IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

Copyright Rightsholder Identified in Exhibit 1,	)	
Plaintiff,	)	Case No. 1:23-cv-04507
v.	)	Dist. Judge Matthew F. Kennelly
The Partnerships and Unincorporated Associations Identified on Schedule "A",	)	Mag. Judge Gabriel A. Fuentes
Defendants	)	

Declaration of Adam E. Urbanczyk

I, Adam E. Urbanczyk, of the City of Sarasota, in the State of Florida, declare as follows:

1. I am an attorney at law, duly admitted to practice before the Courts of the State of Illinois and the United States District Court for the Northern District of Illinois. I am the attorney for Plaintiff. Except as otherwise expressly stated to the contrary, I have personal knowledge of the following facts and, if called as a witness, I could and would competently testify to the following:

2. According to a 2023 report by U.S. Customs and Border Protection entitled "FY 2022 Fact Sheet", there were 20,812 seizures of shipments containing counterfeit goods suggested retail price (MSRP) of the seized goods, had they been genuine, of more than $2.98B, 82% of these originating from China or Hong Kong. A true and correct copy of this report is attached hereto as **Exhibit 1**.

3. According to a 2018 report by U.S. Customers and Border Protection entitled "Intellectual Property Rights Fiscal Year 2017 Seizure Statistics," intellectual property rights (IPR) seizures increased 8% over 2016 to a record 34,143 reflecting a total manufacturer's suggested retail price (MSRP) of the seized goods, had they been genuine, of more than $1.2B. A true and correct copy of this report is attached hereto as **Exhibit 2**.

4. According to a 2017 report entitled "The Report of the Commission on the Theft of American

Intellectual Property (also known as the IP Commission Report)," eCommerce trademark infringement, particularly involving counterfeit goods, and piracy / copyright infringement cost merchants in the U.S. alone nearly $41 billion. A true and correct copy of this report is attached hereto as **Exhibit 3**

5. According to a 2015 report by U.S. Customers and Border Protection entitled "Intellectual Property Rights Fiscal Year 2015 Seizure Statistics," there were 28,865 seizures which, according to the IP Commission Report, represented less than 3% of the total infringing goods being sold. A true and correct copy of this report is attached hereto as **Exhibit 4**.

6. According to a 2015 report by the World Economic Forum entitled "State of the Illicit Economy," the "cost to the global economy of counterfeiting alone could reach USD 1.77 Trillion." A true and correct copy of this report is attached hereto as **Exhibit 5**.

7. In my experience with online counterfeiting and piracy over the last six years, I have observed counterfeiters using a variety of tactics to evade enforcement efforts. Specifically, infringers like Defendants in the present case may often register new online marketplace accounts under new aliases once they receive notice of a lawsuit, or otherwise utilize a plethora of accounts to minimize the risk that the removal or deactivation of one storefront due to their counterfeiting activities will stall their entire operation.

8. In my experience, once notice of a lawsuit is received, counterfeiters like those Defendants in the present case may move funds, if at all possible, from their U.S.-based accounts (*e.g.*, PayPal) to off-shore bank accounts outside the jurisdiction of this Court.

9. For these reasons, in the absence of an *ex parte* Order, Defendants in this case, in the interest of shielding their assets could and likely would modify payment account registration data and content and to shuffle any assets from accounts in U.S.-based financial institutions (e.g., Amazon or PayPal), to offshore accounts.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on this July 14, 2023 at Sarasota, Florida.

/s/Adam E. Urbanczyk
Adam E. Urbanczyk
AU LLC
444 W. Lake St., 17th Floor
Chicago, IL 60606
(312) 715-7312
adamu@au-llc.com
Counsel for Plaintiff

Exhibit 1

U.S. Customs and Border Protection

FY 2022 FACT SHEET
Intellectual Property Rights

CBP Publication No. 3101-0323

U.S. Customs and Border Protection (CBP) enforces Intellectual Property Rights (IPR) most visibly by seizing products that infringe IPR, such as trademarks, copyrights, and patents. The theft of intellectual property and trade in fake goods threaten United States' economic vitality and national security, as well as the health and safety of the American people. Trade in these illicit goods often help to fund criminal activities and organized crime.

To protect both industry and consumers, CBP has made IPR enforcement a priority trade issue. As a result, CBP has developed a multi-layered, strategic approach to IPR enforcement that includes efforts to educate and engage stakeholders to deter the importation of illicit goods and employs innovative approaches to enforce IPR law at all ports of entry.

IPR Resources:

For assistance regarding IPR enforcement, contact IPR help desk at: IPRHELPDESK@cbp.dhs.gov .

To request information on CBP's recordation program, please contact the IPR Branch at: IPRRQUESTIONS@cbp.dhs.gov .

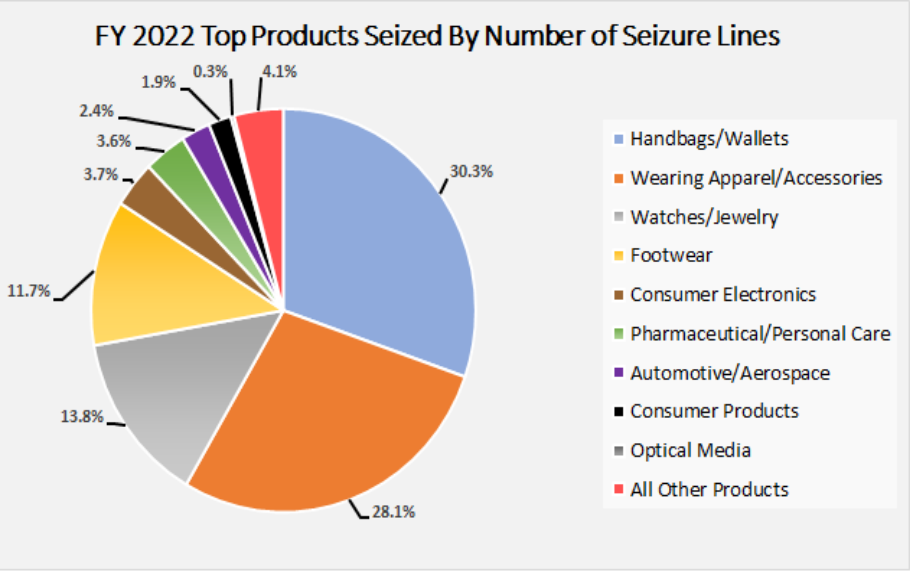
To request information on CBP's e-Allegations program, please contact eallegations@cbp.dhs.gov .

In Fiscal Year 2022, CBP seized 20,812 shipments containing counterfeit goods, corresponding to 102,297 seizure lines, which equates to nearly 25 million counterfeit goods. The total estimated manufacturer's suggested retail price (MSRP) of the seized goods, had they been genuine, was over $2.98 billion (USD). By value, approximately 82% of these goods originated in or were transshipped through China or Hong Kong.

In addition to seizing goods at U.S. borders, the strategy includes expanding the border through post-import audits of companies that have been caught bringing fake goods into the United States, collaborating with foreign governments and multi-lateral organizations, and working closely with industry and partner government agencies. CBP also issues civil fines and, where appropriate, refers cases to other law enforcement agencies for criminal investigation.

CBP collaborates closely with Immigration and Customs Enforcement-Homeland Security Investigations (ICE- HSI) and 25 additional partners at the IPR Center to ensure that IPR border seizures representing criminal activities lead to investigations, arrests, and convictions.

Working with rights holders to use CBP's web-based tool to record their trademarks and copyrights with CBP is a priority. This program, known as the e-Recordation program, makes information on protected rights available to CBP offices throughout the United States. CBP's e-Allegations program provides an electronic portal through which the public can report possible IPR violations and other suspected trade violations.



To help educate the public on the dangers of counterfeit goods, CBP hosts "The Truth Behind Counterfeits" public awareness campaign. For more information about this effort visit: https://www.cbp.gov/trade/fakegoodsrealdangers.

Exhibit 2

Intellectual Property Rights Seizure Statistics

Fiscal Year 2017

Disclaimer: The information contained in this report does not constitute the official trade statistics of the United States. The statistics, and the projections based upon those statistics, are not intended to be used for economic analysis, and are provided for the purpose of establishing U.S. Department of Homeland Security workload.

Homeland Security

Executive Summary

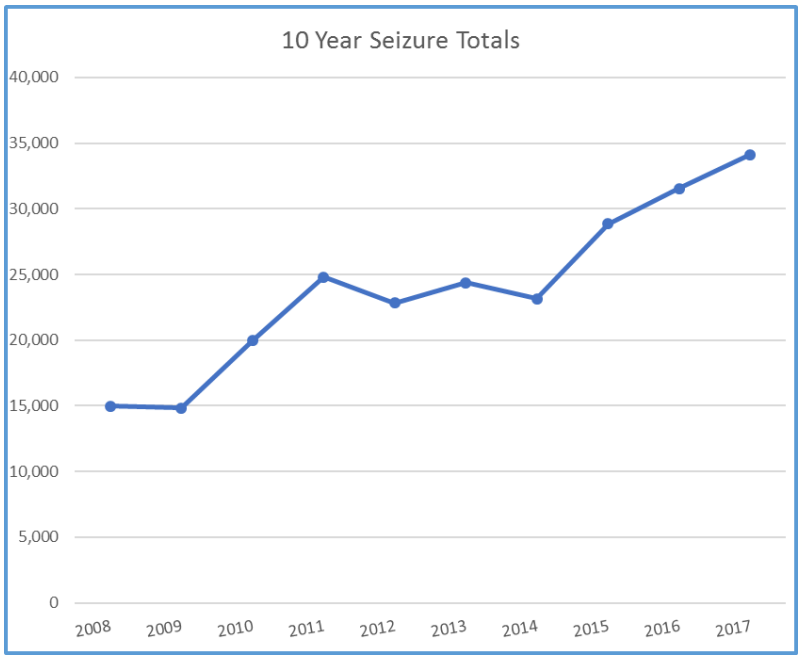
Products that infringe U.S. trademarks and copyrights or are subject to exclusion orders issued by the United States International Trade Commission threaten the health and safety of American consumers and pose risks to our national interests. U.S. Customs and Border Protection's (CBP) and U.S. Immigration and Customs Enforcement (ICE) - Homeland Security Investigations' (HSI) enforcement of intellectual property rights (IPR) mitigates the financial and welfare risks posed by imports of such illicit products.

In Fiscal Year (FY) 2017, the number of IPR seizures increased 8% to 34,143 from 31,560 in FY 2016. The total estimated manufacturer's suggested retail price (MSRP) of the seized goods, had they been genuine, decreased to $1,206,382,219 from $1,382,903,001 in FY 2016.

In FY 2017, ICE-HSI arrested 457 individuals, obtained 288 indictments, and received 242 convictions related to intellectual property crimes.

Each year, more than 11 million maritime containers arrive at our seaports. At our land borders, another 10 million arrive by truck and 3 million arrive by rail. An additional quarter billion more cargo, postal, and express consignment packages arrive through air travel. The components within the Department of Homeland Security (DHS) remain vigilant in targeting shipments containing IPR-infringing goods, levying civil fines and criminally investigating those who seek to violate our trade laws, harm our people and damage our economy.

Year in Review



- **In partnership with the Express Association of America and its members, CBP continued the voluntary abandonment pilot program. This program—supported through a formal recommendation by the Commercial Customs Operations Advisory Committee (COAC), CBP's federal advisory committee—resulted in 5,588 voluntary abandonments of detained goods and significant interdiction cost savings to the government.**
- **In FY 2017, CBP completed 115 exclusion order enforcement actions (shipments seized and shipments excluded).**
- **CBP seized 297 shipments of circumvention devices for violations of the Digital Millennium Copyright Act (DMCA), a 324% increase from 70 such seizures in FY 2016.**
- **The combined total number of all IPR border enforcement actions in FY 2017 increased 12% over FY 2016.**

Homeland Security

Year in Review

- Components of CBP's Integrated Trade Targeting Network (ITTN) conducted 12 national level IPR-mitigating trade operations in FY 2017. These operations targeted high-risk shipments at seaports, airports, international mail facilities and express carrier hubs across the U.S., and resulted in 1,845 seizures of IPR-infringing goods which, if genuine, would have an estimated MSRP of $44 million.

- Eight of these operations were conducted by Mobile Intellectual Property Enforcement Teams (MIPETs), groups of IPR experts deployed to assist enforcement operations. MIPET operations resulted in 1,687 seizures of IPR-infringing goods valued at $34.6 million MSRP and 67 abandonments.

- CBP and the General Administration of China Customs (GACC) conducted a month-long joint operation in April 2017 that focused on household consumer electronics, including lamps, lights, light fixtures, light bulbs, lighted signs, projectors, kitchen appliances, and personal grooming products. During the operation, both CBP and GACC focused on stopping shipments of IPR-infringing goods from entering U.S. commerce, with CBP making seizures at the U.S. border and GACC interdicting exports of counterfeit goods destined to the United States. The joint operation resulted in over 1,300 seizures.

- The ICE-led National IPR Coordination Center, along with representatives from CBP, conducted Operation Team Player prior to Super Bowl LI to jointly address the illegal importation of counterfeit sports-related merchandise. As a result of these efforts, U.S. task force officers arrested 12 individuals and conducted 104 seizures/abandonments of approximately 24,324 items with an estimated MSRP value of approximately $1.2 million.

- CBP and HSI seized 123 shipments of semiconductor devices affixed with counterfeit trademarks in FY 2017. In total, 49 trademarks were counterfeited in these seizures.

Year in Review

- Consumer Products is a new category of seized products. This category ranks 5th among the top ten categories with 3,912 seizures of products such as insulated drinking tumblers, cell phone and computer accessories, and lights and light fixtures. Some of these goods may have posed threats to health and safety had they not been interdicted.

- Seizures of iconic, mid-century, modern design home and office furniture seizures continued to increase for a second year in a row. There were 38 seizures, and the seized goods would have had an estimated total Manufacturer's Suggested Retail Price of $15.1 million had they been genuine. This represented a 260% increase in seizure value from the previous year. CBP's furniture enforcement efforts have helped to protect over 8,000 American jobs related to the companies that make the genuine furniture. Since these companies also purchase raw materials and parts that are made in the U.S. from other companies, a greater number of American jobs are actually supported.

- A California importer of counterfeit computer networking equipment was sentenced to 37 months in federal prison. CBP identified and seized the counterfeit shipments and referred the case to HSI for criminal investigation. CBP's identification of incoming counterfeit labels led to HSI search warrants resulting in the seizure of counterfeit products, which if genuine, would have had total estimated MSRP value of $2.6 million. The suspect pleaded guilty to attempting to traffic $4 million of counterfeit goods.

- CBP has established 10 Centers of Excellence and Expertise (Centers) to focus CBP's trade expertise on industry-specific issues through account-based processing on a national scale. The Centers, managed from strategic locations around the country, have national authority to make trade decisions at all ports of entry in an effort to meet the goals of strengthening America's economic competitiveness, enhancing industry knowledge and expertise, developing innovative trade processing procedures, applying strategic and impactful trade enforcement actions, and leveraging available trade intelligence. The Centers have been developing and executing enforcement operations to address areas of risk in the IPR Priority Trade Issue. These activities may be directed at a specific port of entry and expanded to all ports of entry as the risk is scoped out nationally.

Year in Review

- During 2017, CBP and ICE continued to implement various *Trade Facilitation and Trade Enforcement Act of 2015* (TFTEA) provisions that specifically call for actions regarding IPR enforcement and provide mechanisms to supplement IPR enforcement. These include mandates to enhance CBP's and ICE's collaboration with rights holders, interagency coordination through the National IPR Coordination Center, and international partnerships to stop counterfeiting at the source.

- Pursuant to the TFTEA Section 308(d), CBP has prescribed regulations 19 CFR 133.61 for receiving donations from private sector parties of hardware, software, equipment, and technologies for the purpose of enforcing IPR.

- In FY 2017, CBP developed and ran *The Truth Behind Counterfeits* public awareness campaign to inform international travelers of the legal, economic and public health and safety impacts of importing IPR infringing merchandise into the United States. The campaign consisted of ads placed on the large electronic bulletin boards at six major airports throughout the United States and online ads on several travel websites during the busy travel months of June and July. The ads were designed to educate travelers on the unknown dangers of counterfeit goods, alert them that purchasing counterfeit goods may support criminal activity, and encourage them to shop from reputable sources. In FY 2017, the campaign reached an estimated 97 million travelers. CBP also launched a dedicated website on the campaign at www.cbp.gov/fakegoodsrealdangers .

- The ICE-led IPR Center engages in partnerships with the public and private sectors to combat IP theft through its Operation Joint Venture initiative. This initiative is designed to increase information sharing with public and private sectors to combat the illegal importation and distribution of counterfeit, substandard and tainted goods. Joint Venture targets rights holders, manufacturers, importers, customs brokers, freight forwarders, bonded facilities, carriers and others to discuss the IPR Center's priorities of protecting public health and safety, the economy, and securing the Government's supply chain. In addition to the industry outreach mission, it conducts domestic and international training of federal, state, local and foreign law enforcement to facilitate seizure of illicit goods. In FY 2017, more that 14,000 people participated in 339 outreach and training events.

Year in Review

- CBP concentrates its IPR border enforcement on federally registered trademarks and copyrights that have been recorded with CBP by their owners using the Intellectual Property Rights e-Recordation (IPRR) system, https://iprr.cbp.gov/. CBP administers these recordations using a secure proprietary database that CBP can access to make IPR border enforcement determinations. Product ID manuals that are prepared by rights holders are also linked to the database and used by CBP in making IPR border enforcement determinations.

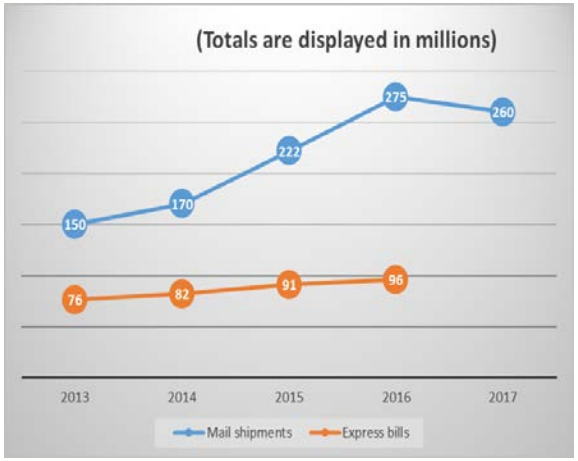
- At the close of FY 2017, CBP enforced trademarks and copyrights pertaining to over 18,209 active recordations, including 2,343 new recordations or renewals of expiring recordations.

- Since August 2016, pursuant to Section 304 of the TFTEA, 22 new recordations were initiated for copyrights which had pending registration applications with the U.S. Copyright Office (USCO). For one right holder, during FY 2017, there were nearly two hundred seizures of athletic shoes involving such recorded but not yet federally registered copyrights. Previously, recordation with CBP was not possible until the copyright was registered with the USCO. Now, once recorded, these unregistered copyrights receive the same benefits of IPR border enforcement and protection as those that are federally registered and recorded.

- CBP works closely with rights holders in making IPR enforcement determinations. A public database of both active and inactive recordations is available using a search engine called the Intellectual Property Rights Search (IPRS) at http://iprs.cbp.gov/. Information on potential IPR infringements can be submitted to CBP using the e-Allegations Online Trade Violation Reporting System at https://eallegations.cbp.gov/Home/Index2.

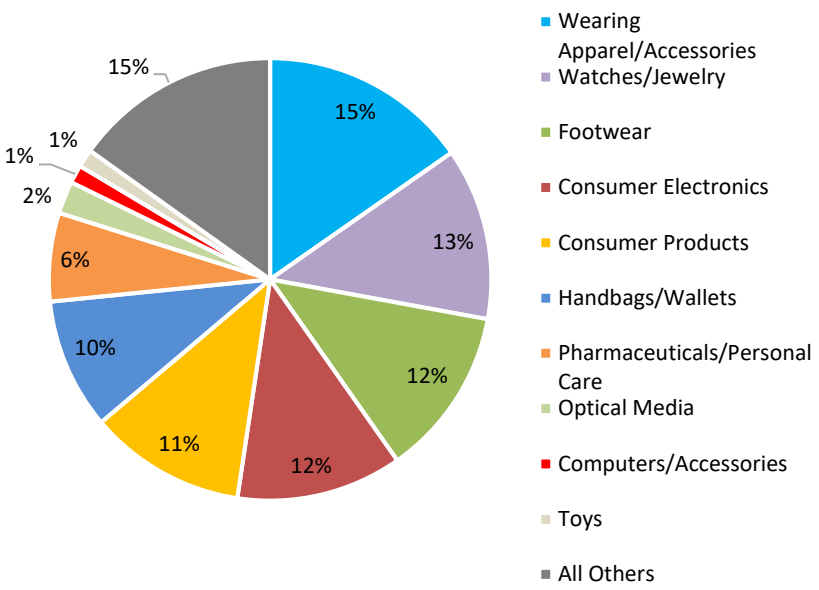
IPR & E-Commerce

- **E-Commerce sales including those through third-party platforms have resulted in a sharp increase in small packages into the U.S. Annually, 260 million packages are shipped through the mail, and there were nearly 100 million bills of lading, which may pertain to more than one package, in the express environment.**
- **89% of all IPR seizures take place in the international mail and express environments.**
- **In September 2016, CBP officially established the e-Commerce and Small Business Branch, which has led the development a strategy and plan for combating violations of U.S. trade and customs laws pertaining to e-commerce shipments.**
- **More e-commerce related information can be found at https://www.cbp.gov/trade/basic-import-export/e-commerce**



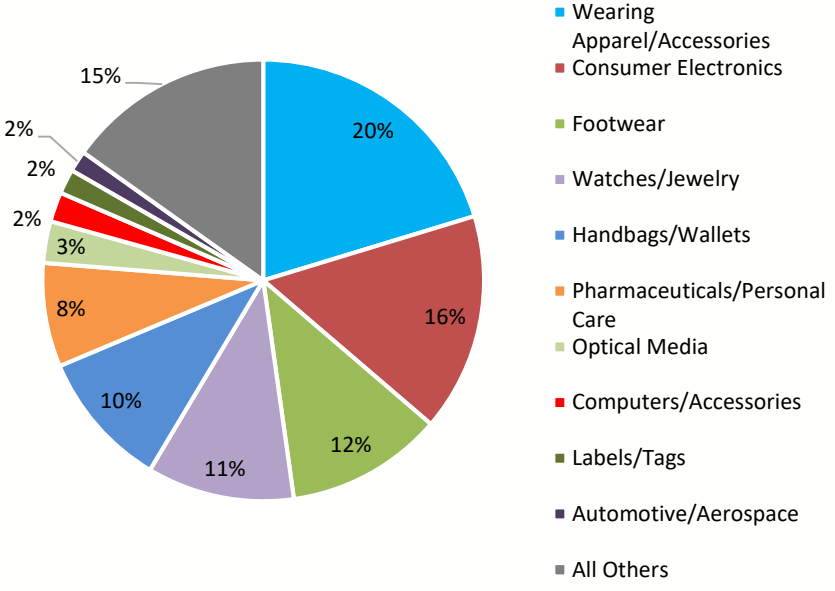
Number of Seizures

Fiscal Year 2017



Total Number of Seizures: 34,143

Fiscal Year 2016



Total Number of Seizures: 31,560

Note: Seizures involving multiple product categories are included in the "All Others" category.

