112TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
112–610

FOREIGN AND ECONOMIC ESPIONAGE PENALTY ENHANCEMENT ACT OF 2012

JULY 19, 2012.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SMITH of Texas, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany H.R. 6029]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 6029) to amend title 18, United States Code, to provide for increased penalties for foreign and economic espionage, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

Purpose and Summary

H.R. 6029, the Foreign and Economic Espionage Penalty Enhancement Act of 2012, amends the Federal criminal code to combat the significant and growing threat presented by criminals who engage in espionage on behalf of foreign adversaries and competitors. The bill amends § 1831(a) of title 18, United States Code, to

increase the maximum penalties for the theft of trade secrets by criminals who knowingly commit economic espionage to benefit a foreign entity. By strengthening penalties and enhancing criminal deterrence, the bill protects U.S. jobs and technologies while promoting investments and innovation. When enacted, H.R. 6029 will advance the economic and national security interests of the United States.

Background and Need for the Legislation

Foreign Economic Espionage a Persistent Threat to U.S. Businesses:

In October 2011, the National Counterintelligence Executive (ONCIX) published its biennial report to Congress on Foreign Economic Collection and Industrial Espionage. The report concluded, "Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security,"[1] and provided further:

> Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.[2]

Of particular concern, the report identified two "Intelligence Adversaries,"[3] noting that, "China and Russia view themselves as strategic competitors of the United States and are the most aggressive collectors of US economic information and technology."[4] The report warned:

> We judge that the governments of China and Russia will remain aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace.[5]

And the Intelligence Community predicted:

> Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security.[6]

In January 2012, the Director of National Intelligence (DNI), James R. Clapper, echoed the ONCIX report's warnings when he delivered the Worldwide Threat Assessment of the US Intelligence Community. Addressing counterintelligence threats, General Clapper testified:

> We assess that foreign intelligence services (FIS) are constantly developing methods and technologies that challenge the ability of the US Government and private sector

---

[1] *Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011,* Office of the National Counterintelligence Executive, p. i, (October 2011).
[2] *Id.*
[3] *Id.* at p. 4
[4] *Id.*
[5] *Id.* at p. ii.
[6] *Id.* at p. i.

> to protect US national security and economic information, information systems, and infrastructure.[7]

And stated, "the most menacing foreign intelligence threats in the next two to 3 years will involve" the need to confront and counter three activities:

1) cyber-enabled espionage;

2) insider threats; and

3) espionage by China, Russia and Iran.[8]

Elaborating on the last point, the DNI stated:

> Russia and China are aggressive and successful purveyors of economic espionage against the United States. . . . We assess that FIS from these three countries [including Iran] will remain the top threats to the United States in the coming years.[9]

In explaining the threat posed by cyber intrusions, the DNI referred to the ONCIX report, when he testified:

> Among state actors, China and Russia are of particular concern . . . entities within these countries are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property.[10]

Existing U.S. Legal Protections and Authority:

In the United States, trade secret[11] law protects secret, valuable business information from misappropriation by others.[12]

To promote legitimate competition and protect the investments and trade secrets of U.S. companies, Congress enacted the Economic Espionage Act of 1996 (EEA)[13] to provide criminal penalties for the theft of commercial trade secrets.

The EEA addresses two types of trade secret misappropriation. Section 1831 provides penalties for the theft of a trade secret to benefit a foreign government, instrumentality or agent while section 1832 provides penalties for the commercial theft of a trade secret carried out for economic advantage, whether or not the theft is intended to benefit a foreign entity.

Reflecting the more serious nature of economic espionage committed in furtherance of a foreign interest, the maximum sentence for an individual convicted is 15 years' imprisonment or a fine of $500,000, or both. In contrast, the maximum sentence for an individual convicted of the theft of a trade secret under § 1832 is 10

---

[7] *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence,* James R. Clapper, Director of National Intelligence, p. 8, January 31, 2012.

[8] *Id.*

[9] *Id.*

[10] *Id.* at p. 7

[11] "A trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret by executing confidentiality agreements with employees and others and by hiding the information from outsiders by means of fences, safes, encryption, and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or tort." *Confold Pac v.Polaris Indus.,* 433 F.3d 952, 959 (7th Cir. 2006). The statutory definition of a trade secret is codified at 18 USC § 1839(3).

[12] *Intellectual Property: The Law of Copyrights, Patents and Trademarks,* Roger E. Schechter and John R. Thomas, p. 528, (2003).

[13] The EEA is codified at 18 USC§§ 1831–1839.

years' imprisonment or a fine of $250,000, or both. An organization convicted of a violation of § 1831 may be fined up to $10 million while an organization convicted of a violation of § 1832 is eligible for a fine of up to $5 million.

