Before the United States Sentencing Commission

Hearing on the Proposed Amendments to the Federal Sentencing Guidelines

March 13, 2013

Testimony of John W. Powell
American Superconductor Corporation ("AMSC"), Vice President and General Counsel

Mr. Chairman and members of the United States Sentencing Commission, thank you for inviting me to speak with you today. My name is John Powell, and I serve as the Vice President and General Counsel for AMSC. I would like to share with you the challenges that our company has faced over the past two years resulting from the theft of AMSC's valuable trade secret software source code and then provide you with my perspective on the amendments that are being considered for the Federal Sentencing Guidelines relating to trade secret theft and economic espionage.

AMSC Background

AMSC was founded in 1987 by several MIT professors with a mission to capitalize on the multi-billion-dollar potential they saw in what we now know as the Clean Technology Industry. Over the next two decades, with the help of the U.S. government and our investors, our company invested nearly a billion dollars to develop, demonstrate, patent, and produce a range of solutions that help to generate and distribute electric power. AMSC's product offerings include superconductor wire and superconductor wire based products, power electronic based electric grid stabilization systems, electrical control systems for wind turbines, and proprietary wind turbine designs. As of March 31, 2011, these investments were paying significant dividends for AMSC, for the U.S. and overseas economies, and for our shareholders. But it was at this point that our business and the personal lives of all AMSC employees abruptly changed.

The Theft of AMSC Trade Secrets

Among our core product offerings are proprietary wind turbine designs and electrical control systems for wind turbines. Our electrical control systems include both hardware and software – and they serve as the "brains" of the wind turbine, helping to convert and condition power flows, maximize power output, and monitor the turbine's performance. Our largest customer for these systems – and, in fact, our largest customer overall in 2011, accounting for approximately seventy five percent (75%) of AMSC's business – was Sinovel Wind Group Co. Ltd. ("Sinovel"). This Chinese company was founded in 2006. Its initial investors included New Horizon Capital, which was led by Winston Wen, the son of former Chinese Premier Wen Jiabao. Sinovel remains partially state owned to this day, with Dalian Heavy Industries, a state owned enterprise ("SOE") owning approximately twenty percent (20%) of the stock in the company.

Within just five years, Sinovel became the largest wind turbine manufacturer in China and the second largest wind turbine manufacturer in the world, producing thousands of wind turbines annually, primarily for the Chinese market. AMSC worked very closely with Sinovel from the very beginning helping them scale production, develop and field their next generation wind turbines, and stay at the forefront of the industry with our high-performance power electronics.

On March 31, 2011, however, our relationship changed abruptly when Sinovel refused contracted shipments from AMSC valued at approximately $70 million. Sinovel also failed to pay AMSC approximately $70 million for past product shipments that AMSC made to Sinovel. At this time, Sinovel told AMSC that the rejection of shipments was due to excess inventory at its factories. As you might expect, this sent our stock into a tailspin, losing forty percent (40%) of its value overnight.

From April through early June, AMSC executives tried repeatedly to resolve its issues with Sinovel, but all offers were ultimately rejected by Sinovel. In early June, AMSC saw several indications that Sinovel had gotten access to AMSC's wind turbine control software source code and that Sinovel was actively using this valuable trade secret within its wind turbines. These indications sparked an investigation that eventually led law enforcement in Austria to arrest

Dejan Karabasevic, a now former AMSC employee. Austrian law enforcement in cooperation with AMSC have compiled an extensive amount of evidence demonstrating how Dejan Karabasevic worked hand-in-hand with multiple senior-level Sinovel employees to steal AMSC's intellectual property and deploy it in thousands of Sinovel's wind turbines. The evidence includes:

- An extensive number of electronic communications between Dejan Karabasevic and multiple Sinovel employees, including messages containing the actual intellectual property transfers
- Contracts entered into between Dejan Karabasevic and Sinovel and parties related to Sinovel valued at more than $1.5 million
- Documentation demonstrating that Sinovel has been utilizing this stolen IP to upgrade its wind turbines in wind farms in China

Simply put, the case is exceptionally well documented and clear-cut. And, our former employee confessed to colluding with Sinovel, was convicted of economic espionage and fraudulent misuse of data, and was imprisoned in Austria. After completing the investigation with law enforcement in Austria, AMSC again approached Sinovel in an attempt to settle the contractual and criminal issues quietly. When these efforts failed and Sinovel denied any wrongdoing, AMSC filed the following civil and criminal actions:

- Beijing Arbitration Commission Case: AMSC is seeking approximately $70 million for past product shipments and enforcement of eight ongoing contracts, which are valued at approximately $700 million in total.

