Strategy echoes that urgency, stating that "[e]merging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is increasing."[3]

1. Diplomatic Efforts to Protect Trade Secrets Overseas

The Strategy recognizes that theft of U.S. trade secrets often is committed by persons outside of the U.S. including "[f]oreign competitors of U.S. corporations, some with ties to foreign governments…."[4] Accordingly, the

[1] The Administration Strategy on Mitigating the Theft of U.S. Trade Secrets is available at: http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (last accessed Feb. 21, 2013).

[2] Id. at 1.

[3] Id.

[4] Id.

Strategy states that "[t]he Administration will continue to apply sustained and coordinated diplomatic pressure on other countries to discourage trade secret theft."[5] The Strategy also provides that the Administration will use trade policy tools, such as the Trans Pacific Partnership and the Trade-Related Aspects of Intellectual Property Rights Council, and other methods to urge increased international enforcement against trade secret theft. Further, the Strategy provides that the Departments of Justice, Commerce, State, Treasury, and Homeland Security will work with global organizations to strengthen international enforcement efforts.

2. Voluntary Best Practices by Private Industry to Protect Trade Secrets

The Strategy observes that "[a]dvancements in technology, increased mobility, rapid globalization, and the anonymous or pseudonymous nature of the Internet create growing challenges in protecting trade secrets. Companies need to consider whether their approaches to protecting trade secrets [keep] pace with technology…."[6] The U.S. Intellectual Property Enforcement Coordinator ("IPEC") is charged with working with appropriate agencies, including the Departments of Justice and State, to help develop "industry led best practices to protect trade secrets."[7] However, the Strategy is careful to state that "[i]dentified best practices may not be suitable for every company or organization," that reasonable measures to protect trade secrets may vary by company and by industry, and that identified best practices are not intended to set a minimum standard.[8] The Strategy suggests that companies review their policies and practices with respect to compartmentalization of research and development, information security, physical security, and human resources.

3. Enhancing Domestic Law Enforcement

The Strategy states that the Department of Justice and the FBI have made "investigation and prosecution of corporate and state sponsored trade secret theft a top priority."[9] The Strategy also implicitly recognizes that the government may be better positioned to collect, analyze, and report about trade secret theft than any single private-sector entity. Accordingly, to keep the private sector up to date with the types of threats to trade secrets that the law enforcement and intelligence communities are observing, the Strategy provides that the Office of the Director of National Intelligence will coordinate with the government's intelligence community to inform the private sector about ways to identify and prevent trade secret theft. As an example of intelligence sharing, the Strategy cites a report from the Office of the National Counterintelligence Executive ("ONCIX") that identifies private industries at most risk, and identifies characteristics of businesses that make them more vulnerable to trade secret theft.[10] Further, the Strategy provides that the Department of Justice, the FBI, and the Department of Defense will continue to engage in educational efforts with the private sector.

---

[5] Id. at 3.

[6] Id. at 6.

[7] Id.

[8] Id.

[9] Id. at 7.

[10] The ONCIX Report, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," October 2011, is available at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (last accessed Feb. 21, 2013). The industries identified as most at risk include (i) information and communications technology; (ii) scarce natural resources; (iii) military technologies including marine systems, unmanned aerial vehicles, and aerospace/aeronautic technologies; and (iv) fast-growth industries such as clean energy, health care, and pharmaceuticals. The characteristics identified as making businesses more vulnerable include (i) use of portable devices; (ii) globalization of business activities; (iii) electronic storage of sensitive information; (iv) storage of information in the "cloud"; and (v) companies with employees who work remotely.

4. Improving Domestic Legislation

The Strategy notes that President Obama signed the Clarification Act and the Enhancement Act, both of which are discussed below. In addition, the IPEC is charged with reviewing existing federal laws within 120 days to determine whether changes are advisable.