Number of Seizures

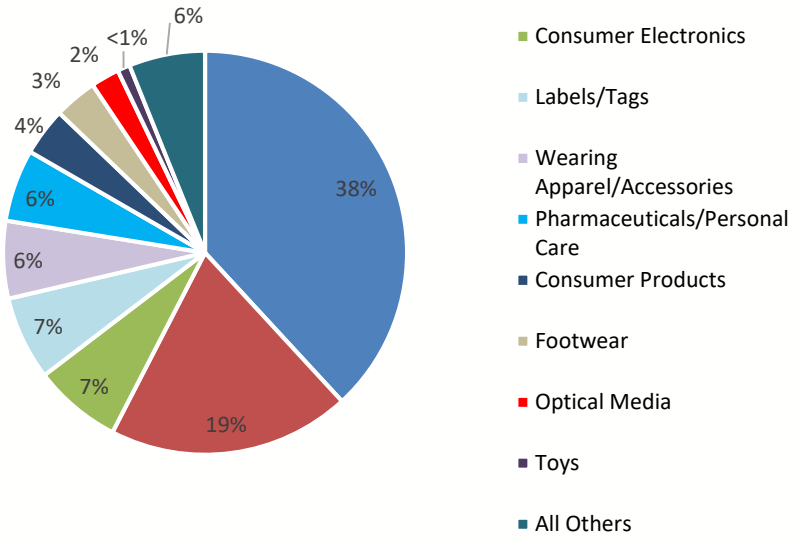
FY 2017 Products	Number of Seizures	Percent of Total
Wearing Apparel/Accessories	5,223	15%
Watches/Jewelry	4,297	13%
Footwear	4,224	12%
Consumer Electronics	4,137	12%
Consumer Products	3,912	11%
Handbags/Wallets	3,266	10%
Pharmaceuticals/Personal Care	2,209	6%
Optical Media	809	2%
Computers/Accessories	454	1%
Toys	449	1%
All Others	5,163	15%
Number of Seizures	***34,143***	

FY 2016 Products	Number of Seizures	Percent of Total
Wearing Apparel/Accessories	6,406	20%
Consumer Electronics	5,043	16%
Footwear	3,630	12%
Watches/Jewelry	3,407	11%
Handbags/Wallets	3,184	10%
Pharmaceuticals/Personal Care	2,401	8%
Optical Media	963	3%
Computers/Accessories	686	2%
Labels/Tags	572	2%
Automotive/Aerospace	486	2%
All Others	4,782	15%
Number of Seizures	***31,560***	

Notes: Seizures involving multiple product categories are included in the "All Others" category.
Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100%.

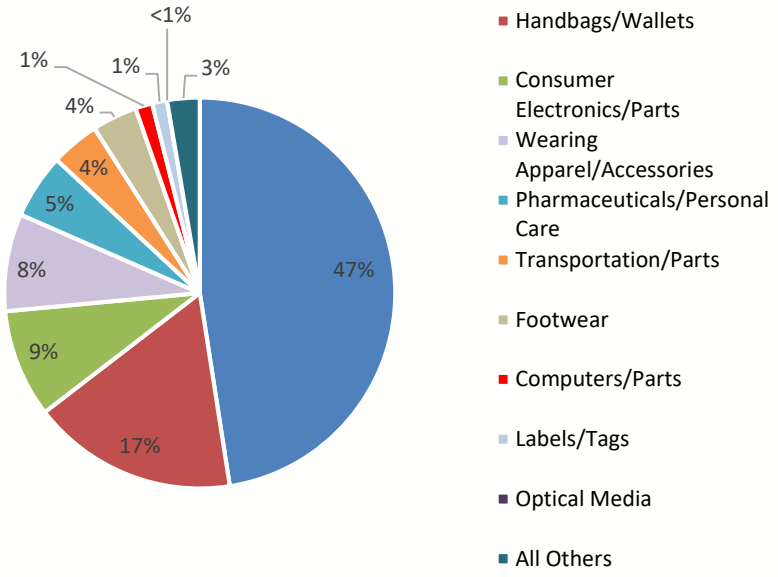
MSRP by Product

FY 2017



Total FY 2017 Est. MSRP: $1,206,382,219

FY 2016



Total FY 2016 Est. MSRP: $1,382,903,001

Note: Seizures involving multiple product categories are included in the "All Others" category.

MSRP by Product

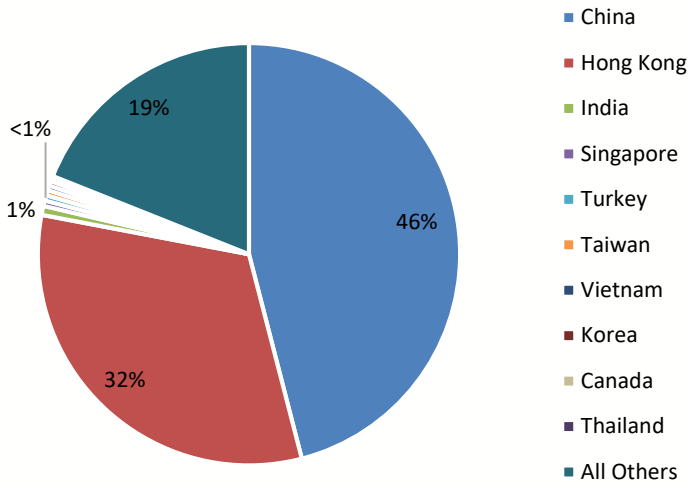
FY 2017 Products		MSRP	Percent of Total
Watches/Jewelry	$	460,162,145	38%
Handbags/Wallets	$	234,451,926	19%
Consumer Electronics	$	85,115,639	7%
Labels/Tags	$	80,951,055	7%
Wearing Apparel/Accessories	$	74,880,617	6%
Pharmaceuticals/Personal Care	$	69,758,720	6%
Consumer Products	$	46,265,355	4%
Footwear	$	41,490,429	3%
Optical Media	$	27,573,775	2%
Toys	$	12,128,156	1%
All Others	$	73,604,401	6%
Total FY 2017 MSRP	*$*	*1,206,382,219*	
Number of Seizures		*34,143*	

FY 2016 Products		MSRP	Percent of Total
Watches/Jewelry	$	653,590,442	47%
Handbags/Wallets	$	234,078,645	17%
Consumer Electronics/Parts	$	122,892,442	9%
Wearing Apparel/Accessories	$	110,805,624	8%
Pharmaceuticals/Personal Care	$	73,716,381	5%
Transportation/Parts	$	55,199,025	4%
Footwear	$	51,231,396	4%
Computers/Parts	$	19,319,416	1%
Labels/Tags	$	17,052,517	1%
Optical Media	$	8,165,968	1%
All Others	$	36,851,145	3%
Total FY 2016 MSRP	*$*	*1,382,903,001*	
Number of Seizures		*31,560*	

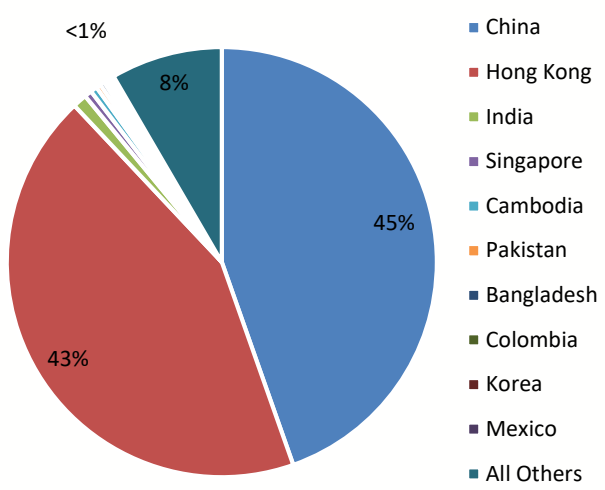
Note: Seizures involving multiple product categories are included in the "All Others" category. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100%.

MSRP by Economy

FY 2017



FY 2016



Total FY 2017 Est. MSRP: $1,206,383,219

Total FY 2016 Est. MSRP: $1,382,903,001

Note: The aggregate seizure data reflect the reported country of origin, not necessarily where the seized goods were produced.

MSRP by Economy

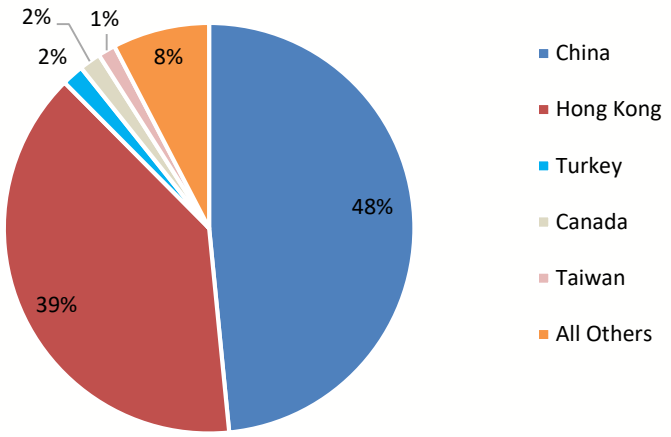
FY 2017 Trading Partner		MSRP	Percent of Total
China	$	554,631,765	46%
Hong Kong	$	386,242,271	32%
India	$	8,341,949	1%
Singapore	$	4,997,430	0.4%
Turkey	$	4,983,051	0.4%
Taiwan	$	4,902,390	0.4%
Vietnam	$	4,391,835	0.4%
Korea	$	4,235,107	0.4%
Canada	$	3,036,994	0.3%
Thailand	$	1,856,892	0.2%
All Others	$	228,762,535	19%
Total FY 2017 MSRP	*$*	*1,206,382,219*	
Number of Seizures		*34,143*	

FY 2016 Trading Partner		MSRP	Percent of Total
China	$	616,881,043	45%
Hong Kong	$	599,785,306	43%
India	$	14,668,153	1%
Singapore	$	7,706,059	1%
Cambodia	$	7,014,825	1%
Pakistan	$	4,776,159	0.3%
Bangladesh	$	4,591,756	0.3%
Colombia	$	4,220,544	0.3%
Korea	$	3,585,190	0.3%
Mexico	$	3,538,991	0.3%
All Others	$	116,134,976	8%
Total FY 2016 MSRP	*$*	*1,382,903,001*	
Number of Seizures		*31,560*	

Note: The aggregate seizure data reflect the reported country of origin, not necessarily where the seized goods were produced. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100%.

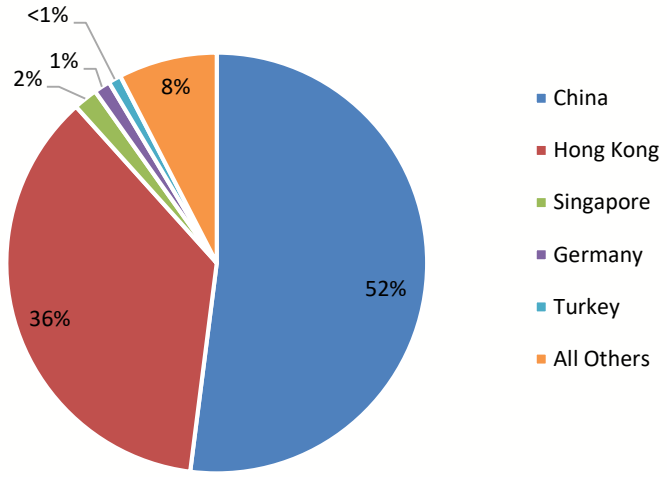
Seizures by Economy

FY 2017



Total Number of Seizures: 34,143

FY 2016



Total Number of Seizures: 31,560

Note: These aggregate seizure data reflect the reported country of origin, not necessarily where the seized goods were produced.

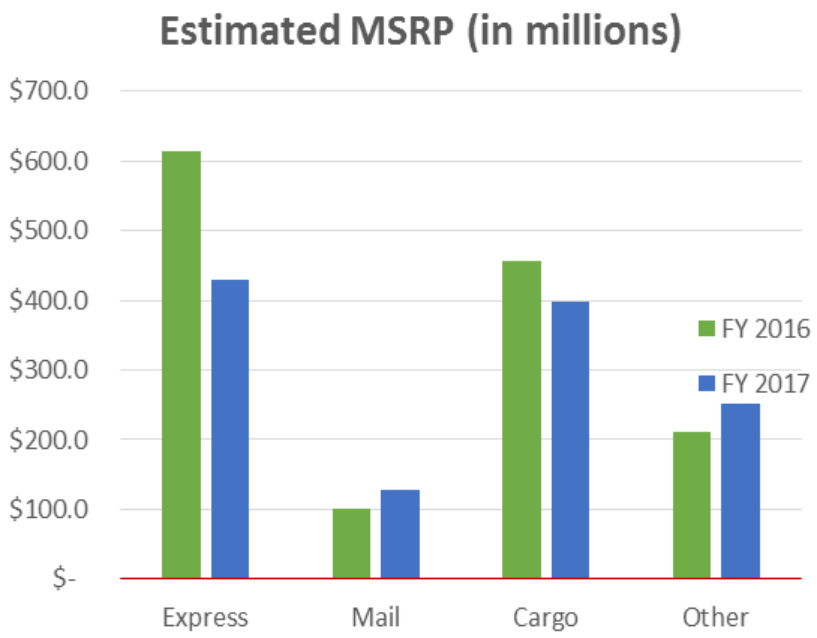
Seizures by Economy

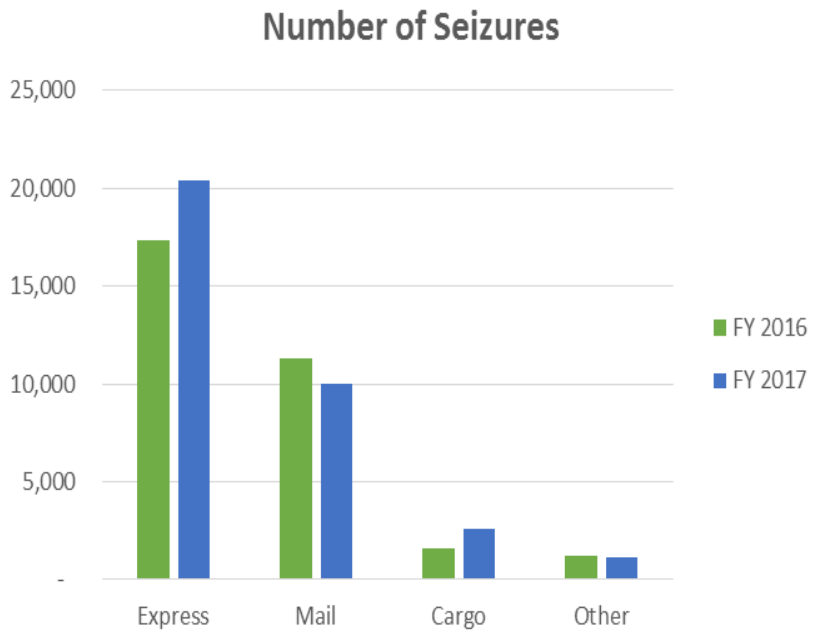
FY 2017 Trading Partner	Number of Seizures	Percent of Total
China	16,538	48%
Hong Kong	13,357	39%
Turkey	587	2%
Canada	581	2%
Taiwan	472	1%
All Others	2,608	8%
Number of Seizures	*34,143*	

FY 2016 Trading Partner	Number of Seizures	Percent of Total
China	16,417	52%
Hong Kong	11,462	36%
Singapore	583	2%
Germany	396	1%
Turkey	309	1%
All Others	2,393	8%
Number of Seizures	*31,560*	

Note: The aggregate seizure data reflect the reported country of origin, not necessarily where the seized goods were produced. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100%.

Modes of Transport





Note: Seizures included in the "Other" category involve exports, passenger baggage, or other enforcement actions.

Modes of Transport

Estimated Manufacturer's Suggested Retail Price (in Millions)

Mode	FY 2016	FY 2016 Percent of Total	FY 2017	FY 2017 Percent of Total	Difference	FY 2016 to FY 2017 Percentage Change
Express	$ 614.5	44%	$ 429.3	36%	$ (185.20)	-30%
Mail	$ 100.4	7%	$ 128.4	11%	$ 28.00	28%
Cargo	$ 457.7	33%	$ 397.5	33%	$ (60.20)	-13%
Other	$ 210.3	15%	$ 251.1	21%	$ 40.80	19%
Total	$ 1,382.9		$ 1,206.3		$ (176.60)	-13%

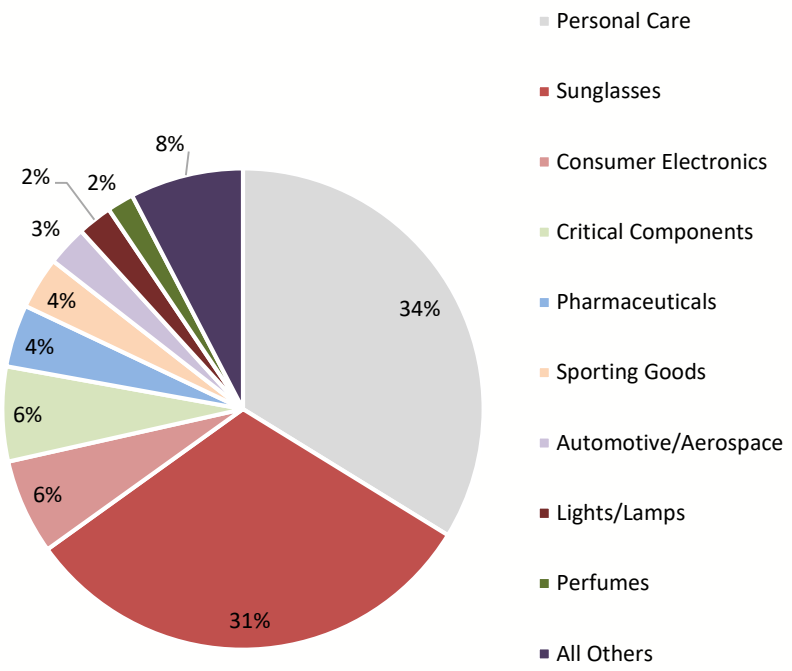
Number of Seizures

Mode	FY 2016	FY 2016 Percent of Total	FY 2017	FY 2017 Percent of Total	Difference	FY 2016 to FY 2017 Percentage Change
Express	17,363	55%	20,417	60%	3,054	18%
Mail	11,326	36%	9,992	29%	(1,334)	-12%
Cargo	1,621	5%	2,628	8%	1,007	62%
Other	1,250	4%	1,106	3%	(144)	-12%
Total	31,560		34,143		2,583	8%

Note: Seizures included in the "Other" category involve exports, passenger baggage, or other enforcement actions. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100%.

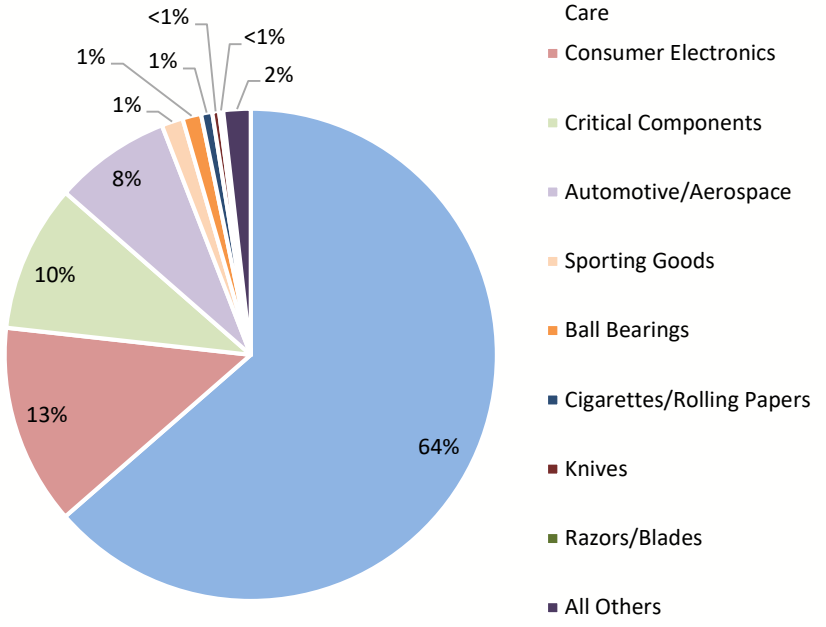
Health, Safety, and Security

FY 2017



Total Number of Seizures: 4,171

FY 2016



Total Number of Seizures: 4,897

Health, Safety, and Security

FY 2017 Health, Safety and Security	Number of Seizures	Percent of Total
Personal Care	1,409	34%
Sunglasses	1,306	31%
Consumer Electronics	267	6%
Critical Components	265	6%
Pharmaceuticals	175	4%
Sporting Goods	146	4%
Automotive/Aerospace	113	3%
Lights/Lamps	97	2%
Perfumes	75	2%
All Others	318	8%
Number of Seizures	*4,171*	

FY 2016 Health, Safety and Security	Number of Seizures	Percent of Total
Pharmaceuticals/Personal Care	3,114	64%
Consumer Electronics	645	13%
Critical Components	474	10%
Automotive/Aerospace	376	8%
Sporting Goods	69	1%
Ball Bearings	60	1%
Cigarettes/Rolling Papers	36	1%
Knives	22	0.4%
Razors/Blades	13	0.3%
All Others	88	2%
Number of Seizures	*4,897*	

Note: Shipments with multiple types of products are included in the "All Others" category.
Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100%.

Exclusion Orders

- CBP enforces exclusion orders issued by the United States International Trade Commission (ITC).
- Most ITC exclusion orders are patent-based.
- The ITC issues both limited and general exclusion orders. Limited exclusion orders apply only to infringing articles of named respondents. General exclusion orders bar the entry of infringing articles by all.
- Exclusion orders prohibit the entry of all covered articles, even if they were not specifically accused and found to infringe by the ITC.
- Once excluded, subsequent importations of the same articles by the same importer are subject to seizure.

Fiscal Year 2016

Shipments Seized	Shipments Excluded	Seizure Est. MSRP	Rulings Issued*	Advice to Ports
52	113	$3,254,654	19	54

Fiscal Year 2017

Shipments Seized	Shipments Excluded	Seizure Est. MSRP	Rulings Issued	Advice to Ports
52	63	$1,865,192	20	64

Note: The term "rulings" covers rulings and other interpretive decisions.

IPR Points of Contact

Contact the IPR Help Desk to Report Violations and Obtain Assistance - CBP's IPR Help Desk is staffed Monday through Friday to answer questions on IPR enforcement. Contact the IPR Help Desk at **(562) 980-3119** ext. **252**, or via email at iprhelpdesk@cbp.dhs.gov.

Consult a CBP IPR Attorney - For those who have legal questions about CBP's IPR enforcement and would like to interface with a CBP IPR attorney, the IPR Branch is available to help. To request information on CBP's recordation program, please contact the IPR Branch at iprrquestions@cbp.dhs.gov. For general inquiries on IPR enforcement, please contact hqiprbranch@cbp.dhs.gov.