Since Congress enacted the EEA nearly two decades ago, it has not updated the penalty structure to reflect the increasing importance and value of intellectual property to our collective economy or its unique role as a catalyst to the continued growth and success of individual enterprises.

Foreign Economic Espionage Imposes Enormous Costs on U.S. Businesses, Compromises Critical Technologies and Undermines U.S. Security and Competitiveness:

Today, U.S businesses are built on the foundation of intangible assets. These include trade secrets, proprietary data, marketing plans, business processes and source code. An estimated 81% of the market value of S&P 500 companies in 2009 was derived from the value of their intangible portfolios.[14]

On average, US organizations spend an estimated $1 million a day on information technology.[15] Despite this investment, U.S. businesses are increasingly targeted for and vulnerable to the theft of their intellectual capital. In many cases, businesses aren't aware of advanced persistent threats that target their valuable trade secrets. Even when detected, businesses may not discover thefts until well after they've incurred serious damage.

In May 2012, the Federal Bureau of Investigation (FBI) reported U.S. companies lost more than $13 billion to trade secret theft in cases opened in a brief period—just over 6 months during the current fiscal year.[16]

Writing in the Washington Post in November 2011, Ellen Nakashima summarized U.S. official's estimates of losses to specific U.S. companies:

> The head of the military's U.S. Cyber Command, Gen. Keith Alexander, said one U.S. company recently lost $1 billion worth of intellectual property over the course of a few days. [17]

Continuing, the report stated:

> A senior intelligence official, briefing reporters on the condition of anonymity, noted a few cases in which estimates were given in economic espionage prosecutions over the past 6 years: $100 million worth of insecticide research from Dow Chemical, $400 million worth of chemical formulas from DuPont, $600 million worth of proprietary

---

[14] *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency,* p. 6, March 28, 2011, available at http://www.mcafee.com/us/resources/reports/rp-underground-economies.pdf

[15] *Id.* at p. 1

[16] *FBI's New Campaign Targets Corporate Espionage,* article by Evan Perez, May 11, 2012, The Wall Street Journal, available at http://online.wsj.com/article/SB10001424052702304543904577396520137905092.html.

[17] *In A World of Cybertheft, U.S. Names China, Russia As Main Culprits,* article by Ellen Nakashima, November 3, 2011, The Washington Post, available at http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html

data from Motorola, $20 million worth of paint formulas from Valspar.[18]

Private sector experts validate that extensive damages and losses are being sustained by U.S. and global enterprises. A 2009 report from McAfee, the world's largest dedicated security technology company, found "companies worldwide lost more than an estimated $1 trillion in 2008 due to data leaks, the cost of remediation and reputational damage." [19]

A 2011 report from McAfee and Science Applications International Corporation (SAIC), a leading scientific, engineering and technology applications company, concluded, "[t]he cyber underground economy has shifted its focus to the theft of corporate intellectual capital—the new currency of cybercrime" [20], and "[t]he target and motivation are almost always financial." [21]

The value of losses is difficult to establish with absolute certainty but the Intelligence Community has offered a proxy for "the cost of developing new ideas, and . . . an indicator or the value of the information that is most vulnerable to economic espionage"—corporate and government spending on research and development (R&D).[22] In 2008, the most recent year available, the National Science Foundation "calculated that US industry, the Federal Government, universities, and other nonprofit organizations expended $398 billion on R&D, or 2.8% of the US Gross Domestic Product." [23]

The McAfee/SAIC analysis framed the cost/benefit analysis for potential criminals in a succinct manner: "What is a few million dollars [expended to steal intellectual capital] if a competitor company can save billions in research and development by stealing . . . proprietary data?" [24]

Responding to accelerating losses to American businesses and increasing threats to U.S. national and economic security, U.S. law enforcement are stepping up the investigation and prosecution of trade secret theft and economic espionage cases. In 2010, the FBI and the Department of Justice opened 66 such investigations.[25] Of seven insider EEA cases prosecuted in 2010, six involved links to a single country—China.[26] In April 2012, Dan Freedman of the Houston Chronicle reported that since 2010, "prosecutors brought at least 30 China-related cases involving economic espionage or violations of the law barring unlicensed export of militarily sensitive technology." [27]

The U.S. Intellectual Property Enforcement Coordinator recently recommended that Congress increase both the statutory maximum penalty for economic espionage cases and the U.S. Sentencing Guideline range for the theft of trade secrets and economic espionage, including trade secrets transferred or attempted to be trans-