- Beijing Number 1 Intermediate Court Case #1: AMSC is seeking more than $400 million for misappropriation and use of its trade secret wind turbine control software source code. This is the largest intellectual property case ever undertaken in China.

- Beijing Number 1 Intermediate Court Case #2: Copyright infringement case against Sinovel for use and copying of AMSC's software in which AMSC is seeking

approximately $6 million in compensation and a cease and desist order for the infringing intellectual property.

- Hainan Number 1 Intermediate Court Case: Copyright case against Sinovel and its subsidiary, Guotong Electric, for use and copying of AMSC's software. In this case, AMSC is seeking a nominal amount of damages and a cease and a desist order for the infringing intellectual property.
- Chinese criminal complaint for trade secret theft filed with Beijing Public Security Bureau.
- Austrian criminal investigation instituted against Sinovel and certain employees and officers.

AMSC has invested more than $6 million in legal costs and one and one half years in time in this dispute with Sinovel. All legal cases are still pending and to date AMSC has not received any restitution from Sinovel. As a result of Sinovel's actions, AMSC has suffered hundreds of millions of dollars in loss, its annual revenues have fallen by 75%, its stock price has plummeted by 90% ($1+ billion loss to shareholders), and it has been forced to reduce its employee base by nearly 70%.

The threat of trade secret theft is very real and the impact can be devastating to U.S. companies and the U.S. economy. Therefore, I urge the Sentencing Commission to ensure that the Sentencing Guidelines be strengthened to the greatest extent possible to appropriately reflect the seriousness of trade secret offenses, account for the potential and actual harm caused by these offenses, and provide adequate deterrence against such offenses.

Comments on Proposed Amendments to the Federal Sentencing Guidelines Concerning Trade Secrets

I have reviewed the Commission's amendments to the Federal Sentencing Guidelines with a specific focus on the section concerning trade secrets and commend the Commission for taking action on this issue of vital importance.

I note that The Commission seeks comments on what, if any, changes to the guidelines should be made to respond to the Directive of the Foreign and Economic Espionage Penalty Enhancement Act of 2012. In particular, the Commission seeks comments on six (6) specific points, which I address in turn below.

I provide my comments based on my experiences and lessons learned acting as General Counsel to a company who has fallen victim to the devastating effects of trade secret theft and not as an expert in criminal law or setting penalties for violations of criminal law. These comments are my own and do not necessarily represent the opinions of American Superconductor Corporation.

(1) ***What offenses, if any, other than sections 1831 and 1832 should the Commission consider in responding to the directive? What guidelines, if any, other than §2B1.1 should the Commission consider amending in response to the directive?***

In addition to 18 U.S.C. Section 1905 and 7 U.S.C. Section 136, which the Commission has indicated are statutes that should also be reviewed, I provide the following thoughts. In the case of trade secret theft involving software, obtaining evidence to prove the misappropriation and use of software source code can be very challenging. However, obtaining evidence of use of object code (i.e. the machine readable code generated when the source code is compiled) which is installed on a hardware device can be much easier to detect. A copy of object code can be extracted from the hardware on which it is stored and can then be compared to the victim's object code. Making and deploying copies of object code without authorization is a copyright violation. I, therefore suggest that the U.S. Code sections relating to criminal copyright violations and corresponding guidelines for criminal sentencing also be reviewed and considered.

In addition, federal laws pertaining to cybercrime, such as the Computer Fraud and Abuse Act, and corresponding guidelines for criminal sentencing should be reviewed and considered. U.S. companies are increasingly under cyber-attack by individuals and organizations of foreign countries many of which are sponsored by foreign governments. This is a real and dangerous threat that companies must pay attention to and implement measures to guard against.

(2) ***What should the Commission consider in reviewing the seriousness of the offenses? described in the directive, the potential and actual harm caused by these offenses, and the need to provide adequate deterrence against such offenses?***

In considering the seriousness of a trade secret offense, the potential and actual harm caused by the offense, and the need to provide adequate deterrence against such offenses, I believe that the Commission should primarily consider (i) the potential and actual loss to the victim, (ii) whether the misappropriated trade secret was transmitted outside of the U.S, and (iii) whether the crimes were committed to benefit a foreign government.

