

March 4, 2013

The Honorable Patti B. Saris
Chair
United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, D.C. 20002-8002

Dear Judge Saris,

I commend the Sentencing Commission for its proposed amendment to §2B5.3(b)(5) of the Sentencing Guidelines, which applies to trafficking in counterfeit goods. An amendment to raise sentences for trafficking in counterfeit military goods and services is needed to reflect the seriousness of this criminal conduct. As previously stated in my letter of May 10, 2012, I would urge the Commission to add a four-level enhancement and raise the minimum offense level for offenses involving counterfeit military products to 14.

I write today on a different subject, however: the need to amend the Sentencing Guidelines to address the harm to our economy caused by the theft of trade secrets through cyber means.

According to unclassified reports from both the Intelligence Community and the private sector, foreign economic espionage against American companies through cyber means is on the rise. A recent report by Mandiant, for example, described one Chinese operation's approach as follows:

Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership.

Such practices are far too common. Using malware or various exploits to misappropriate the proprietary information that is the lifeblood of our economy, foreign agents, criminal organizations and individual hackers cost American companies tens of billions of dollars each year. This theft is difficult to detect; even when discovered, its full extent and the effect of the loss often remains unknown. One thing can be certain, though: the harm it causes will be felt for years to come.

The Foreign and Economic Espionage Penalty Enhancement Act of 2012, P.L. 112-269, responded to both cyber and traditional threats to trade secrets by increasing the maximum penalties for foreign individuals or organizations that steal trade secrets. It also instructed the

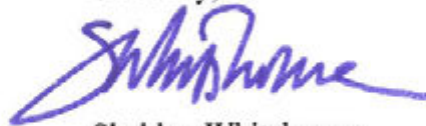
Sentencing Commission to consider raising the guideline range for the theft of trade secrets when the stolen trade secret is transmitted overseas.

Currently, a first time offender who engaged in no other aggravating conduct and who accepted responsibility would receive a Guideline range of zero to six months in prison for an overseas misappropriation of a trade secret. Such limited sentences are inappropriate considering the damage caused by the theft of trade secrets by cyber means.

The Commission should amend §2B1.1 of the Sentencing Guidelines to deter international trade secret theft and to reflect the severity of this crime. Specifically, it should consider four amendments. First, the Commission should establish a four-level enhancement and a minimum offense level of 14 if the defendant transmitted or attempted to transmit the stolen trade secret outside the United States. This would cause an offender to face at least a 10 to 16 month Guideline range. Second, the Commission should establish a six-level enhancement and a minimum offense level of 16 if the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent. This would cause an offender to face at least a 15 to 21 month Guideline range. Third, loss calculations in the Sentencing Guidelines should be amended to reflect the enormous harm caused by the theft of trade secrets. Competitive disadvantages caused by foreign trade secret theft – including the overnight appearance of foreign competitors – can result in lost jobs and other cascading economic injuries for Americans. The challenge of identifying the extent of an intrusion and how much data was exfiltrated means that resulting harms likely will be underestimated. At a minimum, the Sentencing Guidelines should calculate loss to include any reasonable cost to any victim, not just the costs the offender would have had to incur to generate the trade secret through legitimate means. Only by ensuring that an offender is held responsible for the full effects of their crime will an appropriate deterrent effect be achieved. Fourth, the Sentencing Commission should establish a two-level enhancement for a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, that involves trade secret theft or attempted trade secret theft. Existing Guidelines provisions establish two-level enhancements for violations of 18 U.S.C. § 1030 that involve threats to privacy or to critical infrastructure computers. Hacking to gain trade secrets similarly should be subject to such enhanced penalties.

Foreign trade secret theft by cyber means is causing massive damage to our economy. I urge the Sentencing Commission to provide for appropriate sanctions for such dangerous conduct.

Sincerely,



Sheldon Whitehouse
United States Senator

United States Senate
WASHINGTON, DC 20510-3905

March 4, 2013

The Honorable Ketanji Brown Jackson
Vice Chair
United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, D.C. 20002-8002

Dear Ms. Jackson,

I commend the Sentencing Commission for its proposed amendment to §2B5.3(b)(5) of the Sentencing Guidelines, which applies to trafficking in counterfeit goods. An amendment to raise sentences for trafficking in counterfeit military goods and services is needed to reflect the seriousness of this criminal conduct. As previously stated in my letter of May 10, 2012, I would urge the Commission to add a four-level enhancement and raise the minimum offense level for offenses involving counterfeit military products to 14.

I write today on a different subject, however: the need to amend the Sentencing Guidelines to address the harm to our economy caused by the theft of trade secrets through cyber means.

According to unclassified reports from both the Intelligence Community and the private sector, foreign economic espionage against American companies through cyber means is on the rise. A recent report by Mandiant, for example, described one Chinese operation's approach as follows:

Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership.