Obtain Guidance on CBP IPR Policy and Programs - The IPR Policy and Programs Division (IPR Division) coordinates with rights holders, members of the trade community, CBP staff, other Federal agencies, and foreign governments in developing and implementing the Agency's IPR strategy, policy and programs. To contact the IPR Division, email iprpolicyprograms@cbp.dhs.gov.

e-Allegations - If you are aware of or suspect a company or individual is committing IPR crime, please report the trade violation using CBP's e-Allegations Online Trade Violation Reporting System at https://eallegations.cbp.gov/Home/Index2. Trade violations can also be reported by calling 1-800-BE-ALERT.

National Intellectual Property Rights Coordination Center - To report violations of intellectual property rights, including counterfeiting and piracy, contact the National IPR Coordination Center at https://www.iprcenter.gov/referral/ or telephone 1-866-IPR-2060.

Exhibit 3

UPDATE

TO THE

IP COMMISSION REPORT

THE THEFT OF AMERICAN INTELLECTUAL PROPERTY:
REASSESSMENTS OF THE CHALLENGE
AND UNITED STATES POLICY

2017

UPDATE

TO THE

IP COMMISSION REPORT

THE THEFT OF AMERICAN INTELLECTUAL PROPERTY:
REASSESSMENTS OF THE CHALLENGE
AND UNITED STATES POLICY

This report was published on behalf of
The Commission on the Theft of American Intellectual Property
by The National Bureau of Asian Research.

The Report of the Commission on the Theft of American Intellectual Property (also known as the *IP Commission Report*) was published in May 2013. This update was published in February 2017.

UPDATE

TO THE

IP COMMISSION REPORT

TABLE OF CONTENTS

ACKNOWLEDGMENTS

Over three years ago we co-chaired a report by the Commission on the Theft of American Intellectual Property. The report outlined the enormous magnitude of the problem and presented a series of recommended actions to stem the loss of the lifeblood of American entrepreneurship. The original report received, and continues to receive, widespread public attention. Congress adopted several Commission recommendations to provide the executive branch and private industry with unprecedented, powerful tools with which to fight intellectual property (IP) theft. The executive branch took a limited number of actions, while American businesses have continued to confine their actions to defensive measures. The Commission still believes that IP theft is one of the most pressing issues of economic and national security facing our country. It is our unanimous opinion that the issue has not received the sustained presidential focus and strong policy attention that it requires.

This Commission remains composed of its original, extraordinary members. We are indebted to our fellow Commissioners for their selfless bipartisanship, insights, and help in explaining the original report to the American people, policymakers, and members of the press for over three years.

The Commission's staff has continued to be terrifically effective. It includes several who have remained in their positions, including Commission Director Richard Ellings and Deputy Director Roy Kamphausen. Other stalwarts working on the Commission since the beginning are John Graham, Amanda Keverkamp, and Joshua Ziemkowski. New commission staff who contributed to the update to the original report include Dan Aum, Jessica Keough, Mariana Parks, Craig Scanlan, and Sandra Ward. Special thanks are due to Mike Dyer, who shouldered more than his fair share of this latest round of research, and to outside specialists for their guidance and reviews. The Commission is grateful to The National Bureau of Asian Research (NBR) and its Slade Gorton International Policy Center, which have provided the unrestricted support that has underwritten the Commission's work and complete independence.

The importance of ensuring the viability and success of the U.S.-China relationship in part gave rise to this Commission and our participation in it. We offer this update so that the United States can better understand, prioritize, and solve a critical challenge.

Dennis C. Blair
Co-chair

Jon M. Huntsman, Jr.
Co-chair

The Commission on the Theft of American Intellectual Property is an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academia, and politics. The members are listed in the section About the Commissioners.

The three purposes of the Commission are as follows:

1. Document and assess the causes, scale, and other major dimensions of international intellectual property (IP) theft as they affect the United States.
2. Document and assess the role of China and other infringers in international IP theft.
3. Propose appropriate U.S. policy responses that would mitigate ongoing and future damage and obtain greater enforcement of IP rights (IPR) by China and other infringers.

IP theft pervades international trade in goods and services due to lack of legal enforcement and national industrial policies that encourage IP theft by public, quasi-private, and private entities. While some indicators show that the problem may have improved marginally, the theft of IP remains a grave threat to the United States. Since 2013, at the release of the *IP Commission Report*, U.S. policy mechanisms have been markedly enhanced but gone largely unused. We estimate that the annual cost to the U.S. economy continues to exceed **$225 billion** in counterfeit goods, pirated software, and theft of trade secrets and could be as high as **$600 billion**.[1] It is important to note that both the low- and high-end figures do not incorporate the full cost of patent infringement—an area sorely in need of greater research. We have found no evidence that casts doubt on the estimate provided by the Office of the Director of National Intelligence in November 2015 that economic espionage through hacking costs $400 billion per year.[2] At this rate, the United States has suffered over $1.2 trillion in economic damage since the publication of the original *IP Commission Report* more than three years ago.

Scale and Cost of IP Theft

In three categories of IP theft, new evidence and studies make it possible to provide more accurate assessments of the damage done to the U.S. economy today than was the case in 2013.[3] These categories are counterfeit and pirated tangible goods, pirated software, and trade secret theft.

With regard to the first category, the most reliable data available now suggests that in 2015 the United States imported counterfeit and pirated tangible goods valued between $58 billion and $118 billion, while counterfeit and pirated tangible U.S. goods worth approximately $85 billion were sold that year worldwide.[4] The estimate by the Organisation for Economic Co-operation and

---

[1] On November 18, 2015, William Evanina, national counterintelligence executive of the Office of the Director of National Intelligence, estimated that economic espionage through hacking costs the U.S. economy $400 billion a year, which falls within the range of the findings of the IP Commission. Evanina also stated, "We haven't seen any indication in the private sector that anything has changed [in terms of Chinese government involvement in hacking]." To date, the IP Commission has not found any evidence to the contrary. Chris Strohm, "No Sign China Has Stopped Hacking U.S. Companies, Official Says," Bloomberg, November 18, 2015, https://www.bloomberg.com/news/articles/2015-11-18/no-sign-china-has-stopped-hacking-u-s-companies-official-says. The full report from the Office of the Director of National Intelligence is available from the IP Commission website at http://www.ipcommission.org/report/Evolving_Cyber_Tactics_in_Stealing_US_Economic_Secrets_ODNI_Report.jpg.

[2] Strohm, "No Sign China Has Stopped Hacking U.S. Companies, Official Says."

[3] *The Report of the Commission on the Theft of American Intellectual Property* (Seattle: National Bureau of Asian Research on behalf of The Commission on the Theft of American Intellectual Property, 2013), http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

[4] These values were found using statistics from the Organisation for Economic Co-operation and Development (OECD) and European Union Intellectual Property Office (EUIPO), *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact* (Paris: OECD Publishing, 2016), http://dx.doi.org/10.1787/9789264252653-en.

Development (OECD) and the European Union Intellectual Property Office (EUIPO) for the total value of counterfeit and pirated tangible goods imported into the United States or counterfeit and pirated tangible U.S. goods sold abroad on the conservative low end was $143 billion in 2015. The Commission believes that these goods did not displace the sale of legitimate goods on a dollar-for-dollar basis and estimates that at least 20% of the total amount of counterfeit and pirated tangible goods actually displaced legitimate sales. Thus, the cost to the American economy, on the low end of the estimate, is $29 billion.[5]

The same OECD/EUIPO study found that while 95% of counterfeit goods seized by customs officials were protected by trademarks, only 2% were counterfeits of patent-protected goods.[6] This means that although there is some overlap between our estimates of the value of counterfeit goods and patent infringement, the vast majority of patent infringement is unaccounted for in this report. We are disappointed that there is a paucity of reliable data on the economic costs of patent infringement, but from anecdotal evidence we are led to believe the costs are substantial.

The proliferation of pirated software is believed to be a much larger problem in scope than statistics suggest because of the ease of downloading software, ubiquitous use of software across industries and countries, and inadequate surveys. The value of software pirated in 2015 alone exceeded $52 billion worldwide. American companies were most likely the leading victims, with estimated losses of at least 0.1% of the $18 trillion U.S. GDP, or approximately $18 billion.[7]

The cost of trade secret theft is still difficult to assess because companies may not even be aware that their IP has been stolen, nor are firms incentivized to report their losses once discovered. As IP theft remains hard for firms to detect, much less obtain legal redress for, their incentives are to rely more on their own efforts to conceal trade secrets and less on patents that entail public disclosure.[8] New estimates suggest that trade secret theft is between 1% and 3% of GDP, meaning that the cost to the $18 trillion U.S. economy is between $180 billion and $540 billion.[9]

These figures, while startling, do not take into account the second-order effects on the economy from IP theft. First, there is the practical matter of IP protection costs, which have skyrocketed, especially in response to cyber-enabled IP theft. More importantly, when trade secrets and other IP are stolen by competitors, U.S. firms are discouraged from investing the substantial capital required to innovate or effort required to work to be the first movers to market. The immediate and long-term loss of these advantages makes American firms less competitive globally.

China

China, whose industrial output now exceeds that of the United States, remains the world's principal IP infringer. China is deeply committed to industrial policies that include maximizing the

---

[5] For purposes of aggregating the direct costs of IP theft in the three listed categories—counterfeit and pirated tangible goods, software piracy, and trade secret theft—the Commission estimates that no less than 20% of counterfeit sales would displace legitimate sales. However, the precise amount is unknowable, because the purchase of counterfeit goods does not displace the sale of legitimate goods on a dollar-for-dollar basis. For more discussion on the complex relationship between counterfeit and legitimate sales, see OECD, "The Economic Impact of Counterfeiting," 1998, 26–29, https://www.oecd.org/sti/ind/2090589.pdf.

[6] OECD and EUIPO, *Trade in Counterfeit and Pirated Goods*.

[7] Business Software Alliance (BSA), "Seizing Opportunity through License Compliance," BSA Global Software Survey, May 2016, http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf.

[8] R. Mark Halligan, "Trade Secrets v. Patents: The New Calculus," *Landslide*, July/August 2010, http://www.americanbar.org/content/dam/aba/migrated/intelprop/magazine/LandslideJuly2010_halligan.authcheckdam.pdf.

[9] Center for Responsible Enterprise and Trade (CREATe.org) and PricewaterhouseCoopers, "Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats," 2014, https://create.org/resource/economic-impact-of-trade-secret-theft.

acquisition of foreign technology and information, policies that have contributed to greater IP theft. IP theft by thousands of Chinese actors continues to be rampant, and the United States constantly buys its own and other states' inventions from Chinese infringers. China (including Hong Kong) accounts for 87% of counterfeit goods seized coming into the United States.[10]

China continues to obtain American IP from U.S. companies operating inside China, from entities elsewhere in the world, and of course from the United States directly through conventional as well as cyber means. These include coercive activities by the state designed to force outright IP transfer or give Chinese entities a better position from which to acquire or steal American IP.

U.S. Policy Response

After the release of the *IP Commission Report* in May 2013, the Obama administration and Congress made important procedural changes to how the United States defends itself from IP theft and related cyberattacks, but they have been applied unevenly.

First, there are several positive developments. Chief among them is that cyberattacks may have declined in volume since about 2014, although whether this is a result of a crackdown in China on responsible units in the People's Liberation Army (PLA) or other factors is not entirely clear. In any case, the cyber units of the PLA may have responded by shifting their tactics from blatant mass hacking of U.S. entities to a more targeted and discreet approach.[11]

Second, the gravity and complexity of IP theft are better understood today than in 2013. Our report and other studies raised public awareness through extensive media coverage and government attention. The *IP Commission Report* continues to be cited by the world's press and commentators. The report was downloaded over 20,000 times in the first week of its release and over 200,000 times since then. It has come to be viewed as the foundational study in the field.

Implementation is the major challenge today. The Obama administration and Congress adopted some of the report's key recommendations that set in place the legal basis for combatting IP theft successfully. The report's major impact is Section 1637 of the 2015 National Defense Authorization Act (NDAA). The law requires the president to issue a report on economic cyberespionage and on actions taken by the executive branch against those who are stealing American IP through cyber means. More importantly, the language gives the president the power to sanction foreign entities, from persons to companies to countries. The deadline for issuance of the report was June 17, 2015. Unfortunately, however, the report was not published until November 2016, and it gives no indication that President Obama used Section 1637 to sanction foreign IP infringers.

In addition, last year Congress passed, and President Obama signed, the Defend Trade Secrets Act of 2016, which, among other things, creates a private right of action for U.S. entities under the Economic Espionage Act. This was another IP Commission recommendation. The president took into account some of our recommendations for cybersecurity when he implemented the administration's Cybersecurity National Action Plan and signed Executive Order 13691 to mitigate vulnerabilities in cyberspace and increase cooperation between the private and public sectors on this issue. The National Cybersecurity and Communications Integration Center has proved effective, as far as we can ascertain.

---

[10] U.S. Customs and Border Patrol, "Intellectual Property Rights Seizure Statistics Fiscal Year 2015," 2016, https://www.cbp.gov/sites/default/files/assets/documents/2016-Apr/FY%202015%20IPR%20Stats%20Presentation.pdf.

[11] FireEye iSight Intelligence, "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," Special Report, June 2016, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Introduction

As the authors of the original *Report of the Commission on the Theft of American Intellectual Property* (also known as the *IP Commission Report*), we were encouraged by the widespread interest in the report and its impact on new legislation. In addition to the high volume of downloads, the report was regularly cited, quoted, or referred to in the national and international media, including the *New York Times*, *Wall Street Journal*, *Washington Post*, and *Economist*.

We are pleased that Congress and the Obama administration took the lead from our report and implemented several of our top recommendations. Congress gave the president the power to sanction foreign entities that engage in cyberespionage of IP and gave U.S. entities private right of action in federal courts against thieves of their trade secrets. For its part, the Obama administration set up a mechanism to sanction foreign persons engaged in "significant malicious activities."[12]

Despite the success of the report and resulting legislation, there is still much work that needs to be done. We estimate that at the low end the annual cost to the U.S. economy of several categories of IP theft exceeds $225 billion, with the unknown cost of other types of IP theft almost certainly exceeding that amount and possibly being as high as $600 billion annually.[13] Further, while cyberespionage may have decreased from some actors, several sources report that the worst and most capable actors still persist in hacking for economic gain. IP thieves continue to use traditional means to attack targets.

What follows is an update to our original report. This update begins with an overview of the legislative and executive actions that the U.S. government has taken since 2013. It moves on to assess the economic cost of IP theft and discuss the challenges to IP protections abroad that persist despite attempts to deal with the problem. In the conclusion, we argue that Section 1637 of the 2015 NDAA needs to be implemented and that many of our original recommendations remain relevant and ripe for adoption. Our recommendations are outlined in detail in the appendix.

New Developments to Counter IP Theft

After the release of the *IP Commission Report* in May 2013, the Obama administration and Congress took several actions to reduce the theft of American IP. Some of the policies enacted have borrowed from the recommendations that the Commission made in 2013, while others have fallen short and left the Commission wanting more. Outlined below are the statutory and executive actions that the U.S. government has implemented over the past three-plus years:

Indictment of five PLA officers. One year after the release of the *IP Commission Report*, the Department of Justice indicted five members of PLA unit 61398 in Shanghai on economic espionage charges. The indictment alleges the PLA officers hacked into the networks of several U.S. companies and maintained access over several years to steal trade secrets and other sensitive information. The indictment of the five officers signified a break with the Obama administration's strategy of

[12] "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," Executive Order 13694, April 1, 2015, Code of Federal Regulations, title 3 (2015), 297–99, https://www.gpo.gov/fdsys/pkg/CFR-2016-title3-vol1/pdf/CFR-2016-title3-vol1-eo13694.pdf.

[13] As noted in the Executive Summary, in November 2015 William Evanina, national counterintelligence executive of the Office of the Director of National Intelligence, estimated that economic espionage through hacking costs the U.S. economy $400 billion a year, which is within the range of the IP Commission's findings. See Strohm, "No Sign China Has Stopped Hacking U.S. Companies, Official Says." The full report from the Office of the Director of National Intelligence is available from the IP Commission website at http://www.ipcommission.org/report/Evolving_Cyber_Tactics_in_Stealing_US_Economic_Secrets_ODNI_Report.jpg.

quietly pressuring the Chinese government to establish mutually acceptable norms in cyberspace.[14] However, the indictment is largely symbolic; the PLA officers will likely never be tried in a U.S. court as they are unlikely to travel to the United States. The action seemed intended to shame the People's Republic of China (PRC) as publicly as possible, but in reality it probably served to disperse the hackers away from the PLA unit and the associated unit headquarters, without achieving real punishment for cyberattacks.

2015 National Defense Authorization Act, Section 1637, Actions to Address Economic or Industrial Espionage in Cyberspace. The language of the section is remarkably similar to the Deter Cyber Theft Act, which was introduced in its original sanction-less form in May 2013 by Senator Carl Levin, then chairman of the Senate Armed Services Committee. (The bill cosponsors included Senator John McCain, current chairman of the committee.) In May 2014 the Deter Cyber Theft Act was reintroduced with the sanctions provision and was referred to the Senate Banking, Housing, and Urban Affairs Committee, where no action was taken. In December 2014, Section 1637 was included in the 2015 NDAA.

Section 1637 has two major components. First, it directs the president to submit a report to Congress that contains a list of countries that engage in "economic and industrial espionage in cyberspace" and a list of technologies or services that are being targeted by foreign actors. The list of countries is similar to that of the Special 301 Report published by the United States Trade Representative (USTR). Both require "priority" categories for the most egregious offending countries. The report also must identify the actions taken by the president to "decrease the prevalence of economic or industrial espionage in cyberspace."[15] The National Counterintelligence and Security Center released the report in November 2016—some seventeen months late. The report outlines how state intelligence services have improved their cyberespionage techniques over the past several years while U.S. companies have become more vulnerable targets due to increased use of the cloud and other factors. The report concludes that the cost from cyber theft to U.S. businesses appears to be increasing.[16]

Second, and more importantly, the bill authorizes the president "to prohibit all transactions in property" of any person who the president determines "knowingly engages in economic or industrial espionage in cyberspace."[17] This authority is an expansion of the long-standing International Emergency Economic Powers Act (IEEPA). There are two points worth considering on what counts as a "person." First, the bill is limited to foreign persons. Therefore, people within the United States still must be prosecuted under the Economic Espionage Act. Second, IEEPA has been used for many years, and it has targeted organizations as well as people.

---

[14] Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times*, May 19, 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html.

[15] U.S. Congress, *Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015*, 113th Cong., Public Law 113-291 (Washington, D.C., December 19, 2014).

[16] Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Evolving Cyber Tactics in Stealing U.S. Economic Secrets: Report to Congress on Foreign Economic Collection and Industrial Espionage in Cyberspace 2015," 2016, available at http://www.ipcommission.org/report/Evolving_Cyber_Tactics_in_Stealing_US_Economic_Secrets_ODNI_Report.jpg. Much of the data in the report only goes through 2015. For a report dated November 2016, we had hoped that more current data would be available. The report also lacks the priority country list and the description of actions taken by the executive to decrease economic espionage in cyberspace, as mandated by Section 1637. As noted above, the report concludes that the problem is growing worse due to several factors. These findings would seem to contradict President Obama's assertion that cyber theft would get better in light of the agreement he struck with President Xi Jinping.

[17] For the purposes of Section 1637, cyberspace is defined as "the interdependent network of information technology infrastructures" and includes "the internet, telecommunications networks, computer systems, and embedded processors and controllers." See U.S. Congress, *Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015*.

Five months after this legislation was signed into law, President Obama signed Executive Order 13694 invoking the IEEPA emergency powers as urged by Congress, but unfortunately he apparently never applied them to address the problem of IP theft. See the section below on Executive Order 13694 for more information.

National Cybersecurity Protection Act of 2014. This law amends the Homeland Security Act of 2002 and codifies the Department of Homeland Security's cybersecurity operations center (the National Cybersecurity and Communications Integration Center, or NCCIC). It grants authority for the Department of Homeland Security to work with private and public entities to encourage information sharing, including with international partners. It further instructs the NCCIC to report to Congress on several issues, including the secretary's recommendations for how to "expedite the implementation of information-sharing agreements" between the public and private sectors and the NCCIC's progress in creating the center and implementing the law. The act also introduces a federal agency "data breach notification" law, requiring federal agencies to notify Congress and individuals affected by a data breach as quickly as possible. (There are already 47 states with similar data statutes requiring agencies to alert applicable persons.)

Federal Information Security Modernization Act (FISMA) of 2014. This law amends the Federal Information Security Management Act of 2002 and instructs agencies to update their monitoring systems for identifying data security compliance. Currently these processes require a lot of redundant paperwork. FISMA outlines responsibilities for agencies and forces them to develop better information security practices.

Cybersecurity Workforce Assessment Act of 2014. This act mandates that the Department of Homeland Security review, update, and bolster its cybersecurity workforce. It also requires the secretary of homeland security to develop a strategy to enhance "the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department."

Cybersecurity Enhancement Act of 2014. With the aim to enhance the security of federal networks and to "support the development of a voluntary, consensus-based, industry-led set of standards," the Cybersecurity Enhancement Act of 2014 authorizes the National Institute of Standards and Technology to coordinate and consult with government agencies and the private sector to develop best practices, including establishing research centers and scholarships for cultivating cybersecurity professionals.

Executive Order 13691 of February 13, 2015, promoting private-sector cybersecurity information sharing. Executive Order 13691 establishes "information-sharing and analysis organizations" to strengthen the security cooperation among private industries, nongovernmental organizations, and the federal government. The administration hopes these organizations will help U.S. firms in the asymmetrical fight against state-sponsored cyberespionage.

Executive Order 13694 of April 1, 2015, blocking the property of certain persons engaging in significant malicious cyber-enabled activities. As urged by Congress in Section 1637 of the 2015 NDAA, President Obama signed Executive Order 13694 blocking the transfer, payment, or export of property of individuals who have engaged in cyberespionage directed against the "national security, foreign policy, economic health, or financial stability of the United States." The executive order specifically states that it will apply to individuals engaged in misappropriating trade secrets for commercial or competitive advantage as well as to the commercial entities in receipt of such information. President Obama declared that the national emergency would continue for another

year on March 29, 2016, as required by law. As of December 2016, Executive Order 13694 had yet to be used against any individual in response to IP theft.[18]

Executive Order 13718 of February 9, 2016, establishing the Commission on Enhancing National Cybersecurity. President Obama established the bipartisan Commission on Enhancing National Cybersecurity to make "detailed recommendations to strengthen cybersecurity in both the public and private sectors" through raising awareness, studying risk management strategies, and developing methods to improve the adoption of best practices throughout the government. The commission's goal was to seek input from both cybersecurity experts and the victims of significant cybersecurity incidents to identify barriers to improved cybersecurity. The commission submitted its final report in early December 2016.