5. Public Awareness and Stakeholder Outreach

The Strategy states that education of the public will continue through various methods, and mentions as an example the FBI's publication "Economic Espionage – How to Spot an Insider Threat."[11]

B. Other Significant Federal Developments in the Last Sixty Days

1. The Clarification Act

The Clarification Act was enacted on December 28, 2012, in response to the holding of *United States v. Aleynikov*,[12] in which the Second Circuit reversed the conviction under the EEA of Sergey Aleynikov, a Goldman Sachs software programmer who stole High Frequency Trading ("HFT") source code from Goldman Sachs before terminating his employment with Goldman Sachs to work for another company that sought to develop HFT code. The Second Circuit found that the HFT code that Aleynikov had taken from Goldman Sachs had not been "produced for" or "placed in" interstate commerce or foreign commerce. Observing that Goldman did not intend to sell the HFT code, the Second Circuit concluded that the code was not "produced for" and had not been "placed" in interstate and foreign commerce, and therefore Aleynikov did not violate the EEA. In reaction to the acquittal of Aleynikov, the Clarification Act amended the EEA to apply to any trade secret "that is related to a product or service used in or intended for use in interstate or foreign commerce." Accordingly, the Clarification Act expands the EEA to allow federal prosecutors to pursue cases of trade secret misappropriation related to products and services that companies do not necessarily sell in interstate or foreign commerce, but that are used internally.

2. The Enhancement Act

The Enhancement Act was signed into law on January 14, 2013, and significantly increased the criminal penalties available under the EEA for violations that benefit a foreign government. Maximum fines for individuals have been increased from $500,000 to $5 million. Maximum fines for corporations have been increased from a cap of $10 million to the greater of (i) $10 million or (ii) the trebled value that the organization derived from the misappropriated trade secret. The maximum term of imprisonment has been increased from fifteen to twenty years.

C. Potential Future Federal Legislation

As noted above, the IPEC is charged with reviewing existing federal law to determine whether enhancements to trade secret protection may be advisable. The IPEC's review likely will include consideration of proposed federal legislation which would amend the EEA by creating a private civil cause of action for misappropriation of trade secrets that is aimed in part at overseas misappropriation. The Protecting American Trade Secrets and Innovation Act of 2012 ("PATSIA") would limit the types of cases that could be brought in federal court by requiring higher

[11] Available at http://www.fbi.gov/news/stories/2012/may/insider_051112/ (last accessed Feb. 21, 2013).

[12] 676 F.3d 71 (2d Cir. 2012).

pleading standards for companies alleging trade secret misappropriation, such as "(A) describ[ing] with specificity the reasonable measures taken to protect the secrecy of the alleged trade secrets in dispute; and (B) includ[ing] a sworn representation by the party asserting the claim that the dispute involves either substantial need for nationwide service of process or misappropriation of trade secrets from the United States to another country."[13] PATSIA would explicitly authorize remedies aimed at preventing destruction of electronic evidence and fleeing the U.S., such *ex parte* applications to request the seizure of property related to the alleged misappropriated trade secret for a period of seventy-two hours.

D. Practical Steps Companies Should Consider

The Strategy is the first time that any President of the U.S. has called upon private industry, in the national interest, to engage in reviewing best practices for protection of trade secrets. This provides an excellent opportunity for employee training about data security. Now, companies may explain that their data security programs advance the national interest, not solely the corporate interest. Companies should consider discussing the Strategy and the recent federal legislation with employees during employee orientation, training sessions, and in particular, exit interviews. Departing employees who may be considering misappropriation of trade secrets may be deterred by learning about the priority that law enforcement has placed on investigating and prosecuting misappropriation cases. But new hires also need to understand that their new employers do not wish them to bring trade secrets from other companies, so that neither the new hire nor the new employer is embroiled in trade secret litigation.

The Strategy's call to private industry to develop and share information about best practices to protect trade secrets may provide an opportunity for companies that have not yet been victims of trade secret theft to learn about protecting trade secrets based on the collective experience of other companies. If the law enforcement and intelligence communities continue to share information about trade secret threats, and countermeasures to mitigate threats, companies may be able to strengthen existing data security programs. The Strategy's comments that any identified best practices are not intended to create a minimum standard may help companies tailor best practices to their own situations, with reduced concern that not following best practices will be deemed a failure to take reasonable efforts to protect trade secrets as required under trade secret law.

Contact:

Daniel P. Westman
(703) 760-7795
dwestman@mofo.com

[13] S. 3389, 112th Cong. (2d Sess. 2012). The text is available at: http://beta.congress.gov/112/bills/s3389/112s3389is_pdf.pdf (last accessed Feb. 21, 2013).

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.