Such practices are far too common. Using malware or various exploits to misappropriate the proprietary information that is the lifeblood of our economy, foreign agents, criminal organizations and individual hackers cost American companies tens of billions of dollars each year. This theft is difficult to detect; even when discovered, its full extent and the effect of the loss often remains unknown. One thing can be certain, though: the harm it causes will be felt for years to come.

The Foreign and Economic Espionage Penalty Enhancement Act of 2012, P.L. 112-269, responded to both cyber and traditional threats to trade secrets by increasing the maximum penalties for foreign individuals or organizations that steal trade secrets. It also instructed the

Sentencing Commission to consider raising the guideline range for the theft of trade secrets when the stolen trade secret is transmitted overseas.

Currently, a first time offender who engaged in no other aggravating conduct and who accepted responsibility would receive a Guideline range of zero to six months in prison for an overseas misappropriation of a trade secret. Such limited sentences are inappropriate considering the damage caused by the theft of trade secrets by cyber means.

The Commission should amend §2B1.1 of the Sentencing Guidelines to deter international trade secret theft and to reflect the severity of this crime. Specifically, it should consider four amendments. First, the Commission should establish a four-level enhancement and a minimum offense level of 14 if the defendant transmitted or attempted to transmit the stolen trade secret outside the United States. This would cause an offender to face at least a 10 to 16 month Guideline range. Second, the Commission should establish a six-level enhancement and a minimum offense level of 16 if the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent. This would cause an offender to face at least a 15 to 21 month Guideline range. Third, loss calculations in the Sentencing Guidelines should be amended to reflect the enormous harm caused by the theft of trade secrets. Competitive disadvantages caused by foreign trade secret theft – including the overnight appearance of foreign competitors – can result in lost jobs and other cascading economic injuries for Americans. The challenge of identifying the extent of an intrusion and how much data was exfiltrated means that resulting harms likely will be underestimated. At a minimum, the Sentencing Guidelines should calculate loss to include any reasonable cost to any victim, not just the costs the offender would have had to incur to generate the trade secret through legitimate means. Only by ensuring that an offender is held responsible for the full effects of their crime will an appropriate deterrent effect be achieved. Fourth, the Sentencing Commission should establish a two-level enhancement for a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, that involves trade secret theft or attempted trade secret theft. Existing Guidelines provisions establish two-level enhancements for violations of 18 U.S.C. § 1030 that involve threats to privacy or to critical infrastructure computers. Hacking to gain trade secrets similarly should be subject to such enhanced penalties.

Foreign trade secret theft by cyber means is causing massive damage to our economy. I urge the Sentencing Commission to provide for appropriate sanctions for such dangerous conduct.

Sincerely,



Sheldon Whitehouse
United States Senator

United States Senate
WASHINGTON, DC 20510-3905

March 4, 2013

The Honorable Ricardo H. Hinojosa
Commissioner
United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, D.C. 20002-8002

Dear Chief Judge Hinojosa,

I commend the Sentencing Commission for its proposed amendment to §2B5.3(b)(5) of the Sentencing Guidelines, which applies to trafficking in counterfeit goods. An amendment to raise sentences for trafficking in counterfeit military goods and services is needed to reflect the seriousness of this criminal conduct. As previously stated in my letter of May 10, 2012, I would urge the Commission to add a four-level enhancement and raise the minimum offense level for offenses involving counterfeit military products to 14.

I write today on a different subject, however: the need to amend the Sentencing Guidelines to address the harm to our economy caused by the theft of trade secrets through cyber means.

According to unclassified reports from both the Intelligence Community and the private sector, foreign economic espionage against American companies through cyber means is on the rise. A recent report by Mandiant, for example, described one Chinese operation's approach as follows:

Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership.

Such practices are far too common. Using malware or various exploits to misappropriate the proprietary information that is the lifeblood of our economy, foreign agents, criminal organizations and individual hackers cost American companies tens of billions of dollars each year. This theft is difficult to detect; even when discovered, its full extent and the effect of the loss often remains unknown. One thing can be certain, though: the harm it causes will be felt for years to come.

The Foreign and Economic Espionage Penalty Enhancement Act of 2012, P.L. 112-269, responded to both cyber and traditional threats to trade secrets by increasing the maximum penalties for foreign individuals or organizations that steal trade secrets. It also instructed the

Sentencing Commission to consider raising the guideline range for the theft of trade secrets when the stolen trade secret is transmitted overseas.

Currently, a first time offender who engaged in no other aggravating conduct and who accepted responsibility would receive a Guideline range of zero to six months in prison for an overseas misappropriation of a trade secret. Such limited sentences are inappropriate considering the damage caused by the theft of trade secrets by cyber means.