The Commission should consider the potential and actual loss to the victim caused by the offenses to ensure that victims of these crimes are adequately compensated. Section 2 of the Foreign and Economic Espionage Penalty Enhancement Act of 2012 amended 18 USC 1831 to provide a maximum fine for a defendant who is an organization equal to the greater of $10 million or three (3) times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has avoided.

I am hopeful that the statute will be interpreted such that the value of the trade secret will not be limited to the costs of reproducing the trade secret. In calculating the fine in this way victims of trade secret theft will in many cases, including the case of AMSC, be left far short of being made whole. When the fine is calculated on the basis of the cost for the defendant to replicate the trade secret, the true value of the trade secret will not be captured. In the case of AMSC, we estimate the cost to reproduce the trade secret would be several tens of millions of dollars. In stark contrast, the actual loss suffered by AMSC due to the trade secret theft by Sinovel is in the

hundreds of millions of dollars. In addition, the share price of AMSC stock has plummeted over 90% resulting in over $1 billion in loss to AMSC's shareholders.

I believe that the impact of a trade secret theft on victims is likely to be greater if the trade secret is transmitted outside of the United States. Once the trade secret leaves the U.S., especially if it is transmitted to one or more developing countries which have less well developed judicial systems, it is not likely that trade secret use and propagation can be effectively stopped. This, of course, will result in greater damage to the victim. Moreover, it is not likely that the victim will receive adequate compensation, if any at all, for the damages suffered. Therefore, providing an increased penalty for theft of trade secrets which are transmitted out of the U.S. is highly recommended and should be strongly considered in assessing the seriousness of the offense.

Given the rise in state sponsored trade secret theft in recent years, the potential impact on U.S. companies and the U.S. economy is very significant. Therefore, whether the trade secret offense was committed to benefit a foreign government should be heavily weighed when considering the seriousness of the offenses defined 18 USC Sections 1831 and 1832.

When foreign governments have a level of involvement in trade secret theft, the impact on U.S. Companies can be far greater given the great resources of such foreign governments to assist in carrying out the crimes. In addition, the companies and individuals carrying out the crimes for their governments are likely to receive protection from their governments. Given these factors, defendants who are acting with a level of state involvement pose a more serious threat to the U.S. than individuals acting on their own and this should factored into the Commissions consideration in amending the Guidelines.

(3) ***Do the guidelines appropriately account for the simple misappropriation of a trade secret? Is the existing enhancement at §2B1.1(b)(5), which provides a 2-level enhancement "[i]f the offense involved misappropriation of a trade secret and the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent," sufficient to address the seriousness of the conduct involved in the offenses described in the directive?***

I believe that the guidelines appropriately account for simple misappropriation of a trade secret. According to the proposed amendment to Section 2B1.1(a), the base offense level for a trade secret misappropriation would be level 6. This level would be adjusted according to the loss pursuant to Section 2B1.1(b). In the case of losses between $1 million and $2.5 million, the offense level would be increased to level 24. The Sentencing Table in the 2012 Sentencing Guidelines Manual provides 51 to 63 months for level 24 for the lowest Criminal History Category. For losses more than $20 million the sentence would increase to 78 to 97 months.

These are fairly significant sentences for trade secret misappropriation where there is no transmission of the trade secret outside of the U.S. and/or it was not done for the benefit of a foreign government and I believe they are adequate.

However, I do not believe that a 2-level enhancement is sufficient for trade secret misappropriations which are done to benefit a foreign government. I believe that in most cases this level of enhancement will not provide a sufficient deterrent effect or a severe enough penalty considering the potential loss.

According to the Sentencing Table, and taking into account the proposed amendments, for a violation of 18 USC Section 1832, with a loss of up to $20 million and a Level I Criminal History Category, the 2-level enhancement would provide an additional 19 months to a 78 month sentence. This equates to a 20% increase in the length of the sentence. If the intent is to provide a strong deterrent for state sponsored trade secret theft, I do not believe the proposed differential penalty will provide the intended effect.

