Published on *The National Law Review* https://natlawreview.com

Administration Launches Strategy on Mitigating Theft of U.S. Trade Secrets

Article By:

Intellectual Property Practice Group

The strategy announced on February 20, 2013, should serve as both a wake-up call from the government and an offer of assistance. Given the losses that can arise from competitors' purposeful theft of trade secrets, entities should review the announcement and decide whether they need to be more active in protecting their trade secrets. The strategy also offers opportunities for increased collaboration with the government.

On February 20, 2013, the White House announced an "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets." Companies should view the announcement of this strategy as both a wake-up call from the government and an offer of assistance. Given the losses that can arise from competitors' purposeful theft of trade secrets, entities should review this government announcement and decide whether they need to be more active in protecting their trade secrets.

The administration strategy articulates a broad governmental commitment to addressing an "accelerating" threat to U.S. intellectual property. The strategy encompasses five action items:

- Focusing diplomatic efforts to protect trade secrets through diplomatic pressure, trade policy and cooperation with international entities
- Promoting voluntary best practices by private industry to protect trade secrets
- Enhancing domestic law enforcement, including through outreach and information-sharing with the private sector
- Improving domestic legislation to combat trade secret theft
- Improving public awareness and stakeholder outreach

Three main themes emerge from the administration strategy that are important for U.S. businesses.

First, the strategy and its supporting documentation highlight how frighteningly real the prospect of trade secrets theft is. The White House report is peppered with references to household name companies that have been victimized by trade secrets theft over the past few years, often at a cost of tens of millions of dollars or more. Mandated reports from the defense industry to the government indicate a 75 percent increase between FY2010 and FY2011 in reports of suspicious activity aimed at acquiring protected information. Coupled with a recent *New York Times* article asserting Chinese government involvement in more than 100 attempted cyber attacks on U.S. companies since 2006,

these reports warrant sitting up and taking notice. According to a report by the Office of the National Counterintelligence Executive, particular targets include companies that possess the following:

- Information and communications technologies
- Business information that relates to supplies of scarce natural resources or that gives foreign actors an edge in negotiations with U.S. businesses or the U.S. government
- Military technologies, particularly in connection with marine systems, unmanned aerial vehicles and other aerospace/aeronautic technologies
- Civilian and dual-use technologies in sectors likely to experience fast growth, such as clean energy, health care and pharmaceuticals, advanced materials and manufacturing techniques, and agricultural technology

Second, the government alone cannot solve the problem. The administration commits to making the investigation and prosecution of trade secret theft a "top priority" and states that the Federal Bureau of Investigation has increased the number of trade secret theft investigations by 29 percent since 2010. On its face, however, a 29 percent increase in investigations cannot keep pace with a 75 percent increase in attempted trade secret thefts. Historically, as a result of limited resources, the government has been able to address only a tiny fraction of trade secret thefts, and there is no indication that there will be the massive influx of resources necessary to change this dynamic materially. Indeed, the administration strategy recognizes the need for public-private partnerships on this issue and asks companies and industry associations to develop and adopt voluntary best practices to protect themselves against trade secret theft. And, of course, there are significant drawbacks to any after-the-fact solution, whether relying on government intervention or a private lawsuit.

The best solution is to prevent a trade secret theft from ever occurring. Even if that is not possible, having taken strong measures to protect trade secrets will aid success both in any civil litigation against the perpetrator and in any criminal action the government may bring. Entities should consider at least the following types of protective measures:

- Research and development compartmentalization, i.e., keeping information on a "need to know" basis, particularly where outside contractors are involved in any aspect of the process
- Information security policies, e.g., requiring multiple passwords or multi-factor authentication measures and providing for data encryption
- Physical security policies, e.g., using controlled access cards and an alarm system
- Human resources policies, e.g., using employee non-disclosure agreements, conducting employee training on the protection of trade secrets and performing exit interviews.

It also will be important in any future litigation that a company has clearly designated as confidential any materials it may wish to assert are trade secrets.

Third, the new administration approach to trade secrets offers some opportunities for U.S. companies.

The government interest in enhancing law enforcement operations indicates that businesses may have a better chance of encouraging the government to investigate and bring criminal charges under the **Economic Espionage Act (EEA)** against the perpetrators of trade secret thefts. The possibility of seeking government involvement is a powerful tool that should be considered and discussed with counsel any time there is a significant suspected trade secret theft. Obtaining government involvement in specific instances of trade secret theft can allow businesses to take advantage of

information learned via government tactics such as undercover investigations and search warrants. It also can significantly enhance any civil litigation—for example, a finding of criminal liability can make a civil outcome a foregone conclusion.

The administration strategy's focus on improving domestic legislation and increasing communication with the private sector suggests that there is an opportunity for the private sector to collaborate with government actors in communicating industry needs and shaping policy. For example, it is possible that the time is ripe for an amendment to the EEA (currently a federal criminal statute that offers no private right of action) to create a federal, private cause of action for misappropriation of trade secrets. A bill to this effect was introduced in Congress in 2012 and did not progress, but two other amendments to strengthen the EEA that passed overwhelmingly in December 2012, plus the recently issued administration strategy, suggest there may be gathering momentum for such a change.

In an executive order signed on February 12, 2013, entitled "Improving Critical Infrastructure Cybersecurity," President Obama outlined government plans to significantly increase the amount of information that the government shares with private sector entities about cyber threats. Specifically, the order directs government agencies to develop procedures to create and disseminate to targeted entities unclassified reports of cyber threats that identify them as targets, to disseminate classified reports of cyber threats under certain circumstances to "critical infrastructure entities," and to expand the Enhanced Cybersecurity Services program (previously available only to defense contractors to assist in information-sharing about cyber threats and protection of trade secrets) to "eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure." The directives in the executive order are in addition to and complement various information-sharing tactics set forth in the administration strategy designed to provide warnings, threat assessments and other information to industry. Companies, particularly those involved in the power grid or the provision of other utilities or critical systems, should be aware of the possibility of obtaining additional information from the government about threats to protected information.

National Law Review, Volume III, Number 60