Defend Trade Secrets Act of 2016. Signed into law on May 11, 2016, the bipartisan Defend Trade Secrets Act establishes private right of action in federal court for U.S. entities that have had their trade secrets stolen and offers them protections in the course of a trial to prevent their trade secrets from becoming public. This was a key recommendation of the IP Commission in 2013. Prior to the passage of the act, a victim of trade secret theft could only seek a remedy with a civil suit in a state court unless the Department of Justice filed a criminal suit, which was rare.[19] The act also requires the Department of Justice to submit a report to Congress on the size and scope of trade secret theft outside the United States no later than one year after the date of enactment of the law and to offer recommendations for combating such theft. At the time of writing, the report, if submitted, is not publicly available

IPEC Joint Strategic Plan on Intellectual Property Enforcement FY2017–2019. Published by the Office of the Intellectual Property Enforcement Coordinator (IPEC), this report was mandated by the Prioritizing Resources and Organization for Intellectual Property Act and presents an account of the economic cost of IP theft and the various methods employed to commit IP-related crime. It then offers several recommendations for securing cross-border trade and promoting frameworks to enhance IPR enforcement.[20] The report was released in the final month of the Obama administration, and the effect on the Trump administration is yet to be determined.

State of the Problem: Damage Report

Despite executive and legislative action to stem the damage from IP infringement, the incentives to steal IP persist, due in part to weak enforcement and penalties and in part to foreign industrial policies and practices. The annual cost to the U.S. economy from IP theft remains in the hundreds of billions of dollars. This update to the *IP Commission Report* provides a conservative, low-end estimate of the cost of IP theft in three categories—counterfeit and pirated tangible goods, software piracy, and trade secret theft—to be in excess of $225 billion, and the cost is possibly as high as $600 billion.

---

[18] Executive Order 13694 was amended on December 29, 2016, and applied to sanction nine individuals and entities "in response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election." "Executive Order—Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," White House, Press Release, December 29, 2016, https://www.whitehouse.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency.

[19] "Congress Authorizes Federal Cause of Action for Trade Secret Misappropriation," Lexology, 2006, http://www.lexology.com/library/detail.aspx?g=9c07d09d-67b7-4937-af54-c7a313bcb85e.

[20] Intellectual Property Enforcement Coordinator, *U.S. Joint Strategic Plan on Intellectual Property Enforcement FY2017–2019: Supporting Innovation, Creativity & Enterprise* (Washington, D.C., December 2016), https://www.whitehouse.gov/sites/default/files/omb/IPEC/2016jointstrategicplan.pdf.

The Continuing Significance of the Problem

The threat to American IP-intensive industries stems from the difficulty of enforcing protections against advanced and persistent foreign threats. Law enforcement lacks the capacity to patrol and protect the vast U.S. business community. When foreign actors are implicated in stealing American IP, it is highly unlikely that they will ever be brought to justice in a U.S. court, as evidenced by the indictment of the five PLA officers implicated in the theft of IP from six U.S. companies.[21] The problem is made worse by foreign industrial policies and practices that rely on securing new technologies cheaply to catch up with developed economies.

The threat of IP theft is in turn significant because of IP's contribution to the U.S. economy. IP protection is important to every business, as trade secrets and trademarks pervade the private sector. According to the Global Intellectual Property Center of the U.S. Chamber of Commerce, sales from IP-intensive firms totaled $6.9 trillion in 2013. IP-intensive industries are also responsible for 56 million jobs in the United States—roughly 35% of the U.S. labor force. Moreover, a job with an IP-intensive company pays on average 26% more than a job with a non-IP-intensive company.[22]

The Difficulty in Measuring the Damage

Measuring the economic impact of IP infringement and counterfeit goods is extraordinarily difficult because of the illicit nature of piracy and trading in counterfeit goods, the ease of using pirated software, and the disincentives associated with reporting trade secret theft. Victims of trade secret theft—to the extent that they are aware of the crime—are often reluctant to share information on the resulting financial loss (when such theft necessitates disclosure) out of fear of declining investment opportunities or diminished market valuation.

Most statistics of trade in counterfeit tangible goods are based on seizure data reports from the Customs and Border Patrol (CBP), with the understanding that customs officials only capture a small portion of counterfeit goods entering U.S. territory at the border and the statistics do not account for counterfeit goods exchanged within the United States. They also do not capture data for counterfeit U.S. goods sold in foreign markets, nor do they take into account the vast amount of pirated goods, which is even more difficult to measure. Moreover, even if the total amount of pirated and counterfeit goods entering the United States could be quantified, this figure would only represent the value of these goods and not necessarily the value of lost revenues. Finally, it is difficult to measure how many buyers know that what they are purchasing is counterfeit and would not otherwise be in the market for legitimate goods at an authorized price.

Despite these difficulties, the damage to the U.S. economy can still be estimated by using existing data and proxies. The following discussion provides a range for the cost to the U.S. economy of counterfeit and pirated tangible goods, software piracy, and trade secret theft.

Estimate of the Cost of IP Theft

Counterfeit and pirated tangible goods. In 2016, the OECD and EUIPO used worldwide seizure statistics from 2013 to calculate that up to 2.5%, or $461 billion, of world trade was in counterfeit

---

21 "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

22 U.S. Chamber of Commerce Global Intellectual Property Center, "Employing Innovation across America," 2016, http://image.uschamber.com/lib/fee913797d6303/m/1/GIPC_Employing_Innovation_Report_2016.pdf.

or pirated products.[23] By applying this percentage to U.S. trade, we estimate that in 2015 the value of these goods entering the U.S. market was at least $58 billion.

The United States, however, is a much larger market for imports than the average market. It is nearly equivalent in size to the European Union, where the OECD/EUIPO study determined that approximately 5% of imports are counterfeit or pirated tangible goods.[24] By using 5% as a proxy for the proportion of counterfeit and pirated tangible goods in U.S. imports ($2.273 trillion),[25] we estimate that the United States may have imported up to $118 billion of these goods in 2015. Thus, anywhere from $58 billion to $118 billion of counterfeit and pirated tangible goods may have entered the United States in 2015. This represents the approximate value of counterfeit and pirated tangible goods (not services) entering the country.

With respect to counterfeit and pirated tangible U.S. goods sold in foreign markets, the OECD/EUIPO study found that they accounted for nearly 20% of the value of reported worldwide seizures.[26] In 2015, estimated worldwide seizures of counterfeit goods totaled $425 billion, meaning that as much as $85 billion of counterfeit U.S. goods (20% of worldwide seizures) entered the world market (including the U.S. market).[27]

Certainly, in the absence of counterfeit goods some sales would never take place, and thus the value of illegal sales is not the same as the sales lost to U.S. firms. The true cost to law-abiding U.S. firms in sales displaced due to counterfeiting and pirating of tangible goods is unknowable, but it is almost certain to be a significant proportion of total counterfeit sales. For purposes of aggregating the total cost to the U.S. economy of IP theft, we have estimated that 20% of counterfeits might have displaced actual sales of goods. *When applied to the low-end estimate ($143 billion) of the total value of counterfeit and pirated tangible goods imported into the United States and counterfeit and pirated tangible U.S. goods sold abroad, the conservative estimate of the cost to the U.S. economy is $29 billion. When applied to the high-end estimate ($203 billion), the cost to the U.S. economy is estimated at $41 billion.*

How much of that total is intercepted by customs officials, where does it come from, and how does it get to the United States? CBP releases the Intellectual Property Rights Seizure Statistics each year. From the nearly 29,000 seizures in 2015, CBP seized $1.35 billion in counterfeit goods at the U.S. border, or 1.2%–2.3% of the estimated total value of counterfeit goods entering the United States, according to the approximation from the OECD/EUIPO model.[28] Worldwide, counterfeit goods travel mostly by postal service (62%) and quite often in small shipments of ten items or fewer (43%).[29] This makes seizing them extraordinarily difficult.

CBP also tracks from where the counterfeit goods are imported. Slightly more than half (52%) of all counterfeit goods entering the United States come from mainland China.[30] This is significantly

---

23 OECD and EUIPO, *Trade in Counterfeit and Pirated Goods*. Because the dynamics of trade have changed since 2013, and because the United States is a larger market for imports than the average country, the 2.5% figure is not directly applicable to the United States, but it can provide a rough approximation in the absence of updated data.

24 Ibid.

25 U.S. Bureau of Economic Analysis, "U.S. International Transaction Tables," December 2016, https://www.bea.gov/scb/pdf/2017/01%20January/0117_international_transactions_tables.pdf. It should be noted that there are significant differences between the two economies, including apparently more porous borders in the European Union. As a result, the EU economy is not a perfect proxy for the U.S. economy.

26 OECD and EUIPO, *Trade in Counterfeit and Pirated Goods*.

27 Ibid.

28 U.S. Customs and Border Patrol, "Intellectual Property Rights Seizure Statistics Fiscal Year 2015."

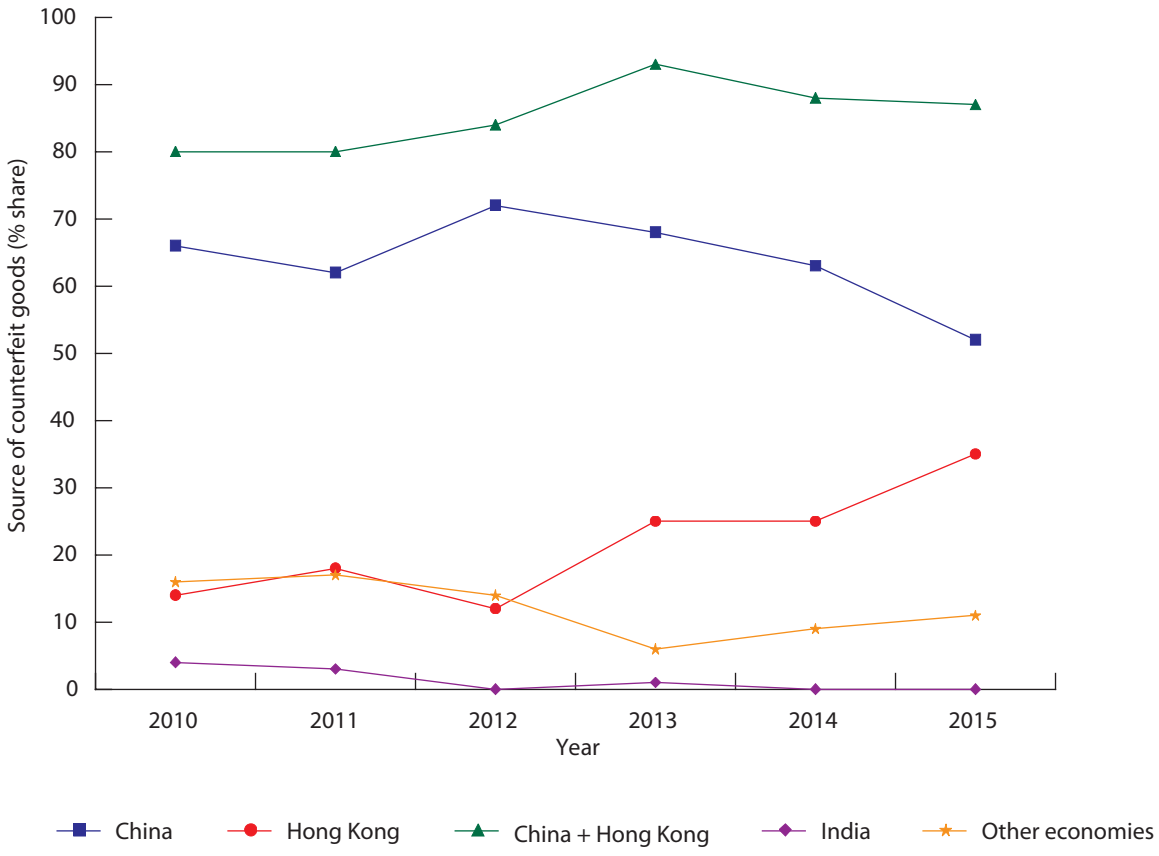
29 OECD and EUIPO, *Trade in Counterfeit and Pirated Goods*.

30 Ibid.

lower than in 2013, which saw 68% of counterfeit goods coming from mainland China. However, these improvements are offset by the increase in counterfeit goods imported from Hong Kong, which, although a separate customs territory and economic entity, is under PRC sovereignty, allowing for a more fluid border with regard to the transport of goods in some cases. The PRC as a whole (including Hong Kong) accounts for 87% of all counterfeit goods seized. This is only slightly lower than in 2013 and is slightly higher than the five-year average. All other economies combined represent around 13% of imported counterfeit goods (see **Figure 1**). It is not just the United States that is receiving counterfeits from China; 80% of the counterfeits seized in Canada are China-sourced as well.[31]

Patent infringement. Unfortunately, our investigation has revealed no reliable quantitative data on the economic cost of patent infringement to the U.S. economy, and therefore this is not included in our total figures. However, through testimony to the Commission and anecdotal evidence in the press, we can conclude that the cost to U.S. businesses from patent infringement abroad is at least in the billions of dollars, although the full scale cannot be estimated.[32] China presents a mixed case. Of particular note, China has become the top source of new patents, accounting for around one-third

FIGURE 1 Source economies of counterfeit goods



[31] "RFA: China Has Become the Largest Fake Product Source for Canada's Online Market," Chinascope, December 13, 2016, http://chinascope.org/archives/10777.

[32] As noted in our 2013 report, the U.S. International Trade Commission (USITC) estimated that U.S. companies suffered $0.2 billion to $2.8 billion in losses from Chinese patent infringement in 2009 alone. USITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy* (Washington, D.C., May 2011), 3–37, http://www.usitc.gov/publications/332/pub4226.pdf.

of all new patents filed in 2015.[33] However, many of these are "petty" or "utility" patents, which grant protections to rights holders without questioning how innovative the subject matter might be.[34] These patent holders are then able to sue foreign companies bringing their IP into the Chinese market. For more background on patent infringement, please see our original report.

Pirated software. The Business Software Alliance (BSA) and International Data Corporation track the rates and value of illicit software in use throughout the world.[35] According to their 2015 data, the "shadow market" for globally pirated software shrunk approximately 17% from $62.7 billion in 2013 to $52.2 billion in 2015.[36] *The low-end estimate for the cost to U.S. firms is $18 billion, using 0.1% of U.S. GDP as a proxy—a percentage in line with BSA's historical estimates of global software piracy.*[37]

Globally the proportion of illicit software was 39% in 2015, down from 43% in 2013. The Asia-Pacific region remains the worst offender, with 61% of all software in use being illicit—which amounts to 36% of the world's illicit software value (see **Figure 2**).[38] Lost sales from pirated goods are difficult to quantify.

The BSA study finds a strong correlation (0.78 coefficient) between illicit software and harmful malware. In a separate study based on data from its wide network of users, Symantec discovered "more than 430 million new unique pieces of malware, up 36 percent from the year before."[39] Malware and ransomware are often components of cyberattacks.

Theft of trade secrets. Of all the forms of IP theft, trade secret theft—in an increasing number of cases enabled by cyberespionage—might do the greatest damage to the U.S. economy. In a 2014 study, "Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats," PricewaterhouseCoopers and the Center for Responsible Enterprise and Trade, using several proxy measures, found that trade secret theft could be estimated to be between 1% and 3% of GDP.[40] Given this calculation, the economic impact of trade secret theft on the U.S. economy in 2015 is estimated to be between $180 billion and $540 billion. *Using the lower end of the range, we estimate that trade secret theft costs the U.S. economy at least $180 billion per year.*

Cyber theft is a cheap way to avoid costly and time-intensive R&D that may simply be beyond the thieves' capacity. Foreign firms benefiting from the cyber theft of American IP are thus able to sell goods and services developed using stolen IP at a much cheaper price than firms investing in R&D organically.

---

33 "Global Patent Applications Rose to 2.9 Million in 2015 on Strong Growth from China; Demand Also Increased for Other Intellectual Property Rights," World Intellectual Property Organization, Press Release, November 23, 2016, http://www.wipo.int/pressroom/en/articles/2016/article_0017.html.

34 USITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*.

35 We consider pirated software as one category of pirated digital goods (other categories include all forms of digital media) that is separate from pirated tangible goods. There is much reliable data on counterfeit and pirated tangible goods based on seizure statistics from customs and border patrol agencies, but much less data is available on pirated digital goods as a result of the ease of downloading and sharing pirated digital content.

36 BSA, "Seizing Opportunity through License Compliance."

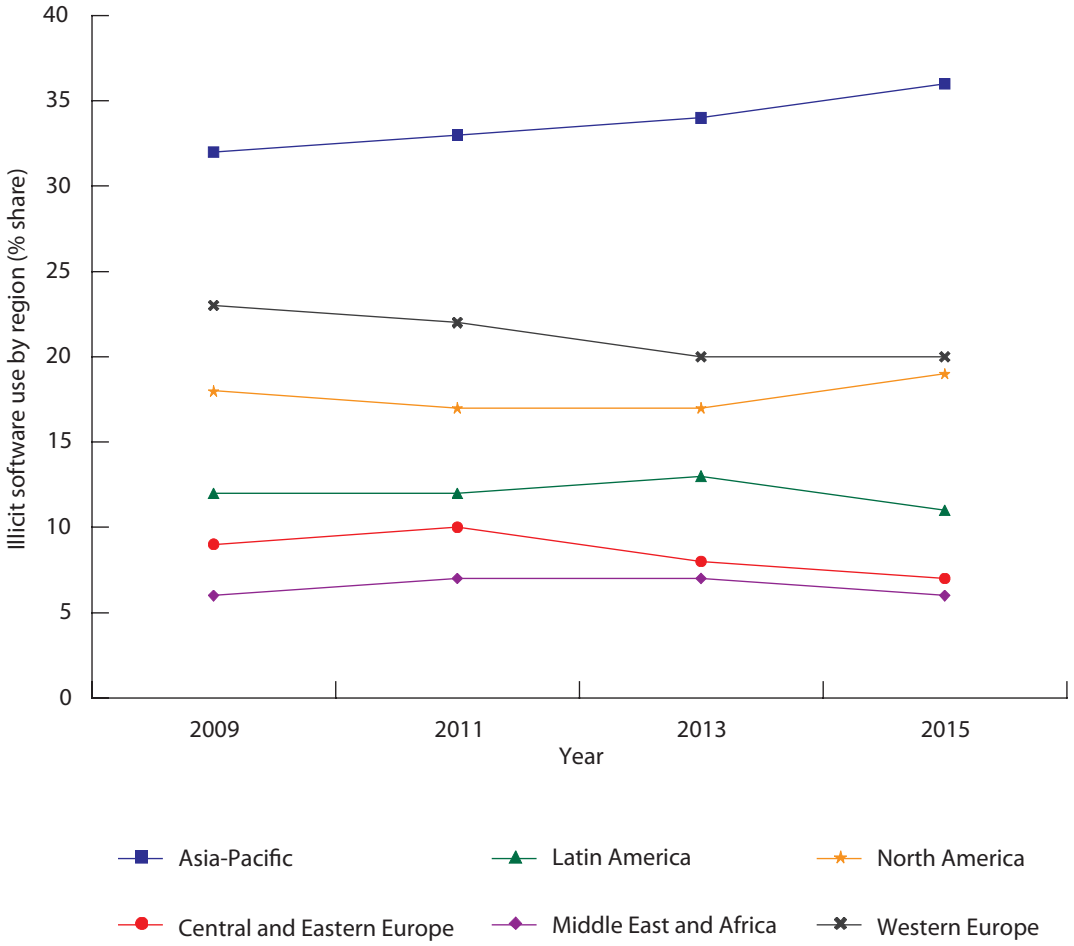
37 CREATe.org and PricewaterhouseCoopers, "Economic Impact of Trade Secret Theft."

38 BSA, "Seizing Opportunity through License Compliance."

39 Symantec, "Internet Security Threat Report," vol. 21, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

40 CREATe.org and PricewaterhouseCoopers, "Economic Impact of Trade Secret Theft."

FIGURE 2 Global proportion of illicit software use by region



Totaling It All Up

In summary, we estimate that the total low-end value of the annual cost of IP theft in three major categories exceeds $225 billion, or 1.25% of the U.S. economy, and may be as high as $600 billion, based on the following components:

- The estimated low-end value of counterfeit and pirated tangible goods imported and exported, based on a conservative estimate that 20% of the cost of these goods detracts from legitimate sales, is $29 billion. The high-end estimate for counterfeit and pirated tangible goods imported and exported is $41 billion.
- The estimated value of pirated U.S. software is $18 billion.
- The estimated low-end cost of trade secret theft to U.S. firms is $180 billion, or 1% of U.S. GDP. The high-end estimate is $540 billion, amounting to 3% of GDP.

We have thus found no evidence that the Office of the Director of National Intelligence's estimate of $400 billion is incorrect.[41] Again, these are only the direct costs of IP theft that can

[41] Strohm, "No Sign China Has Stopped Hacking U.S. Companies, Official Says."

be roughly estimated. The indirect costs to the U.S. economy, such as the loss of competitiveness and devaluation of trademarks, are more difficult to measure, but we conclude that they are no less substantial. It is also important to note that these figures do not account for the economic cost of patent infringement.

Innovation is the United States' greatest competitive advantage.[42] The massive theft of American IP undermines that advantage, making the United States less competitive over the long term. Further, IP-intensive jobs have a greater multiplier effect on employment than do other types of jobs. For every high-tech job created in the United States, five jobs are also created indirectly in a local economy.[43] China does not just steal the most American IP of any country; it targets the sectors at the forefront of innovation that could create the best jobs for Americans in the 21st century. Firms in nascent industries such as biotechnology and next-generation IT that have the greatest potential to drive future growth in the U.S. economy are unfortunately under the greatest threat.

The Intellectual Property Rights Climate Abroad

Every year, the USTR reviews the development in IPR protection abroad and establishes watch lists. In 2016 the USTR reviewed 73 trading partners for its Special 301 Report and listed 34 countries on its Priority Watch List or Watch List. Only Ecuador and Pakistan moved off the Priority Watch List.[44] These watch lists are important for the U.S. government to identify the most salient issues of IPR protection among U.S. trade partners. The Special 301 Report is not all negative; it also identifies best IPR practices by trading partners and other positive developments abroad. The 2016 report recognized China specifically for overhauling its IPR laws and regulations and for signing an expanded memorandum of understanding with the National Intellectual Property Rights Coordination Center of the Department of Homeland Security.[45]

In addition to the watch lists, the USTR announced that it would conduct four out-of-cycle reviews in 2016 to encourage foreign nations to make continued progress on IPR issues. Specifically, the reviews would examine and make recommendations for Colombia, Pakistan, Spain, and Tajikistan. The out-of-cycle reviews were not available from the USTR website at the time of writing.

The Special Case of China

As previously mentioned, China (including Hong Kong) is the source of 87% of counterfeit physical goods entering the United States. It is not surprising, then, that in the "2016 China Business Climate Survey Report" the American Chamber of Commerce in the People's Republic of China lists IP infringement as a concern regarding doing business in China, with 23% of respondents listing it as a top challenge.[46] This evidence is corroborated by the U.S.-China Business Council, which found that IPR enforcement was the eighth-highest concern of U.S. companies it surveyed—an improvement over the previous year. Of note, the top concerns for U.S. companies in the Business

---

42 Derek Scissors, "Fixing U.S.-China Trade and Investment," American Enterprise Institute, April 13, 2016, https://www.aei.org/publication/fixing-us-china-trade-and-investment.