The maximum penalty for an 18 USC Section 1832 (Trade Secret Theft) violation is ten (10) years while the maximum penalty for an 18 USC Section 1831 (Economic Espionage) violation is fifteen (15) years. This is a 50% differential between the pure commercial trade secret theft and the state sponsored theft. If the trade secret theft is determined to be intended for the benefit of the state, then I think the enhancement should be structured to provide a differential sentence of at least 50%.

While this enhancement approach seems reasonable, I am concerned that in practice it will be difficult to obtain sufficient evidence to prove the defendant intended or knew that the offense was committed for the benefit of a foreign government as would be required for the enhancement to apply. I would recommend that the Commission consider specifying in the sentencing guidelines that if the defendant is employed by a foreign corporation which is a state-owned enterprise ("SOE"), that the requisite intent that the defendant intended or knew that the offense was committed for the benefit of a foreign government would be presumed. Further, I recommend that the Commission define a SOE as a foreign entity in which at least a defined percentage of the ownership of the entity (e.g. greater than or equal to 20%) is owned directly or indirectly by a foreign government, foreign instrumentality, or a foreign agent.

(4) Should the Commission provide one or more additional enhancements to account for (A) the transmission or attempted transmission of a stolen trade secret outside of the United States; and (B) the transmission or attempted transmission of a stolen trade secret outside of the United States that is committed or attempted to be committed for the benefit of a foreign government, foreign instrumentality, or foreign agent? If so, under what circumstances should such an enhancement apply, and what level of enhancement should apply?

I believe that the Commission should provide additional enhancements to account for transmission of stolen trade secrets outside of the U.S. and for trade secrets theft committed for the benefit of a foreign government.

As indicated above, I believe that the impact of a trade secret theft on the victim is likely to be greater if the trade secret is transmitted outside of the United States. Once the trade secret leaves the U.S., especially if it is transmitted to one or more developing countries which have less well developed judicial systems, it is not likely that trade secret use and propagation can be effectively stopped. This, of course, will result in greater damage to the victim. Therefore,

providing an increased penalty for theft of trade secrets which are transmitted out of the U.S. is highly recommended.

Also as described above, when foreign governments have some level of involvement in trade secret theft, the impact on U.S. Companies can be far greater given the great resources of such foreign governments to assist in carrying out the crimes. In addition, the companies and individuals carrying out the crimes on behalf of their governments are likely to receive protection from their governments. Given these factors, defendants who are acting with some level of state involvement pose a more serious threat to the U.S. than individuals acting on their own. Therefore, a further enhancement to the available penalties should be provided.

As described above in response to question 3, I believe that the further enhancement should be at least 50% greater than the penalty for simple trade secret theft. In addition, please consider my comments in response to question 3 regarding applying enhanced penalties when a SOE employs the defendant.

(5) Should the Commission restructure the existing 2-level enhancement in subsection (b)(5) into a tiered enhancement that directs the court to apply the greatest of the following: (A) an enhancement of 2 levels if the offense involved the simple misappropriation of a trade secret; (B) an enhancement of 4 levels if the defendant transmitted or attempted to transmit the stolen trade secret outside of the United States; and (C) an enhancement of [5][6] levels if the defendant committed economic espionage, i.e., the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent?

I believe that the Commission should provide additional enhancements to account for transmission of stolen trade secrets outside of the U.S. and for trade secrets theft committed for the benefit of a foreign government. Please refer to my answer to question 4 above.

(6) ***Should the Commission provide a minimum offense level of [14][16] if the defendant transmitted or attempted to transmit stolen trade secrets outside of the United States or***

***committed economic espionage*?**

Transmission of a trade secret outside of the United States and doing so for the benefit of a foreign government is potentially the most serious and harmful type of trade secret offense to victims. Therefore, providing an increased penalty is certainly warranted, as I have indicated above. Setting a much higher minimum offense level under these circumstances is a good way of ensuring that a significant penalty is imposed regardless of the magnitude of the loss. However, the high minimum offense level should be coupled with a tiered enhancement structure based on loss to the victim to ensure the penalty is increased according to the financial impact on the victim.

Conclusion

Thank you for providing me this opportunity to provide comments on such an important topic to U.S. companies and the U.S economy.

I am grateful for the Commission's efforts directed to this important aspect of the law governing trade secret theft. I hope that the Commission will consider my comments and increase the penalties for trade secret theft, in particular, that which results in transmission of trade secrets outside of the U.S. and/or is done for the benefit of a foreign government.