The Commission should amend §2B1.1 of the Sentencing Guidelines to deter international trade secret theft and to reflect the severity of this crime. Specifically, it should consider four amendments. First, the Commission should establish a four-level enhancement and a minimum offense level of 14 if the defendant transmitted or attempted to transmit the stolen trade secret outside the United States. This would cause an offender to face at least a 10 to 16 month Guideline range. Second, the Commission should establish a six-level enhancement and a minimum offense level of 16 if the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent. This would cause an offender to face at least a 15 to 21 month Guideline range. Third, loss calculations in the Sentencing Guidelines should be amended to reflect the enormous harm caused by the theft of trade secrets. Competitive disadvantages caused by foreign trade secret theft – including the overnight appearance of foreign competitors – can result in lost jobs and other cascading economic injuries for Americans. The challenge of identifying the extent of an intrusion and how much data was exfiltrated means that resulting harms likely will be underestimated. At a minimum, the Sentencing Guidelines should calculate loss to include any reasonable cost to any victim, not just the costs the offender would have had to incur to generate the trade secret through legitimate means. Only by ensuring that an offender is held responsible for the full effects of their crime will an appropriate deterrent effect be achieved. Fourth, the Sentencing Commission should establish a two-level enhancement for a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, that involves trade secret theft or attempted trade secret theft. Existing Guidelines provisions establish two-level enhancements for violations of 18 U.S.C. § 1030 that involve threats to privacy or to critical infrastructure computers. Hacking to gain trade secrets similarly should be subject to such enhanced penalties.

Foreign trade secret theft by cyber means is causing massive damage to our economy. I urge the Sentencing Commission to provide for appropriate sanctions for such dangerous conduct.

Sincerely,



Sheldon Whitehouse
United States Senator

United States Senate

WASHINGTON, DC 20510-3905

March 4, 2013

The Honorable Dabney Friedrich
Commissioner
United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, D.C. 20002-8002

Dear Ms. Friedrich,

I commend the Sentencing Commission for its proposed amendment to §2B5.3(b)(5) of the Sentencing Guidelines, which applies to trafficking in counterfeit goods. An amendment to raise sentences for trafficking in counterfeit military goods and services is needed to reflect the seriousness of this criminal conduct. As previously stated in my letter of May 10, 2012, I would urge the Commission to add a four-level enhancement and raise the minimum offense level for offenses involving counterfeit military products to 14.

I write today on a different subject, however: the need to amend the Sentencing Guidelines to address the harm to our economy caused by the theft of trade secrets through cyber means.

According to unclassified reports from both the Intelligence Community and the private sector, foreign economic espionage against American companies through cyber means is on the rise. A recent report by Mandiant, for example, described one Chinese operation's approach as follows:

Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership.

Such practices are far too common. Using malware or various exploits to misappropriate the proprietary information that is the lifeblood of our economy, foreign agents, criminal organizations and individual hackers cost American companies tens of billions of dollars each year. This theft is difficult to detect; even when discovered, its full extent and the effect of the loss often remains unknown. One thing can be certain, though: the harm it causes will be felt for years to come.

The Foreign and Economic Espionage Penalty Enhancement Act of 2012, P.L. 112-269, responded to both cyber and traditional threats to trade secrets by increasing the maximum penalties for foreign individuals or organizations that steal trade secrets. It also instructed the

Sentencing Commission to consider raising the guideline range for the theft of trade secrets when the stolen trade secret is transmitted overseas.

Currently, a first time offender who engaged in no other aggravating conduct and who accepted responsibility would receive a Guideline range of zero to six months in prison for an overseas misappropriation of a trade secret. Such limited sentences are inappropriate considering the damage caused by the theft of trade secrets by cyber means.

The Commission should amend §2B1.1 of the Sentencing Guidelines to deter international trade secret theft and to reflect the severity of this crime. Specifically, it should consider four amendments. First, the Commission should establish a four-level enhancement and a minimum offense level of 14 if the defendant transmitted or attempted to transmit the stolen trade secret outside the United States. This would cause an offender to face at least a 10 to 16 month Guideline range. Second, the Commission should establish a six-level enhancement and a minimum offense level of 16 if the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent. This would cause an offender to face at least a 15 to 21 month Guideline range. Third, loss calculations in the Sentencing Guidelines should be amended to reflect the enormous harm caused by the theft of trade secrets. Competitive disadvantages caused by foreign trade secret theft – including the overnight appearance of foreign competitors – can result in lost jobs and other cascading economic injuries for Americans. The challenge of identifying the extent of an intrusion and how much data was exfiltrated means that resulting harms likely will be underestimated. At a minimum, the Sentencing Guidelines should calculate loss to include any reasonable cost to any victim, not just the costs the offender would have had to incur to generate the trade secret through legitimate means. Only by ensuring that an offender is held responsible for the full effects of their crime will an appropriate deterrent effect be achieved. Fourth, the Sentencing Commission should establish a two-level enhancement for a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, that involves trade secret theft or attempted trade secret theft. Existing Guidelines provisions establish two-level enhancements for violations of 18 U.S.C. § 1030 that involve threats to privacy or to critical infrastructure computers. Hacking to gain trade secrets similarly should be subject to such enhanced penalties.

Foreign trade secret theft by cyber means is causing massive damage to our economy. I urge the Sentencing Commission to provide for appropriate sanctions for such dangerous conduct.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Sheldon Whitehouse', written in a cursive style.

Sheldon Whitehouse
United States Senator