43 Enrico Moretti, *The New Geography of Jobs* (Boston: First Mariner Books, 2013).

44 USTR, "2016 Special 301 Report," April 2016, https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.

45 Ibid.

46 American Chamber of Commerce in the People's Republic of China, "2016 China Business Climate Survey Report," 2016, http://www.amchamchina.org/policy-advocacy/business-climate-survey.

Climate Survey are issues relevant to this report—inconsistent interpretation of regulations and unclear laws—which is a sign that China's regulatory regime is developing in uneven ways.[47]

The Chinese government recognizes that it must reform its regulatory environment to support the development of an IP-intensive economy that produces its own high-value products and to become not just a "large IP country" but also a "strong IP country."[48] The Chinese government has made strengthening its IPR regime a goal since it enacted a series of laws in the 1970s. It signed on to the Agreement on Trade-Related Aspects of Intellectual Property Rights in the 1990s and ultimately joined the World Trade Organization (WTO) in 2001.[49] Yet China has only had IP courts since 2014 and is still reforming its laws and regulations.

To realize those reforms, China's State Council issued a new action plan in 2016. Building on a 2015 policy document outlining goals to develop a stricter IPR regime, the action plan, titled "Opinion of the State Council on Accelerating the Construction of Intellectual Property Powers for China as an Intellectual Property Strong Country under the New Situation—Division of Tasks," duplicates standing policy but also lists several priorities for reform of the IPR regime.[50] According to analysis by Mark Cohen, a long-standing expert on China's IP environment, the document suggests that China is making a greater effort to raise the damages a victim can sue for in Chinese courts.[51] The action plan also stresses international cooperation and the placement of more IP officials overseas to protect Chinese companies. It goes on to encourage the study of China's IP-intensive industries and the use of fiscal policy to promote their development.[52] Taken as a whole, the plan appears to be more geared toward fostering stronger IP-intensive industries at home than developing the rule of law.

In both its Report to Congress on China's WTO Compliance and the Special 301 Report, the USTR identifies problems with trade secret theft, software piracy, and counterfeit physical goods.[53] The "2016 Special 301 Report" outlines several deficiencies in China's IPR regime that go uncorrected in the most recent action plan:

> Progress toward effective protection and enforcement of IPR in China is undermined by unchecked trade secret theft, market access obstacles to ICT [information and communications technology] products raised in the name of security, measures favoring domestically owned intellectual property in the name of promoting innovation in China, rampant piracy and counterfeiting in China's massive online and physical markets, extensive use of unlicensed software, and the supply of counterfeit goods to foreign markets. Additional challenges arise in the form of obstacles that restrict foreign firms' ability to fully participate in standards setting, the unnecessary introduction of inapposite competition concepts into intellectual property laws, and acute challenges in protecting and incentivizing the creation of pharmaceutical inventions and test data. As a result, surveys continue to show that the uncertain intellectual property environment

47 U.S.-China Business Council, "USCBC 2016 Membership Survey: The Business Environment in China—Key Findings," 2016, https://www.uschina.org/sites/default/files/USCBC%202016%20Annual%20Member%20Survey%20%28ENG%29_1.pdf.

48 "New State Council Decision on Intellectual Property Strategy for China as a Strong IP Country," China IPR, July 24, 2016, https://chinaipr.com/2016/07/24/new-state-council-decision-on-intellectual-property-strategy-for-china-as-a-strong-ip-country.

49 Mingde Li, "Current IP Issues in China and the Multilateral Trading System," Chinese Academy of Social Sciences, February 26, 2015, https://www.wto.org/english/tratop_e/trips_e/Li_Mengde.pdf.

50 "New State Council Decision on Intellectual Property Strategy for China as a Strong IP Country."

51 Ibid.

52 Ibid.

53 USTR, "2015 Report to Congress on China WTO Compliance," December 2015, https://ustr.gov/sites/default/files/2015-Report-to-Congress-China-WTO-Compliance.pdf.

> is a leading concern for businesses operating in China, as intellectual property infringements are difficult to prevent and remediate.[54]

China also singles out high-tech sectors for special support in its five-year plans. In testimony to the U.S.-China Economic and Security Commission, Jen Weedon, formerly of the cybersecurity firm FireEye, asserted that while all sectors are potential targets of Chinese cyberespionage, firms in strategic industries identified in the 12th Five-Year Plan are targeted by a greater number of advanced hackers sponsored by the Chinese government.[55] One such targeted high-tech sector is the semiconductor industry. The Chinese government hopes that China can attain "world-class status" in semiconductor production by 2030.[56] It aims to do so through subsidizing domestic firms, and by what the President's Council of Advisors on Science and Technology calls "zero-sum tactics" that hurt the overall industry and global economy but help Chinese firms. These tactics include the overt and covert theft of IP, among others.[57]

Numerous examples help demonstrate the scope of the Chinese industrial policy of gaining access to foreign expertise in key sectors. For example, in the United Kingdom, the sensitive nuclear project at Hinkley Point proposed for co-development with China General Nuclear Power Company was delayed. It came to light that the Chinese firm was indicted (along with one of its senior employees, Allen Ho) for "conspiracy to unlawfully engage and participate in the production and development of special nuclear material outside the United States, without the required authorization from the U.S. Department of Energy."[58]

Perhaps the most recent case is China's development of the Micius satellite, considered the world's first quantum communications satellite, which China launched into orbit in 2016. Scientists at national laboratories and academic institutions around the world have been working on developing technology based on quantum mechanics to create a communications system that is considered to be completely secure from penetration. China is eager to develop this technology to protect its own communications from potential adversaries like the United States. However, perhaps ironically, China was able to develop quantum communications technology ahead of its rivals by incorporating their research findings. In an interview with the *Wall Street Journal*, Pan Jianwei, the physicist leading the project, was quoted saying, "We've taken all the good technology from labs around the world, absorbed it and brought it back."[59] This may be just an innocent quip about how scientists share their basic research findings with one another across borders. However, it has been demonstrated

---

54 USTR, "2016 Special 301 Report."

55 Jen Weedon, testimony before the U.S.-China Economic and Security Review Commission, Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China, Washington, D.C., June 15, 2015, http://www.uscc.gov/sites/default/files/Weedon%20Testimony.pdf.

56 "China's Global Semiconductor Raid," *Wall Street Journal*, January 12, 2017, http://www.wsj.com/articles/chinas-global-semiconductor-raid-1484266212.

57 President's Council of Advisors on Science and Technology, *Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors* (Washington, D.C., January 2017), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf. The other zero-sum tactics include forcing customers to buy domestic and forcing foreign companies to transfer technology for market access. A fourth zero-sum tactic, not mentioned in the report from the President's Council of Advisors on Science and Technology, is barring foreign firms from providing certain services in the Chinese market. For example, value-added telecommunications services cannot be provided by a foreign-owned entity. The best a foreign company can do is own 49% of an entity providing such services because the necessary license can only be granted to a majority-Chinese-owned entity. This means that online stores and cloud storage, among other services, have to be provided by the latter, forcing the foreign company to share the technology and profits with a Chinese partner.

58 "U.S. Nuclear Engineer, China General Nuclear Power Company and Energy Technology International Indicted in Nuclear Power Conspiracy against the United States," U.S. Department of Justice, April 14, 2016, https://www.justice.gov/opa/pr/us-nuclear-engineer-china-general-nuclear-power-company-and-energy-technology-international.

59 Josh Chin, "China's Latest Leap Forward Isn't Just Great—It's Quantum," *Wall Street Journal*, August 20, 2016, http://www.wsj.com/articles/chinas-latest-leap-forward-isnt-just-greatits-quantum-1471269555.

that the Chinese government systematically collects information and secrets from abroad to further its technology development goals, as illustrated by the cases discussed above.

Beyond security issues is the concern that Chinese firms are able to underbid competitors because of unfair business practices, such as a firm enjoying preferential funding arrangements as a state-owned enterprise or engaging in the theft of IP and resources, as the U.S. Department of Justice finds.[60] Not only do these business practices allow Chinese firms to outbid potential rivals; they help Chinese researchers in the state sector develop competitive technology faster than some of their international rivals.

Conclusion

The scourge of IP theft and cyberespionage likely continues to cost the U.S. economy hundreds of billions of dollars a year despite improved laws and regulations. The theft of American IP is not just the "greatest transfer of wealth in human history," as General Keith Alexander once put it; IP theft undercuts the primary competitive advantage of American business—the capacity for innovation. IP-intensive companies generate more jobs both directly and indirectly than firms in other sectors. The growth of the U.S. economy and the strength of the U.S. labor market depend on the ability of Americans to innovate and increase productivity. The scale and persistence of IP theft, often committed by advanced state-backed groups, erode the competitiveness of U.S. firms and threaten the U.S. economy.

Apart from the economic costs of IP theft are the political costs. Allowing persistent state-backed IP theft to continue represents the erosion of the norms between countries that buttress the international order. The United States has chosen to uphold these norms for generations and continues to uphold them when they are threatened in other domains. It should not give up on leading toward a code of conduct in the cyber domain or on addressing the issue of IP theft. Such leadership requires that the United States enforce its own laws.

The commissioners were discouraged by the Obama administration's inaction on IP theft and cyberespionage. Congress has implemented several of the recommendations from our 2013 report, namely Section 1637 of the 2015 NDAA and the Defense Trade Secrets Act of 2016. Although the president took steps to bring his emergency economic powers to bear on cyber-enabled IP theft, the Obama administration failed to bring any cases against the perpetrators of cybercrime or IP theft.

The U.S. government has the capability and resources to address this problem. President Donald Trump should make IP theft a core issue in the early months of his administration. It is perhaps the single best way to correct the problems in the Sino-U.S. relationship that he highlighted during his campaign. To that end, several of this Commission's recommendations (outlined in the appendix) remain ripe for implementation, and we hope that the new Congress and administration will examine them early in 2017. If the makeup of this Commission is any suggestion, there exists broad bipartisan support for addressing IP theft and safeguarding the competitive advantages of U.S. firms, entrepreneurs, and workers.

60 "U.S. Nuclear Engineer, China General Nuclear Power Company and Energy Technology International Indicted in Nuclear Power Conspiracy against the United States."

Adopted Recommendations

Short-term Solutions

- **Enforce strict supply-chain accountability for the U.S. government.**
    - According to the Government Accountability Office, the Department of Defense has made some improvements in its supply-chain management, although much work remains to be done.

Medium-term Solutions

- **Amend the Economic Espionage Act to provide a federal private right of action for trade secret theft.**
    - The Defend Trade Secrets Act of 2016 created private right of action for victims of trade secret theft in U.S. courts. The act also created protections for plaintiffs to conceal the nature of their trade secrets.
- **Strengthen U.S. diplomatic priorities in the protection of American IP.**
    - Additional IP attachés are posted abroad, including a dedicated IP attaché in Beijing.

Long-term Solutions

- **Build institutions in priority countries that contribute toward a rule-of-law environment in ways that protect IP.**
    - This long-term solution is arguably in progress. A key component of the Obama administration's Joint Strategic Plan on Intellectual Property Enforcement was building capacity internationally to contribute to a rule-of-law environment.

Recommendations for Cybersecurity

- **Implement prudent vulnerability-mitigation measures.**
    - This recommendation is being implemented through the Cybersecurity National Action Plan and through Executive Order 13691 establishing information-sharing and analysis organizations.

Recommendations Pending Action

Short-term Solutions

- **Designate the national security adviser as the principal policy coordinator on the protection of American IP to reflect the president's priority and to ensure interagency coordination on this issue.**
    - Not implemented. The U.S. intellectual property enforcement coordinator, within the Office of Management and Budget, is still the principal policy coordinator.

- **Provide statutory responsibility and authority to the secretary of commerce to serve as the principal official responsible for effectively administering the president's policies on IP protection.**
    - Not implemented.
- **Strengthen the International Trade Commission's 337 process to sequester goods containing stolen IP.**
    - Not implemented. However, Section 1637 of the 2015 NDAA allows the president to sanction individuals and organizations found to be involved in economic espionage.
- **Empower the secretary of the Treasury, on the recommendation of the secretary of commerce, to deny the use of the U.S. banking system to foreign companies that repeatedly use or benefit from the theft of American IP.**
    - Authority established but not exercised. The IEEPA allows the president to sanction individuals and organizations and to "prohibit any transaction in foreign exchange."
- **Increase Department of Justice and FBI resources to investigate and prosecute cases of trade secret theft, especially those enabled by cyber means.**
    - Partially implemented. Ad hoc evidence suggests that more resources have been dedicated, but progress on this recommendation is difficult to quantify.
- **Consider the degree of protection afforded to U.S. companies' IP a criterion for approving major foreign investments in the United States under the Committee on Foreign Investment in the U.S. (CFIUS) process.**
    - Not Implemented. No relevant new legislation has passed and no new executive orders have been implemented since 2008 that affect CFIUS.
- **Require the Securities and Exchange Commission to judge whether companies' use of stolen IP is a material condition that ought to be publicly reported.**
    - Not implemented.
- **Greatly expand the number of green cards available to foreign students who earn science, technology, engineering, and mathematics degrees in American universities and who have a job offer in their field upon graduation.**
    - Not implemented.

Medium-term Solutions

- **Make the Court of Appeals for the Federal Circuit the appellate court for all actions under the Economic Espionage Act.**
    - Not implemented.
- **Instruct the Federal Trade Commission to obtain meaningful sanctions against foreign companies using stolen IP.**
    - Not implemented.

Long-term Solutions

- **Develop a program that encourages technological innovation to improve the ability to detect counterfeit goods.**
  - Not implemented.
- **Ensure that top U.S. officials from all agencies push to move China beyond a policy of indigenous innovation toward becoming a self-innovating economy.**
  - Not implemented.
- **Develop IP "centers of excellence" on a regional basis within China and other priority countries.**
  - Not implemented.
- **Establish in the private nonprofit sector an assessment or rating system of levels of legal protection for IP, beginning in China but extending to other countries as well.**
  - Not implemented.

Recommendations for Cybersecurity

- **Support U.S. companies and technology that can both identify and recover IP stolen through cyber means.**
  - Not implemented.
- **On an ongoing basis, reconcile necessary changes in the law with a changing technical environment.**
  - Partially implemented on an ad hoc basis.

Dennis C. Blair is the Chairman of the Sasakawa Peace Foundation USA and the Co-Chair of the Commission on the Theft of American Intellectual Property. He is the former commander in chief of the U.S. Pacific Command and the former U.S. director of national intelligence. Prior to rejoining the government in 2009, Admiral Blair held the John M. Shalikashvili Chair in National Security Studies with the National Bureau of Asian Research and served as deputy director of the Project for National Security Reform. From 2003 to 2006, Admiral Blair was president and chief executive officer of the Institute for Defense Analyses, a federally funded research and development center based in Alexandria, Virginia, that supports the Department of Defense, the Department of Homeland Security, and the intelligence community. He also has been a director of two public companies, EDO and Tyco International. During his 34-year career with the U.S. Navy, he served on guided-missile destroyers in both the Atlantic and Pacific fleets and commanded the *Kitty Hawk* Battle Group. Ashore, Admiral Blair served as director of the Joint Staff and held budget and policy positions on the National Security Council and several major navy staffs. A graduate of the U.S. Naval Academy, Admiral Blair earned a master's degree in history and languages from Oxford University as a Rhodes Scholar and was a White House Fellow at the Department of Housing and Urban Development. He has been awarded four Defense Distinguished Service medals and three National Intelligence Distinguished Service medals and has received decorations from the governments of Japan, Thailand, South Korea, Australia, the Philippines, and Taiwan.

Jon M. Huntsman, Jr., is the former U.S. ambassador to China (2009–11), the former governor of Utah (2005–9), and the Co-Chair of the Commission on the Theft of American Intellectual Property. He is currently the Chairman of the Atlantic Council and Co-Chairman of No Labels. Governor Huntsman was appointed U.S. ambassador to China by President Barack Obama and confirmed by the Senate on August 7, 2009. As ambassador, he worked closely with U.S. business owners to facilitate commerce in the growing Asian market and advocated for the release of U.S. citizens wrongfully imprisoned. As governor of Utah, he cut waste and made government more efficient. As a result, the state held its AAA bond rating and earned national accolades for debt management. Utah also ranked number one in the United States in job creation and was named the best-managed state by the Pew Research Center. Prior to serving as governor, he was named U.S. ambassador to Singapore, becoming the youngest head of a U.S. diplomatic mission in a century. Governor Huntsman also served as U.S. trade ambassador under President George W. Bush, during which time he helped negotiate dozens of free trade agreements with Asian and African nations. Governor Huntsman holds a BA in international politics from the University of Pennsylvania.

Craig R. Barrett is a leading advocate for improving education in the United States and around the world. He is also a vocal spokesman for the value technology can provide in raising social and economic standards globally. Dr. Barrett joined Intel Corporation in 1974 and held the positions of vice president, senior vice president, and executive vice president from 1984 to 1990. In 1992, he was elected to Intel Corporation's Board of Directors and was promoted to chief operating officer in 1993. Dr. Barrett became Intel's fourth president in 1997, chief executive officer in 1998, and

chairman of the board in 2005, a post he held until May 2009. He has served on numerous other boards as well as on policy and government panels. Until June 2009, he was chairman of the United Nations Global Alliance for Information and Communication Technologies and Development, which works to bring computers and other technology to developing parts of the world. Dr. Barrett has also been an appointee of the president's Advisory Committee for Trade Policy and Negotiations and the American Health Information Community. He has co-chaired the Business Coalition for Student Achievement and the National Innovation Initiative Leadership Council, and has served as a member of the Board of Trustees for the U.S. Council for International Business and the Clinton Global Initiative Education Advisory Board. Dr. Barrett has been a member of the National Governors' Association Task Force on Innovation America, the National Infrastructure Advisory Council, and the Committee on Scientific Communication and National Security and has served on the Board of Directors of the U.S. Semiconductor Industry Association, the National Action Council for Minorities in Engineering, and TechNet. Dr. Barrett received BS, MS, and PhD degrees in materials science from Stanford University. After graduation, he joined the faculty of Stanford University in the Department of Materials Science and Engineering and remained there through 1974. He was a Fulbright Fellow at Danish Technical University in Denmark in 1972 and a NATO Postdoctoral Fellow at the National Physical Laboratory in England from 1964 to 1965.

Slade Gorton is a former U.S. senator (1981–87 and 1989–2001) and a member of the National Commission on Terrorist Attacks Upon the United States. Senator Gorton is currently a Counselor at the National Bureau of Asian Research. His years in the Senate saw him appointed to powerful committee posts, including Appropriations; Budget; Commerce, Science, and Transportation; and Energy and Natural Resources. He served as the chairman of the Interior Appropriations Subcommittee (1995–2001), the Commerce Subcommittees on Consumer Affairs (1995–99), and the Aviation Committee (1999–2000). He was also a member of the Republican leadership as counsel to the majority leader (1996–2000). Senator Gorton began his political career in 1958 as a Washington state representative, and he went on to serve as state House majority leader. In 1968, he was elected attorney general of Washington State, in which capacity he argued fourteen cases before the U.S. Supreme Court. In June 1980, Senator Gorton received the Wyman Award, the highest honor accorded by the National Association of Attorneys General. Senator Gorton also served on the president's Consumer Advisory Council (1975–77) and on the Washington State Criminal Justice Training Commission (1969–81). He was chairman of the Washington State Law & Justice Commission (1969–76) and served as an instructor in constitutional law to public administration graduate students at the University of Puget Sound. Senator Gorton received his BA from Dartmouth College and his JD from Columbia Law School.

William J. Lynn III is the Chief Executive Officer of both Leonardo North America and DRS Technologies, Inc. Prior to joining DRS in January 2012, he served as the 30th U.S. deputy secretary of defense (2009–11). As deputy secretary of defense, Mr. Lynn served under Secretaries Robert Gates and Leon Panetta, managing three million personnel and overseeing an annual budget of $700 billion. He also personally led the department's efforts in cybersecurity, space strategy, and energy policy. From 2002 to 2009, Mr. Lynn was senior vice president of government operations and strategy at the Raytheon Company. Previously, he served as undersecretary of defense (comptroller) from 1997 to 2001 and as director of program analysis and evaluation

in the Office of the Secretary of Defense from 1993 to 1997. Mr. Lynn also worked on the staff of Senator Ted Kennedy as his counsel for the Senate Armed Services Committee. He has been recognized for numerous professional and service contributions, including four Department of Defense medals for distinguished public service, the Joint Distinguished Civilian Service Award from the chairman of the Joint Chiefs of Staff, and awards from the U.S. Army, Navy, and Air Force. Mr. Lynn holds a law degree from Cornell Law School and a master's degree in public affairs from the Woodrow Wilson School of Public and International Affairs at Princeton University. He is also a graduate of Dartmouth College.

Deborah Wince-Smith is the President and CEO of the U.S. Council on Competitiveness. Founded in 1986, this unique business-labor-academia coalition of CEOs, university presidents, and labor union leaders puts forth actionable public policy solutions to make the United States more competitive in the global marketplace. In 2004, Ms. Wince-Smith spearheaded the groundbreaking National Innovation Initiative (NII). The NII shaped the bipartisan America COMPETES Act, created state and regional innovation initiatives, and brought a global focus to innovation. She has also led a bilateral dialogue between the United States and Brazil on competitiveness and innovation strategy, including leading the 2007 and 2010 U.S.-Brazil Innovation Summits. Ms. Wince-Smith serves as a director of several publicly and privately held companies, national and international organizations, and U.S. government advisory committees. She is also a Senate-confirmed member of the Oversight Board of the IRS. She chaired the secretary of commerce's Advisory Committee on Strengthening America's Communities and served on the secretary of state's Advisory Committee on International Economic Policy. During her seventeen-year tenure in the federal government, Ms. Wince-Smith held leading positions in the areas of science, technology policy, and international economic affairs. Most notably, she served as the nation's first Senate-confirmed assistant secretary of commerce for technology policy in the administration of President George H.W. Bush. Ms. Wince-Smith received a BA from Vassar College and was one of the first female students to enter King's College at the University of Cambridge, where she read for a master's degree in classical archaeology. In 2006, she received an honorary doctorate in humanities from Michigan State University.

Michael K. Young is the President of Texas A&M University. Also a tenured Professor of Law, he has a distinguished record as an academic leader with broad experience in public service and diplomacy. He previously served as president of the University of Washington, where he led the nation's top public university (second among all universities) in attracting federal research funding. Prior to his appointment at the University of Washington, he served as president and distinguished professor of law at the University of Utah. Under President Young's leadership, Utah raised its stature nationally and internationally. Before assuming the presidency at Utah, he was dean and Lobingier Professor of Comparative Law and Jurisprudence at the George Washington University Law School. He was also a professor at Columbia University for more than twenty years, and prior to joining the Columbia University faculty, he served as a law clerk to justice William H. Rehnquist of the U.S. Supreme Court. President Young has held numerous government positions, including deputy undersecretary for economic and agricultural affairs and ambassador for trade and environmental affairs in the Department of State during the presidency of George H.W. Bush. He also served as a member of the U.S. Commission on

International Religious Freedom from 1998 to 2005 and chaired the commission on two occasions. He has published extensively on a wide range of topics, including the Japanese legal system, dispute resolution, mergers and acquisitions, labor relations, the legal profession, comparative law, industrial policy, international trade law, the North American Free Trade Agreement, the General Agreement on Tariffs and Trade, international environmental law, and international human rights and freedom of religion. He is a member of the Council on Foreign Relations and a fellow of the American Bar Foundation. President Young received a BA from Brigham Young University and a JD from Harvard Law School, where he served as a note editor of the *Harvard Law Review*.