---

[18] *Id.*
[19] *Ibid.* 14, at 5
[20] *Id.* at 3
[21] *Id.* at 5
[22] *Ibid.* 1, at 4
[23] *Id.*
[24] *Ibid.* 14, at p. 6
[25] *Department of Justice Joins in Launch of Administration's Strategic Plan on Intellectual Property Enforcement as Part of Ongoing IP Initiative,* DEPT. OF JUSTICE (June 22, 2010), available at http://www.justice.gov/opa/pr/2010/June/10-ag-722.html.
[26] *Ibid.* 17
[27] *Costs of Economic Espionage Mount,* article by Dan Freedman, April 27, 2012, Houston Chronicle, available at http://www.chron.com/news/houston-texas/article/Costs-of-economic-espionage-mount-3517271.php

ferred outside the U.S., in recognition of the "severity of the conduct inherent in the offense."[28]

Representative Lamar Smith, the Chairman of the Judiciary Committee, and 11 bipartisan members of the House introduced H.R. 6029, the "Foreign and Economic Espionage Penalty Enhancement Act of 2012," on June 27, 2012. A targeted measure, H.R. 6029 increases the maximum penalties for those convicted of foreign economic espionage. The bill responds to the significant and persistent threat of foreign economic espionage by deterring criminal activity and increasing the "costs of doing business" for those who engage in criminal activity that harms the economic and national security interests of the United States.

Hearings

The Committee on the Judiciary held no hearings on H.R. 6029.

Committee Consideration

On July 10, 2012, the Committee met in open session and ordered the bill, H.R. 6029, favorably reported without amendment, by voice vote, a quorum being present.

Committee Votes

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that there were no recorded votes during the Committee's consideration of H.R. 6029.

Committee Oversight Findings

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

New Budget Authority and Tax Expenditures

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

Congressional Budget Office Cost Estimate

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 6029, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

---

[28] *Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations,* p. 4, (March 2011). Available at http://www.whitehouse.gov/sites/default/files/ip__white__paper.pdf

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 17, 2012.

Hon. LAMAR SMITH, CHAIRMAN,
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 6029, the "Foreign and Economic Espionage Penalty Enhancement Act of 2012."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz, who can be reached at 226–2860.

Sincerely,

DOUGLAS W. ELMENDORF,
DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 6029—Foreign and Economic Espionage Penalty Enhancement Act of 2012.

As ordered reported by the House Committee on the Judiciary on July 10, 2012.

H.R. 6029 would increase the maximum penalties, including fines, for revealing trade secrets to foreign entities and would direct the United States Sentencing Commission (USSC) to review and, if necessary, amend sentencing guidelines for economic espionage. Based on information provided by the USSC, CBO estimates that implementing H.R. 6029 would have no significant impact on the Federal budget. Enacting H.R. 6029 could affect direct spending and revenues; therefore, pay-as-you-go procedures apply. However, CBO estimates that the net effects would be insignificant for each year.

Because those prosecuted and convicted under H.R. 6029 could be subject to criminal fines, the Federal Government might collect additional fines if the legislation is enacted. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent. CBO expects that any additional revenues and direct spending would not be significant because of the small number of cases likely affected.

H.R. 6029 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of State, local, or tribal governments.

On January 24, 2012, CBO transmitted a cost estimate for S. 678, the "Economic Espionage Penalty Enhancement Act," as reported by the Senate Committee on the Judiciary on December 8, 2011. The two bills are similar, and the CBO cost estimates are the same.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 6029, the Foreign and Economic Espionage Penalty Enhancement Act of 2012, will improve the U.S. Government's ability to deter acts of foreign espionage and provide a more appropriate range of penalties for those convicted of the theft of trade secrets from U.S. companies.

Advisory on Earmarks

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 6029 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

Section-by-Section Analysis

The following discussion describes the bill as reported by the Committee.

Sec. 1. Short title. Section 1 sets forth the short title of the bill as the "Foreign and Economic Espionage Penalty Enhancement Act of 2012."

Sec. 2. Protecting U.S. Businesses from Foreign Espionage. Section 2 increases the maximum penalty for an individual convicted of foreign espionage to 20 years, a fine of up to $5 million, or both and provides the maximum penalty for an organization convicted of foreign espionage shall be up to $10 million or three times the value of the stolen trade secret.

Sec. 3. Review by the U.S. Sentencing Commission. Provides that the U.S. Sentencing Commission shall review the Federal sentencing guidelines and policy statements that apply to persons convicted of trade secret offenses to ensure they appropriately reflect the seriousness of the offenses, account for their actual and potential harm and provide adequate deterrence.

Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

CHAPTER 90—PROTECTION OF TRADE SECRETS

* * * * * * *

§ 1831. Economic espionage

(a) IN GENERAL.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) * * *

* * * * * * *

shall, except as provided in subsection (b), be fined [not more than $500,000] *not more than $5,000,000* or imprisoned not more than [15 years] *20 years*, or both.

(b) ORGANIZATIONS.—Any organization that commits any offense described in subsection (a) shall be fined [not more than $10,000,000] *not more than the greater of $10,000,000 or 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 thereby avoided*.

* * * * * * *

○