LIST OF COMMON ABBREVIATIONS

CBP – U.S. Customs and Border Patrol

CFIUS – Committee on Foreign Investment in the U.S.

EUIPO – European Union Intellectual Property Office

FISMA – Federal Information Security Modernization Act

IEEPA – International Emergency Economic Powers Act

IP – Intellectual Property

IPR – Intellectual Property Rights

NCCIC – National Cybersecurity and Communications Integrity Center

NDAA – National Defense Authorization Act

OECD – Organisation for Economic Co-operation and Development

PLA – People's Liberation Army

PRC – People's Republic of China

USTR – United States Trade Representative

WTO – World Trade Organization

THE IP COMMISSION

THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY

The Commission on the Theft of American Intellectual Property is an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics. The three purposes of the Commission are to:

1. Document and assess the causes, scale, and other major dimensions of international intellectual property theft as they affect the United States.
2. Document and assess the role of China in international intellectual property theft.
3. Propose appropriate U.S. policy responses that would mitigate ongoing and future damage and obtain greater enforcement of intellectual property rights by China and other infringers.

COMMISSIONERS

Dennis C. Blair
Co-chair

Jon M. Huntsman, Jr.
Co-chair

Craig R. Barrett

William J. Lynn III

Slade Gorton

Deborah Wince-Smith

Michael K. Young

Exhibit 4

INTELLECTUAL PROPERTY RIGHTS

Fiscal Year 2015 Seizure Statistics

Prepared by

U.S. Customs and Border Protection
Office of Trade

Homeland Security

INTELLECTUAL PROPERTY RIGHTS

Fiscal Year 2015 Seizure Statistics

Prepared by

U.S. Customs and Border Protection
Office of Trade

Homeland Security

Table of Contents

Disclaimer: The information contained in this report does not constitute the official trade statistics of the United States. The statistics, and the projections based upon those statistics, are not intended to be used for economic analysis, and are provided for the purpose of establishing U.S. Department of Homeland Security workload.

Executive Summary

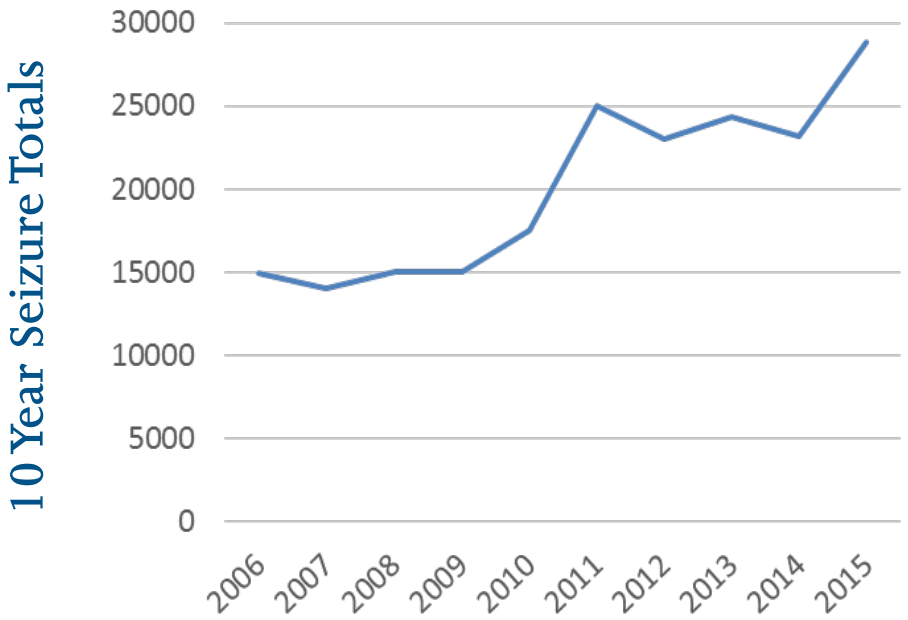
Products that infringe U.S. trademarks and copyrights or are subject to exclusion orders issued by the United States International Trade Commission threaten the health and safety of American consumers and pose risks to our economy and our national security. Continued enforcement of Intellectual Property Rights (IPR) by U.S. Customs and Border Protection (CBP), and U.S.Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) mitigates the financial and welfare risks posed by imports of such illicit products.

In Fiscal Year (FY) 2015, IPR seizures increased nearly 25 percent to 28,865 from 23,140 in FY 2014. The total estimated manufacturer's suggested retail price (MSRP) of the seized goods, had they been genuine, increased 10 percent to $1,352,495,341.

Tactical interagency collaboration with the National Intellectual Property Rights Coordination Center (IPR Center) resulted in 538 arrests, with 339 indictments, and 357 convictions.

Each year, more than 11 million maritime containers arrive at our seaports. At our land borders, another 10 million arrive by truck and 3 million arrive by rail. An additional quarter billion more cargo, postal, and express consignment packages arrive through air travel. Agencies within the Department of Homeland Security remain vigilant in targeting shipments posing risks to the American people.

Year in Review



In early FY 2015, CBP, in partnership with the Express Association of America and its members, established a new process which allows for the voluntary abandonment of detained goods. The pilot program for this new process, which was supported through a formal recommendation by CBP's federal advisory committee, the Commercial Customs Operations Advisory Committee (COAC), resulted in 2,857 voluntary abandonments and an estimated $2.2 million in interdiction cost savings to the government.

Year in Review

In FY 2015, CBP completed 152 exclusion order enforcement actions (shipments seized and shipments excluded), an increase from 53 in FY 2014.

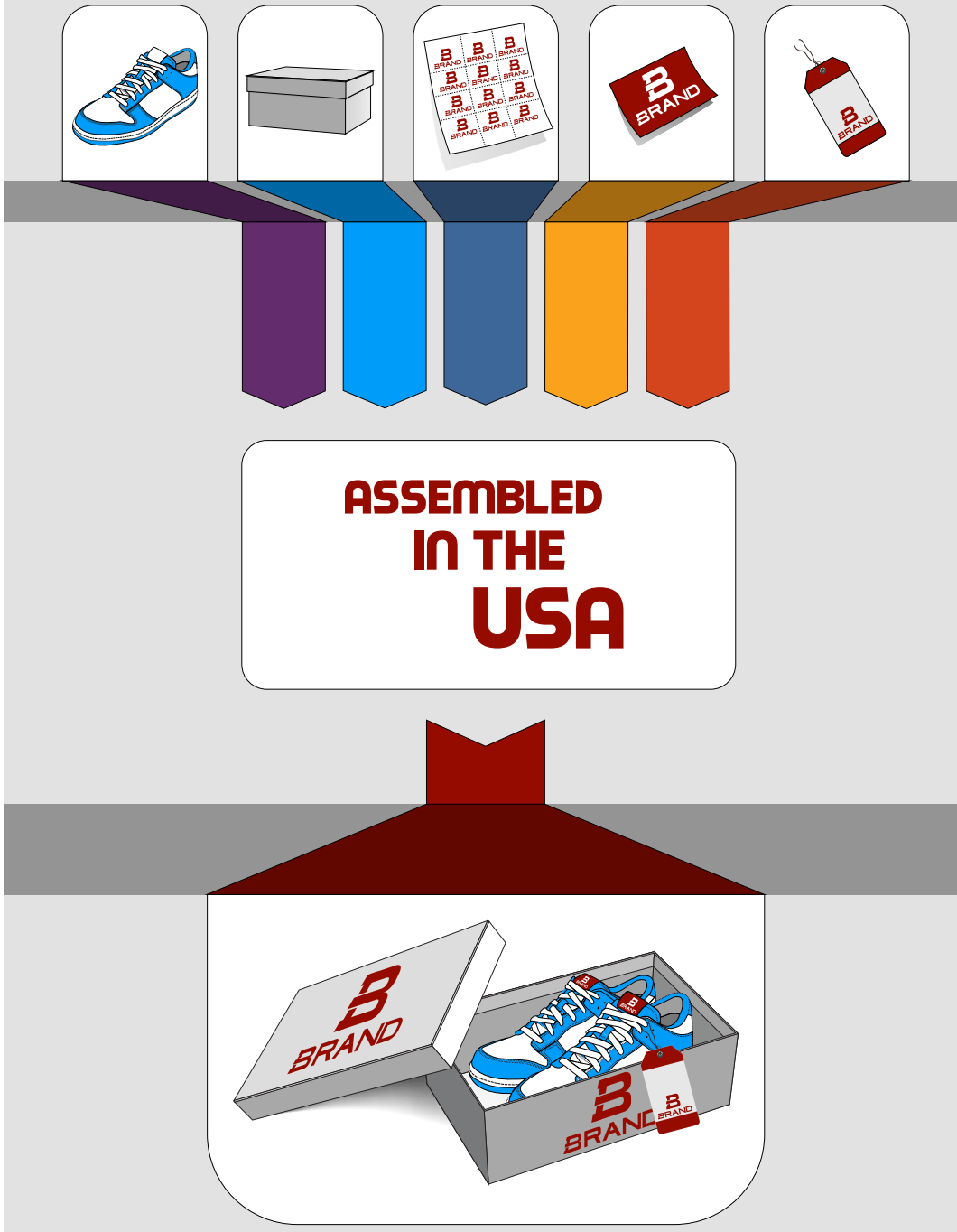
CBP seized 62 shipments of circumvention devices for violations of the Digital Millennium Copyright Act (DMCA), a 57 percent decrease from 144 such seizures in FY 2014.

The combined number of all IPR border enforcement actions in FY 2015 increased 37 percent over FY 2014.

In FY 2015, five Mobile Intellectual Property Enforcement Teams, groups of IPR experts deployed to assist with training and enforcement, conducted operations resulting in 1,349 IPR seizures of goods worth, had they been genuine, a combined estimated MSRP of over $22 million.

CBP seized 550 shipments containing labels and tags bearing counterfeit trademarks and/or pirated copies intended to be applied to articles after importation to create non-genuine products, which if genuine would be worth an estimated MSRP of $33,335,825. These included labels and tags sewn in fabric labels and patches, adhesive stickers and holograms, stamped metal parts including emblems, rivets, zippers, and paper hangtags. They are made for all types of apparel, handbags, shoes, electronics, software, and numerous other types of goods.

Counterfeit Label/Tag Import & Assembly



Year in Review

CBP concentrates its IPR border enforcement on federally registered trademarks and copyrights that have been "recorded" with CBP by owners using the Intellectual Property Rights e-Recordation (IPRR) system, which is available at https://iprr.cbp.gov/. CBP administers these "recordations" using a secure proprietary database that CBP can access to make IPR border enforcement determinations. Product ID manuals that are prepared by right holders are also linked to the database and used by CBP in making IPR border enforcement determinations.

At the close of FY 2015, CBP enforced trademarks and copyrights to over 17,000 active recordations, including 2,026 new recordations or renewals of expiring recordations.

CBP works closely with the rights holders in making IPR enforcement determinations. A public database of both active and inactive recordations is available using a search engine called the Intellectual Property Rights Search (IPRS) at **http://iprs.cbp.gov/index.asp**. Information on potential IPR infringements can be submitted to CBP using the e-Allegations Online Trade Violation Reporting System at **https://eallegations.cbp.gov/Home/Index2**.

In FY 2015, CBP in collaboration with ICE HSI utilized the IPR Strike Unit (ISU) ten times. ISUs are multi-discipline IPR enforcement teams that allow CBP to take enforcement action soon after infringing goods are identified at the ports.

Year in Review

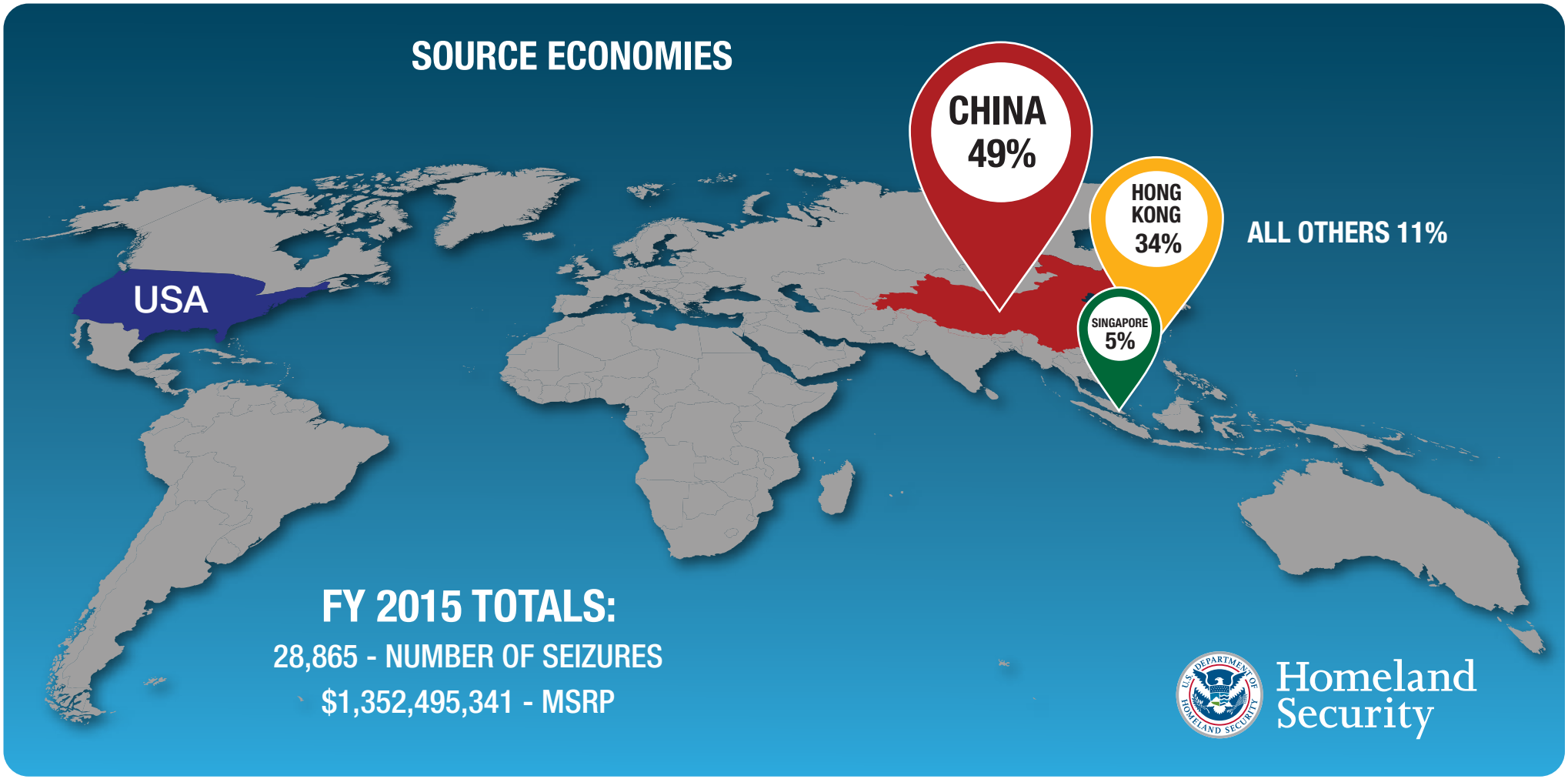
The ISU focuses on real time enforcement and informed compliance to build better cases against IPR violators and improve future compliance.

CBP and French Customs General Directorate jointly participated in Operation Bathe and Beaute, a bilateral IPR enforcement operation targeting counterfeit personal care products and electric personal devices. The joint operation, conducted from April 8, 2015, through May 4, 2015, resulted in seizures of 76 shipments of more than 31,000 counterfeit items with a total estimated MSRP of $541,000, had the goods been genuine.

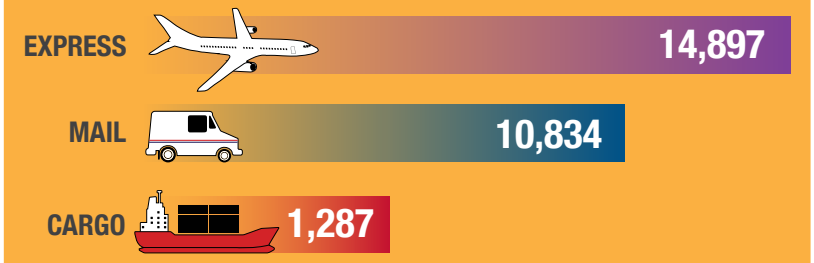
As a result of a collaborative enforcement effort between CBP's IPR Policy and Program Division, CBP's Pharmaceuticals, Health and Chemicals Center of Excellence and Expertise (CEE), ICE-HSI, other U.S. agencies and Zollkriminalamt (the German Customs Investigations Bureau), a Venezuelan man was sentenced to nearly two years of federal prison for his involvement in trafficking a high-volume of illicit pharmaceutical goods into the United States. After serving his term, he will be deported.

On August 12, 2015, in New Jersey, 175,000 watches, manufacturing stamps, and dye casts were seized. These goods infringed multiple trademarks and, had they been genuine, would have a total estimated MRSP of $100 million, an all time high seizure value.

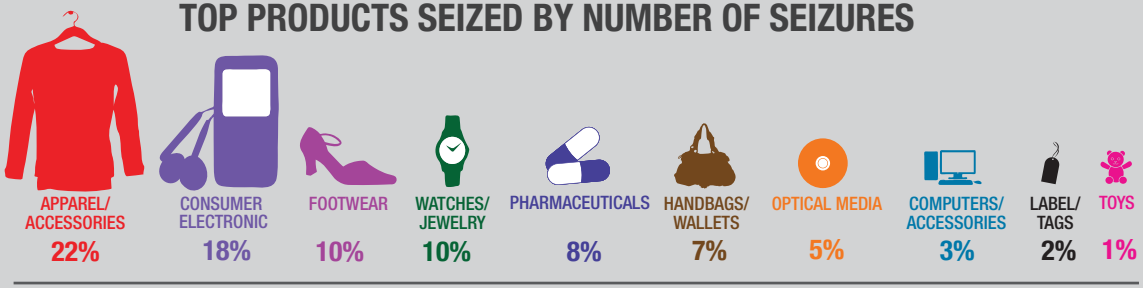
FISCAL YEAR 2015 IPR SEIZURE STATISTICS



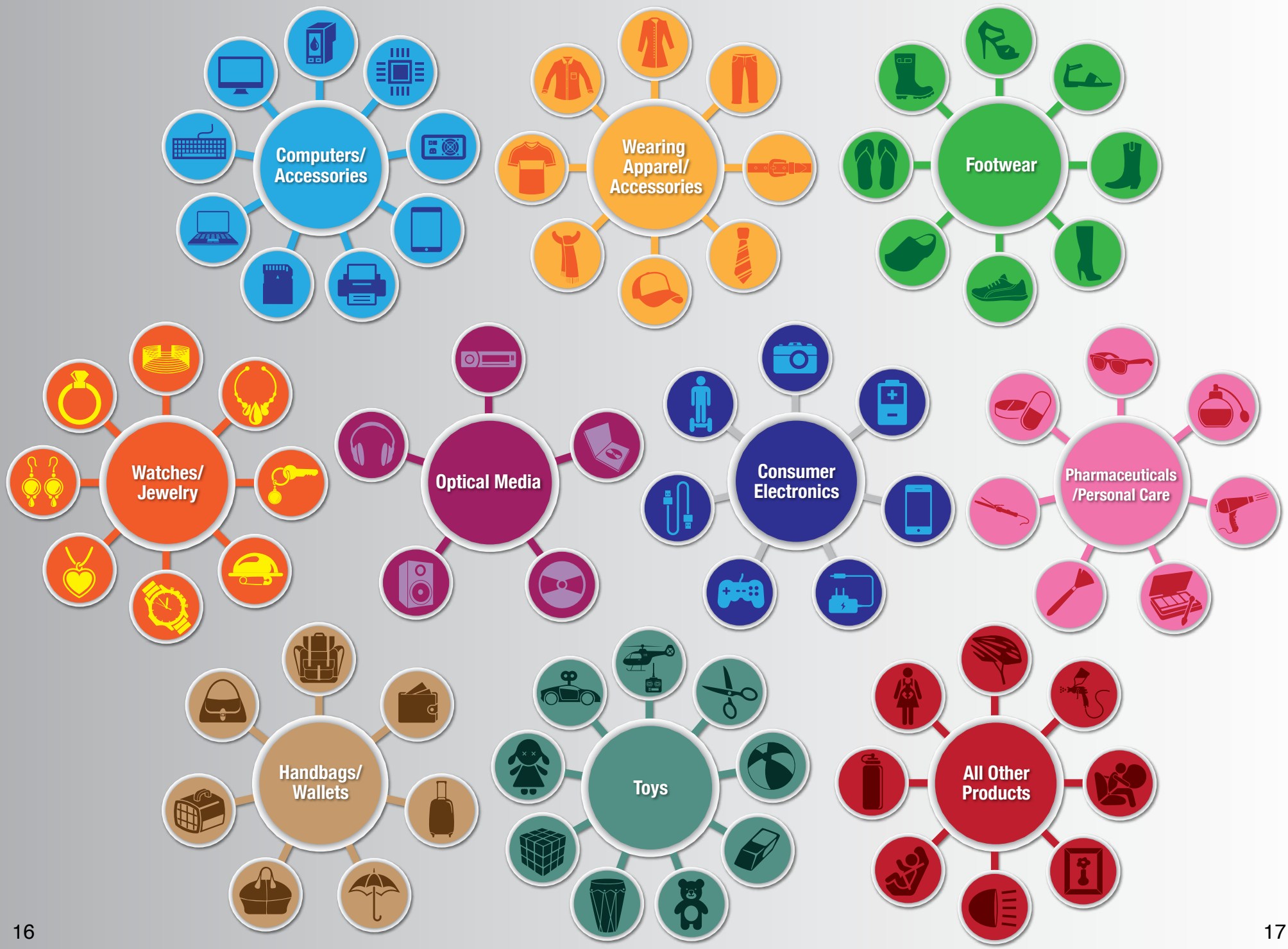
SHIPPING ENVIRONMENT BY NUMBER OF SEIZURES



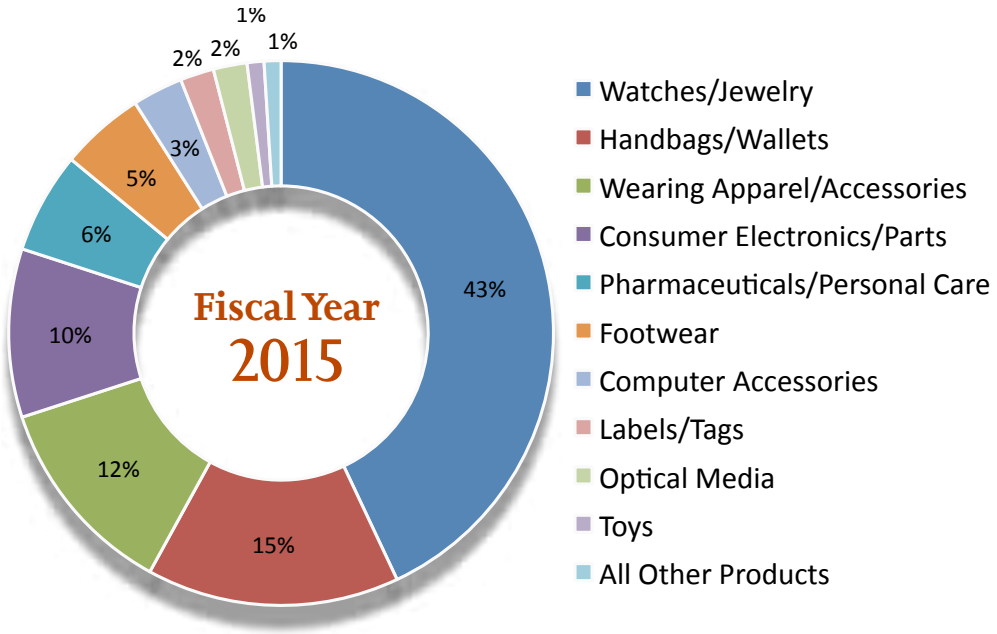
TOP PRODUCTS SEIZED BY NUMBER OF SEIZURES

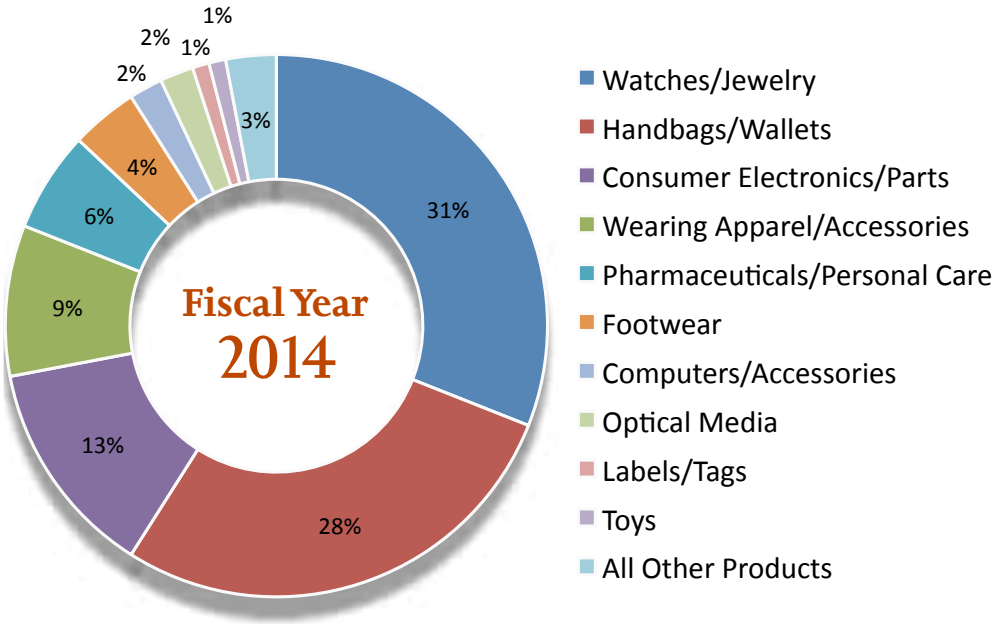


Product Categories



Products Seized by MSRP

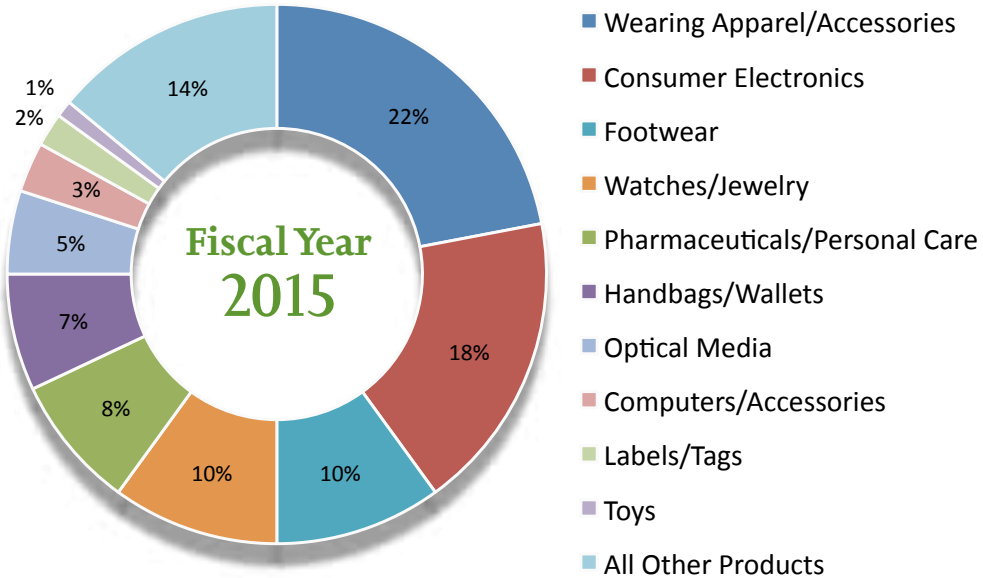


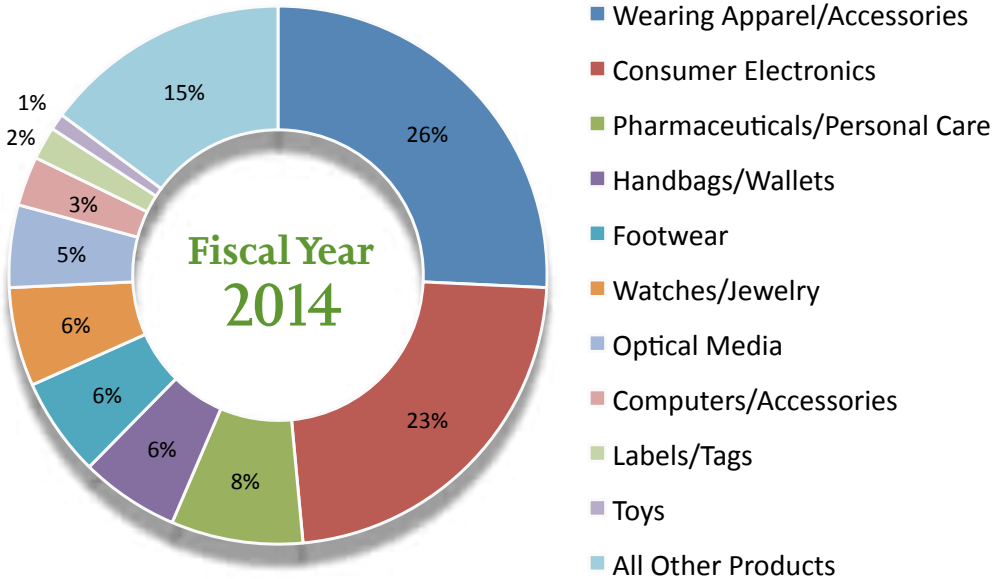


FY 2015 Products	Estimated MSRP	Percent of Total*
Watches/Jewelry	$580,791,647	43%
Handbags/Wallets	$208,378,624	15%
Wearing Apparel/Accessories	$157,196,110	12%
Consumer Electronics	$132,478,776	10%
Pharmaceuticals/Personal Care	$75,061,822	6%
Footwear	$64,967,315	5%
Computers/Accessories	$38,393,149	3%
Labels/Tags	$33,335,825	2%
Optical Media	$32,504,467	2%
Toys	$9,757,358	Less than 1%
All Other Products	$19,630,248	1%
Total FY 2015 Est. MSRP	**$ 1,352,495,341**	
Number of Seizures	**28,865**	

FY 2014 Products	Estimated MSRP	Percent of Total*
Watches/Jewelry	$375,397,333	31%
Handbags/Wallets	$342,031,595	28%
Consumer Electronics/Parts	$162,209,441	13%
Wearing Apparel/Accessories	$113,686,295	9%
Pharmaceuticals/Personal Care	$72,939,399	6%
Footwear	$49,522,859	4%
Computers/Accessories	$26,652,422	2%
Optical Media	$18,780,989	2%
Labels/Tags	$17,675,452	1%
Toys	$8,178,351	Less than 1%
All Other Products	$39,273,404	3%
Total FY 2014 Est. MSRP	**$1,226,347,540**	
Number of Seizures	**23,140**	

Number of Seizures by Product



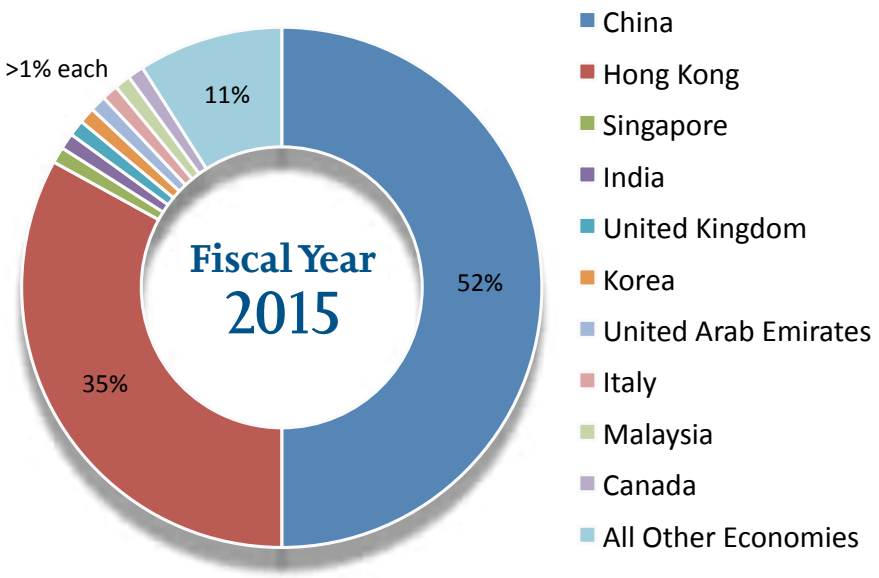


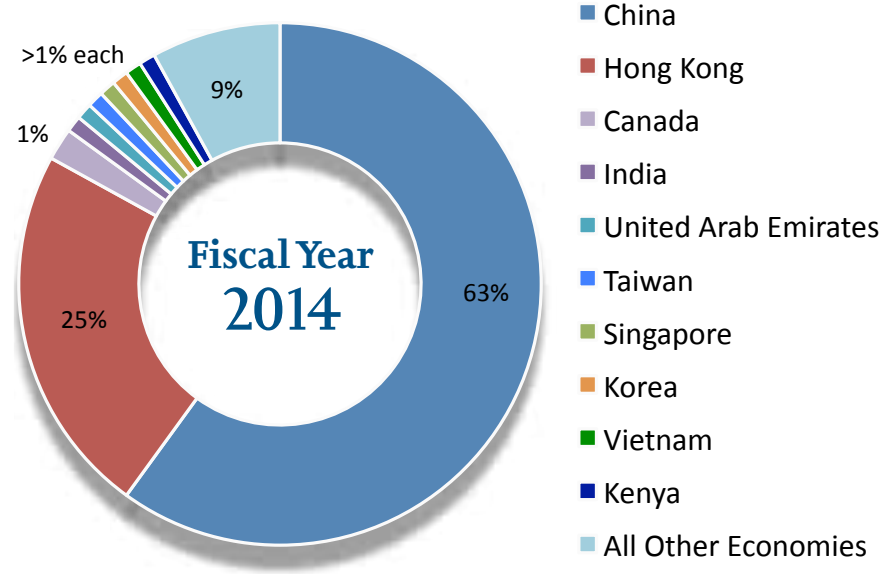
FY 2015 Products	Number of Seizures	Percent of Total*
Wearing Apparel/Accessories	6,232	22%
Consumer Electronics	5,326	18%
Footwear	2,818	10%
Watches/Jewelry	2,754	10%
Pharmaceuticals/Personal Care	2,301	8%
Handbags/Wallets	2,149	7%
Optical Media	1,442	5%
Computers/Accessories	846	3%
Labels/Tags	550	2%
Toys	391	1%
All Other Products	4,056	14%
Number of Seizures	**28,865**	

FY 2014 Products	Number of Seizures	Percent of Total*
Wearing Apparel/Accessories	5,948	26%
Consumer Electronics/Parts	5,432	23%
Pharmaceuticals/Personal Care	1,841	8%
Watches/Jewelry	1,330	6%
Optical Media	1,322	6%
Footwear	1,276	5%
Handbags/Wallets	1,260	5%
Computers/Accessories	671	3%
Labels/Tags	451	2%
Toys	230	1%
All Other Products	3,379	15%
Number of Seizures	**23,140**	

*In an effort to streamline DHS reporting, shipments with multiple products are now categorized as All Other Products. Prior to FY 2015, seizures with more than one type of product were included in more than one category. The FY 2014 totals have been adjusted to reflect this change.

Total MSRP for Products Seized by Source Economy

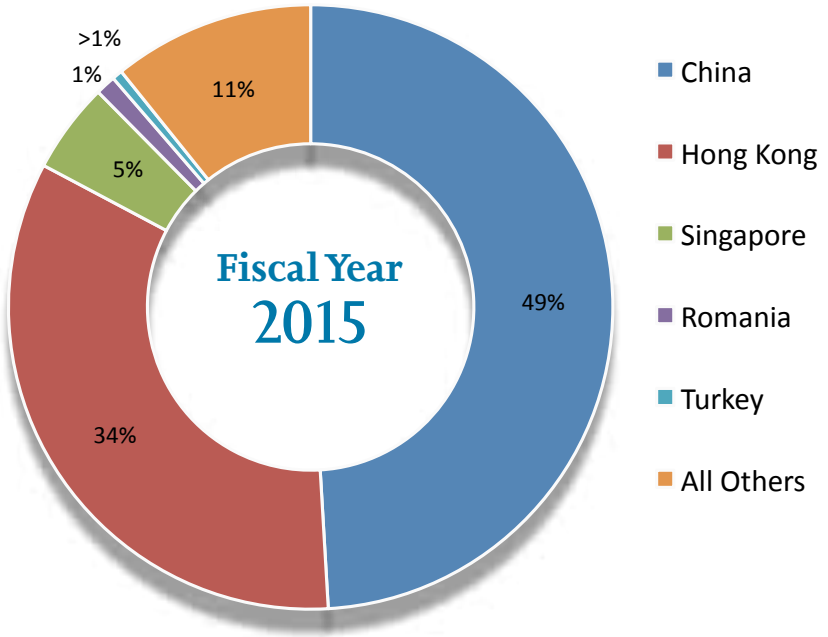


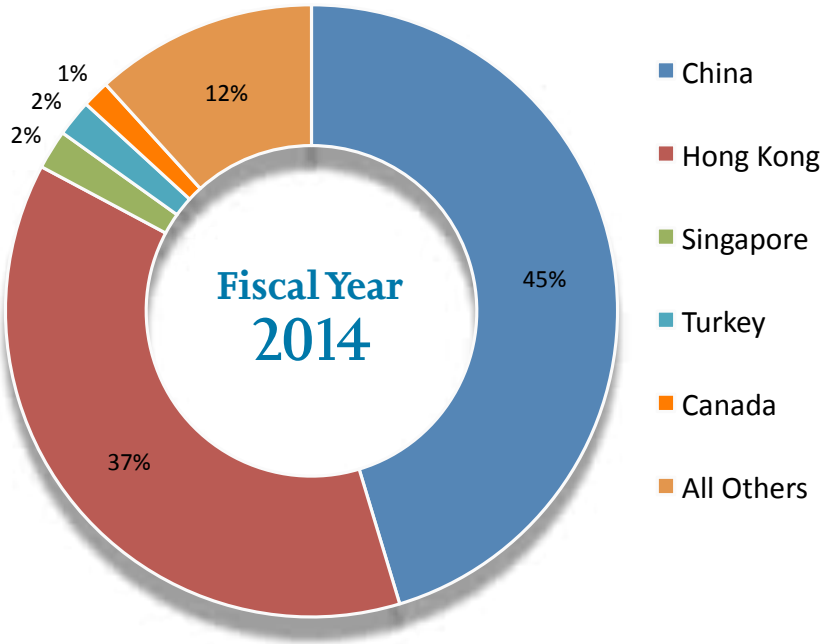


FY 2015 Trading Partner	Estimated MSRP	Percent of Total
China	$697,083,700	52%
Hong Kong	$472,331,251	35%
Singapore	$10,267,324	Less than 1%
India	$6,409,028	Less than 1%
United Kingdom	$4,358,128	Less than 1%
Korea	$3,788,572	Less than 1%
United Arab Emirates	$3,432,950	Less than 1%
Italy	$2,849,267	Less than 1%
Malaysia	$2,345,427	Less than 1%
Canada	$1,973,812	Less than 1%
All Others	$147,655,882	11%
Total FY 2015 Est. MSRP	**$1,352,495,341**	
Number of Seizures	**28,865**	

FY 2014 Trading Partner	Estimated MSRP	Percent of Total
China	$772,629,008	63%
Hong Kong	$310,437,365	25%
Canada	$12,460,242	1%
India	$5,540,652	Less than 1%
United Arab Emirates	$3,791,268	Less than 1%
Taiwan	$3,081,838	Less than 1%
Singapore	$2,538,079	Less than 1%
Korea	$2,514,596	Less than 1%
Vietnam	$2,422,050	Less than 1%
Kenya	$2,292,982	Less than 1%
All Others	$78,948,105	9%
Total FY 2014 Est. MSRP	**$1,226,347,540**	
Number of Seizures	**23,140**	

Seizures by Source Economy



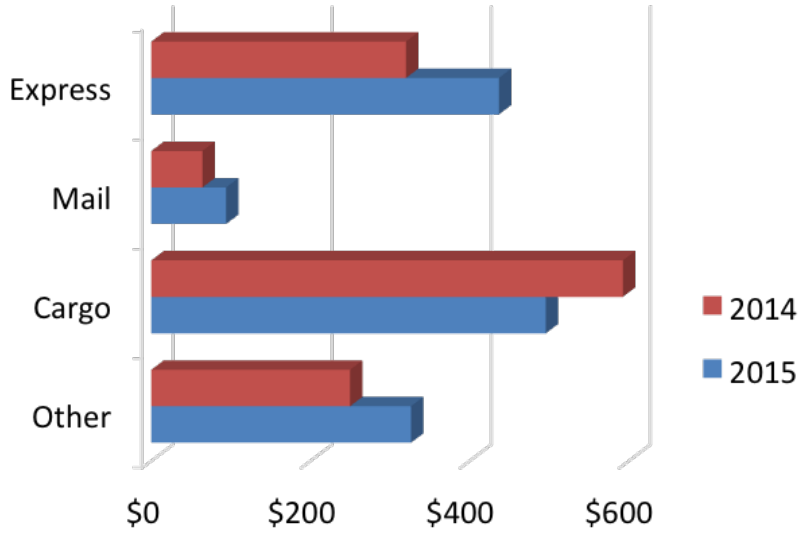


FY 2015 Trading Partner	Number of Seizures	Percent of Total
China	14,164	49%
Hong Kong	9,724	34%
Singapore	1,395	5%
Romania	310	1%
Turkey	160	1%
All Others	3,112	11%
Number of Seizures	**28,865**	

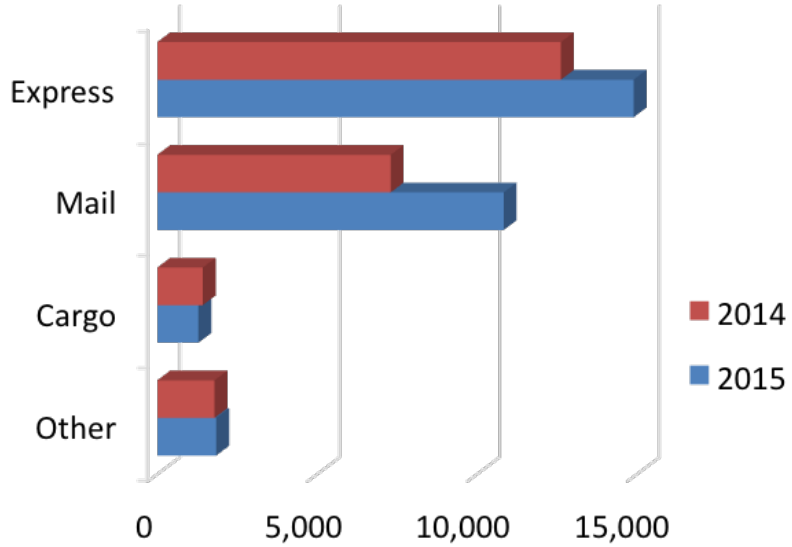
FY 2014 Trading Partner	Number of Seizures	Percent of Total
China	10493	45%
Hong Kong	8,667	37%
Singapore	481	2%
Turkey	447	2%
Canada	335	1%
All Others	2,717	12%
Number of Seizures	**23,140**	

Seizures by Shipping Environment

MSRP of IPR Seizures (in millions)



Number of IPR Seizures



Estimated Manufacturer's Suggested Retail Price (in millions)

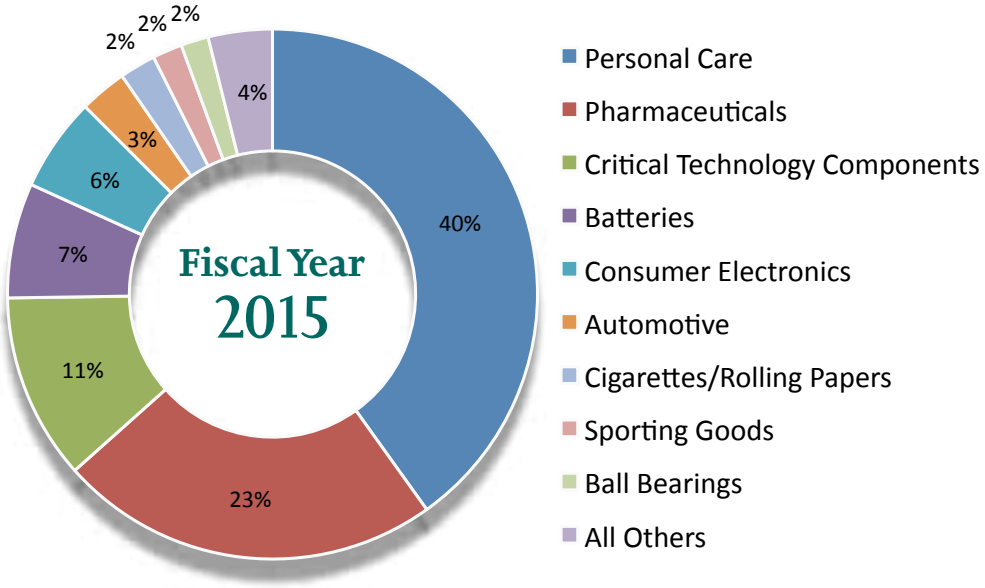
Mode	FY 2014	FY 2014 Percent of Total	FY 2015	FY 2015 Percent of Total	Difference	FY 2014 to FY 2015 Percentage Change
Express	$319.9	26%	$436.6	32%	$116.7	36%
Mail	$64.1	5%	$94.0	7%	$29.9	47%
Cargo	$592.6	49%	$495.6	37%	$(97.0)	-16%
Other	$249.7	20%	$326.3	24%	$76.6	31%
Total	$1,226.3		$1,352.5		$126.2	10%

Number of Seizures

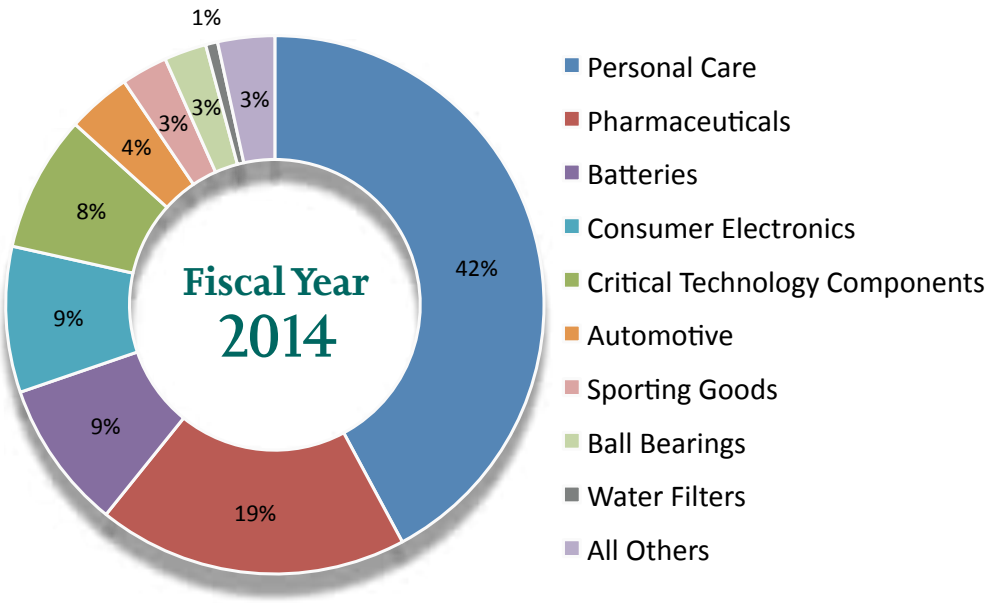
Mode	FY 2014	FY 2014 Percent of Total	FY 2015	FY 2015 Percent of Total	Difference	FY 2014 to FY 2015 Percentage Change
Express	12,623	55%	14,897	52%	2,274	18%
Mail	7,300	32%	10,834	38%	3,534	48%
Cargo	1,423	6%	1,287	4%	(136)	-10%
Other	1,794	8%	1,847	6%	53	3%
Total	23,140		28,865		5,725	25%

***Seizures included in the "Other" category involve exports, passenger baggage, or other enforcement actions.**

Health, Safety and Security



FY 2015 Products	Number of Seizures	Percent of Total
Personal Care	1,836	40%
Pharmaceuticals	1,066	23%
Critical Technology Components	520	11%
Batteries	321	7%
Consumer Electronics	262	6%
Automotive	132	3%
Cigarettes/Rolling Papers	101	2%
Sporting Goods	83	2%
Ball Bearings	77	2%
All Others	179	4%
Number of Seizures	**4,577**	



FY 2014 Products	Number of Seizures	Percent of Total
Personal Care	1,578	42%
Pharmaceuticals	698	19%
Batteries	335	9%
Consumer Electronics	328	9%
Critical Technology Components	307	8%
Automotive	144	4%
Sporting Goods	104	3%
Ball Bearings	95	3%
Water Filters	27	<1%
All Others	128	3%
Number of Seizures	**3,744**	

Exclusion Orders

CBP enforces exclusion orders issued by the United States International Trade Commission (USITC).

Most USITC exclusion orders are patent-based.

The USITC issues both limited and general exclusion orders. Limited exclusion orders apply only to infringing articles of named respondents. General exclusion orders bar the entry of infringing articles by all.

Exclusion orders prohibit the entry of all covered articles, even if they were not specifically accused and found to infringe at the USITC.

Once excluded, subsequent importations of the same articles by the same importer are subject to seizure.

Fiscal Year 2015

Shipments Seized	Shipments Excluded	Seizure Est. MSRP	Rulings* issued	Advice to ports
26	126	$8,741,932	16	46

Fiscal Year 2014

Shipments Seized	Shipments Excluded	Seizure Est. MSRP	Rulings* issued	Advice to ports
2	51	$33,725	9	10

*The term "rulings" covers rulings and other interpretive decisions.

IPR Points of Contact

Contact the IPR Help Desk to Report Violations and Obtain Assistance

CBP's IPR Help Desk is staffed Monday through Friday to answer questions on IPR enforcement. Contact the IPR Help Desk at (562) 980-3119 ext. 252, or via email at *iprhelpdesk@cbp.dhs.gov.*

Consult a CBP IPR Attorney

For those who have legal questions about CBP's IPR enforcement and would like to interface with a CBP IPR attorney, the IPR Branch is available to help. To request information on CBPs recordation program, please contact the IPR Branch at *iprrquestions@cbp.dhs.gov*. For general inquiries on IPR enforcement, please contact *hqiprbranch@cbp.dhs.gov*.

Obtain Guidance on CBP IPR Policy and Programs

The IPR Policy and Programs Division coordinates with rights holders, members of the trade community, CBP staff, other Federal agencies, and foreign governments in developing and implementing the agency's IPR strategy, policy and programs. To contact the IPR Policy and Programs Division, email *iprpolicyprograms@cbp.dhs.gov*.

National Intellectual Property Rights Coordination Center

To report violations of intellectual property rights, including counterfeiting and piracy, to the National IPR Coordination Center visit *https://www.iprcenter.gov/referral/* or telephone 1-866-IPR-2060.

Homeland Security

www.cbp.gov/ipr
www.iprcenter.gov
CBP Publication # 0570-0916

Exhibit 5

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Global Agenda

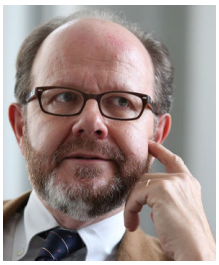
State of the Illicit Economy
Briefing Papers

October 2015

Contents

REF 290915

Foreword



Jean-Luc Vez
Managing Director, Head of Public Security Policy and Security Affairs
Member of the Management Committee, World Economic Forum

While the state of the global economy continues to fluctuate, its illegitimate counterpart, the illicit economy, has seen unprecedented growth. As such, it has etched its way into all aspects of society, and is cause for serious global concern. From healthcare to infrastructure to the arts, the illicit economy does not affect just one aspect of society, but all of them: business, government, civil society and individuals. It is a disruptor of social order to the greatest extent. A call to action must be made.

The illicit economy is formed from the proceeds of illicit trade which is, in turn, largely rooted in organized crime. Whether it is human trafficking, arms trafficking, the illegal wildlife trade, counterfeiting or money laundering, these activities are incredibly lucrative and fuel the magnitude of the illicit economy. Our Global Agenda Council on Illicit Trade 2012-2014 estimated the shadow economy to be worth $650 billion. More current research projects that the cost to the global economy of counterfeiting alone could reach USD 1.77 Trillion in 2015. With technological advancements and the international nature of trade in the world today, this value is expected to continue to rise.

Illicit trade operates on a vast scale and unprecedented pace, making it increasingly challenging to tackle. There are multiple initiatives and organizations, as well as public and private initiatives, dedicated to combating one or several aspects of illicit trade, but this is not a fight that can be won unilaterally. To achieve success, a global and multidisciplinary approach is needed in which the knowledge, expertise and experiences of various actors can be tapped into and shared.

As an international institute for public-private partnership, the World Economic Forum provides a neutral platform for parties to come together and discuss the issue of illicit trade. The aim is to foster structured dialogue between business, civil society and government so that common methods and solutions of tackling this trade can be found. Through multidisciplinary cooperation and joint action, results can be achieved. We can disrupt the proliferation of illicit trade, whether it is by simply raising awareness of the problem within affected communities, or by finding ways of detecting and preventing crimes that contribute to ruining the economy.

The World Economic Forum's Meta-Council on the Illicit Economy aims to take this principle of public-private cooperation forward. By engaging leading experts in the field, the Meta-Council will try to find viable multistakeholder solutions to limiting this criminal activity. This paper on the State of the Illicit Economy is the first step in the process. It sets out the parameters within which illicit trade operates, the contributing factors to illicit trade, the role that various societal sectors can play in the fight against it, and the types of solutions needed to combat it.

My thanks go to the members of the Meta-Council on the Illicit Economy for their cooperation and contributions, to Adam Blackwell for his leadership as chair of this Meta-Council, and to Karen Wong for her tireless coordination of these efforts as council manager. We hope this paper provides you with the valuable insight required to start a conversation to initiate change.

Introduction

Adam Blackwell, Ambassador in Residence at the William Perry Center for Hemispheric Defense and Security Studies, National Defense University, USA

The illicit economy is vast and hampers the growth of the global economy while also jeopardizing the stability of society and governance. With estimations of various illicit activities running into billions of US dollars, these figures rival the GDP of some G20 countries. This cannot be neglected - the illicit economy and its related activities must be addressed.

By producing this paper, we the Meta-Council on the Illicit Economy, seek to shed light on the importance of this topic and the necessity for multiple stakeholders to engage in the fight as each have a role to play. Curtailing the illicit economy requires a range of solutions from technology to public policy. By addressing these points, the Meta-Council hopes to shed light on these issues and highlight the action that can, and should be taken to reduce the rates at which the illicit economy operates.

Numerous initiatives, enterprises and programs dedicated to the fight against illicit trade exist. They take many shapes and forms and involve a variety of actors. With the broad expertise of our council members, we strive to foster collaboration on countering the illicit economy and raise awareness on possible solutions.

The proliferation of illicit activities shows no signs of slowing. It grows particularly in regions where there is lack of governance and social structure. Hence, in an era where several regions in the world are vulnerable and politically unstable, efforts to address these underlying issues must be made.

Special Acknowledgement on the *Deep Dive: Analysis and Recommendations for Controlling the Illicit Mining and Trading of Minerals*

This analysis and recommendations were prepared by Stephen D'Esposito and Herbert M'cleod on behalf of the Global Agenda Council on the Future of Mining and Metals. The Council drew on its membership and external experts. We would like to thank Bob Leet of Intel and Mike Loch, formerly of Motorola Solutions and currently a RESOLVE strategic partners, for their contributions as well as serving as reviewers. In addition to the members of Global Agenda Council on the Future of Mining and Metals (Huguette Labelle, Jamie de Bourbon, Antonio Pedro and Tsagann Puntsag) we would like to thank Eddie Rich of EITI, Tim Martin director of RESOLVE's Resource Diplomacy Initiative, Jennifer Peyser of RESOLVE, Lina Villa of the Alliance for Responsible Mining, Ian Smillie of DDI, Nick Cotts of Newmont, and Marcello Veiga of the University of British Colombia.

The State of the Illicit Economy

The global illicit trade has grown at an unprecedented pace, in both relative and absolute terms, ushering in immense risks to society, governance and the global economy. Much of the illicit trade is opportunistic and thrives on gaps in capacity and vulnerabilities in policy regimes across countries and regions.

The international normative regime which governs the prevention and mitigation of illicit trade is multifaceted and constantly evolving. The variety of actors involved in its implementation at the national, regional and international level is inherently multidisciplinary.

Criminal organizations have not only exploited gaps in capacity and policy, they have been ahead of the curve in their use of technology and sophisticated instruments and schemes. They have used the interconnectedness of trade, finance, communication and transport systems that have affected innovation and growth in the private sector. Indeed, the very forces that enable globalization and that underpin secure, private trans-national commerce are the same as those that also now make us less secure.

The international framework in this area includes the 2003 United Nations Convention against Transnational Organized Crime (UNTOC) and the 2005 United Nations Convention against Corruption (UNCAC). UNTOC offers states a framework for preventing and combating organized crime, and a platform for co-operating. UNCAC's far-reaching approach and the mandatory character of many of its provisions make it a unique tool for developing a comprehensive response to a global problem. The 13th United Nations Congress on Crime Prevention and Criminal Justice, held in Doha, Qatar, in April 2015, adopted the Doha Declaration. This highlighted the way a lack of effective social crime-prevention policies and ineffective criminal justice systems allow crime, terrorism, and violence to hamper social and economic development.

The need to tackle illicit trade has never been more urgent

The cost of illicit trade to the global economy is considerable, if difficult to state with absolute precision. Counterfeiting and piracy alone will cost the global economy an estimated $1.77 trillion in 2015[1], which is nearly 10% of the global trade in merchandise.[2]

The benefits of tackling illicit trade are as compelling for governments and citizens as they are for businesses. Eliminating the illicit trade in tobacco alone could generate annual revenues of up to $31 billion for governments, according to the World Health Organization.[3]

The cost of illicit trade to human life is even more striking. Sub-standard malaria medicines led to the deaths of over 120,000 children in sub-Saharan countries in 2013 alone,[4] while globally, an estimated 700,000 people die each year because of counterfeit malaria and tuberculosis medicines. Counterfeit rates across all sectors have historically run as high as 40% and even today are estimated at 17%.[5,6]

Human trafficking and smuggling are currently front-page news in Europe, but let us not forget that globally, nearly 21 million people are victims of forced labour, generating illegal profits of at least $150 billion.[7] This labour force is larger than the entire working population in countries such as Canada and Poland.[8]

Criminal and terrorist networks profit immensely from illicit trade

ISIS is reported to be the world's richest terrorist organization,[9] funding itself not only through the illicit trade in oil but also through the sale of "blood antiquities".[10]

The illegal trade in wildlife and natural resources is worth up to $213 billion a year[11], - a sum that surpasses the $135 billion in official development assistance given globally in 2014[12] - and is funding global terror groups and militias.[13] But even these figures understate the total value of the proceeds of crime, estimated in 2009 by the United Nations Office on Drugs & Crime to be at 3.6% of global GDP, or $2.1 trillion.[14] This figure significantly exceeds the 2014 figure for combined global military expenditure, of $1.8 trillion.

INTERPOL recently formed a dedicated "Illicit Markets" sub-crime directorate to provide the world's law-enforcement agencies with access to expertise in this area, with particular focus on pharmaceutical crime, environmental crime, counterfeits and smuggled goods, as well as stolen vehicles and works of art.

Implications for the agenda for combating illicit trade

I. Assessing the magnitude of illicit trade

The scale of illicit trade, because of its secret and illegal nature, is difficult to accurately quantify. But even if precise assessments are elusive, it is nonetheless important to understand the orders of magnitude in order to broadly assess impact and to improve the effectiveness and targeting of policy.

The World Economic Forum's Global Agenda Council on Illicit Trade 2012-2014 is often cited[15] as the source that estimates the value of the "shadow economy" at $650 billion, a figure that rises to $2 trillion when money laundering is included.[16]

The $650 billion figure is drawn from Global Financial Integrity's 2011 study, which assessed 12 types of illicit trade to arrive at the aggregate figure. As the table below illustrates, the data on which these figures were based is clearly outdated. Moreover, the scope of these measures is rather limited. The OECD figures on counterfeiting, for instance, only capture the value of cross-border trade, excluding the significant counterfeit trade within countries such as China. They also measure the trade in tangible goods, but exclude the illicit trade in digital products and online services.

Illicit activities (total $650 billion)	2011 figures	Sources used by GFI for 2011 study	Years out-dated
Drug trafficking	$320.0 billion	2005 UNODC World Drug Report[17]	10 years
Counterfeiting (tangible)	$250.0 billion	2009 OECD Report[18]	6 years
Human trafficking	$31.6 billion	2005 ILO Report[19]	10 years
Illicit oil trade	$10.8 billion	2005 Raymond Baker[20]	10 years
Illicit wildlife trade	$10.0 billion	2009 Coalition Against Wildlife Trafficking[21]	6 years
Fish	$9.5 billion	2010 High Seas Task Force Report[22]	5 years
Timber	$7.0 billion	2009 Seneca Creek report[23]	6 years
Art & cultural property	$6.3 billion	2010 UN Crime Prevention & Criminal Justice[24]	5 years
Gold (3 countries only)	$2.3 billion	DRC (2010)[25], S. Africa (2008)[26], Peru (2010)[27]	5-7 years
Human organs	$1.2 billion	2009 for kidney[28], 2007 estimate for liver	6-8 years
Small arms/light weapons	$1.0 billion	2002 Small Arms Survey estimate [29]	13 years
Diamonds	$0.9 billion	2009 Kimberley Process Statistics[30]	6 years

II. Emphasizing the role of business in the fight against illicit trade

Illicit trade is becoming increasingly sophisticated, not only in the quality of production and the speed of distribution that can be achieved, but also in criminals' ability to use social networks, online marketplaces, global production chains and the international financial system. Recent developments have raised questions about the extent of responsibility of business for illicit activities conducted either within their platform and operations or within the global production chain. These include:

- ***Traditional banks***: Chinese state-owned banks have been named as "conduits"[31] for counterfeiters, while big US banks such as Bank of America, JP Morgan Chase and Wells Fargo have been cited as "financial conduits"[32] for the human smuggling industry.

- ***Online marketplaces***: INTERPOL has been coordinating operations with its member states against the online sale of illicit medicines. The result has been the closure of thousands of bogus websites and the seizure of millions of fake medicines. However, online marketplace Alibaba faces pressure from the Chinese government[33] as well as brand owners like Kering[34] to fight the sale of counterfeit goods on its e-commerce platform, and Etsy is facing an investor class-action suit amid allegations it has as many as 2 million items for sale that could be counterfeit or in violation of trademark laws.[35] Iran, meanwhile, is suspected by sanctions officials to have used online marketplaces to build up its nuclear programme.[36] It has been reported that "virtually every dual-use item needed for a proliferator to produce nuclear weapons is advertised for sale on Alibaba".[37]

- ***Online advertising***: Google has agreed to pay $250 million to settle a shareholder lawsuit over years-old charges that it knowingly accepted advertisements from illegal online pharmacies[38], while an Internet safety group has accused YouTube[39] of failing to block videos selling stolen credit card data and profiting from legitimate advertisements running beside them. An International Fund for Animal Welfare study into the online trade in endangered animals and animal parts reported finding more than 33,000 animals or parts for sale in more than 9,000 online ads in 280 online marketplaces[40], including Craiglist.[41]

- ***Social networks***: People smugglers in North Africa are using Facebook and other social networks to recruit migrants from across the Middle East and Africa.[42]

- ***Electronics producers***: The US Securities and Exchange Commission estimates that 6,000 manufacturers and 480,000 suppliers were potentially affected by the 2010 Dodd-Frank Act rules on conflict minerals, but only 1,292 companies filed reports in response.[43]

Risk, Response, Innovation: Human Trafficking and the Private Sector

Approximately 21 million men, women, and children are falling prey to human traffickers, according to the International Labour Organization.[69] The ILO further estimates that 68% of these people are victims of labour exploitation, a further 22% are sexually exploited, with the remainder forced to work in prisons or in work imposed by military or rebel forces.[70] With growing profits to be made from trafficking and a low risk of criminal punishment, the indications are that the number of people being trafficked will grow, as criminal groups shift from other forms of illegal trade to human trafficking.[71]

Exploitation of human trafficking victims can take a variety of forms. One of those most often discussed is the sexual exploitation of women and girls. Human trafficking also occurs in the form of forced labour in numerous business sectors, including manufacturing, construction, shrimp harvesting and processing, agriculture, and electronics. In a recent study, the global NGO Verité concluded that 28% of workers in the Malaysian electronics sector were victims of exploitation.[72] In another recent study, Verité also identified and assessed risk factors in global supply chains, including socio-economic, environmental, policy, and political, which create a complex web of vulnerability for workers and industries.

Counting the cost – why the private sector should be concerned

The human costs, as well as the economic, resource, litigation, and brand and reputation costs of human trafficking, make this something that the private sector needs to address. Traffickers utilize companies to further their exploitation, whether through online recruitment, transport, wire transfers via private financial institutions or hotels and motels as transit sites. Failure to address human trafficking can result in a business inadvertently contributing to a growing illicit economy, as well as risking litigation and a backlash from consumers. Through efforts like the World Economic Forum's Network of Global Agenda Councils Task Force on Human Trafficking and the Meta Council on the Illicit Economy, initiatives are being created to bring issues such as human trafficking to the forefront. In December 2014, the World Economic Forum published *Hedging Risk by Combating Human Trafficking: Insights from the Private Sector*, a report that resulted from a year-long collaboration of the members involved in the Network of Global Agenda Councils Task Force on Human Trafficking. This report included survey-based research in four sectors: financial services, technology, transport, and hospitality and tourism. It concluded with the following analysis and recommendations on the most promising private sector anti-trafficking initiatives and next steps:

1) **Technology and data analysis tools** can be used to identify potential traffickers and track transactions.
2) **Research and collaborative efforts** should be made to promote cross-stakeholder collaboration and public-private partnership, particularly on information sharing and knowledge transfer.
3) **Engagement of senior corporate leaders** can create systemic change throughout a company.
4) **Individuals and employees** can make a difference through raising awareness, and preventing and flagging possible cases of human trafficking.
5) **Best-practice sharing across industries could** foster dialogue and a culture of transparency.
6) **Academic institutions**, particularly business and public-policy schools, have a role to play in training the next generation of business and community leaders in anti-trafficking strategies and entrepreneurial solutions.

The World Economic Forum will be continuing its efforts to build upon this first report and look at innovative private sector approaches to this global human rights abuse. It is critical to work in partnership with business and the licit economy to elevate human freedom on a worldwide scale.

III. Mapping governance gaps and best practice

In tackling illicit trade, governments are constrained not only by the resources needed to enforce the law but also by having to operate within their own national borders. Governments have a difficult time collaborating with other governments when their laws, policies, and interests vary. At the global level, there is room for better coordination among international organizations, several of which, such as INTERPOL and the World Customs Organization,[31] have limited budgets. It would be beneficial to all players to share innovative approaches and best practice, and to map gaps in governance.

Areas to consider include:

1. *International governance gaps*, which include:

– *Internet*: With an estimated 40,000 to 60,000 illegal sites selling drugs, law enforcers say the web administrator the Internet Corporation for Assigned Names and Numbers (ICANN) should do more to combat this trade; ICANN, however, says its powers are limited.[32]
– *Sea*: International laws prevent enforcement officers from boarding foreign vessels to investigate illegal fishing outside a nation's 200-mile exclusion zone. They can board a ship if they believe it is without nationality, but cannot prosecute over crimes alleged to have taken place beyond their jurisdiction.[33]

2. *Adherence to international protocols and agreements*

– *Illicit tobacco trade*: The World Health Organization's Framework Convention for Tobacco Control (FCTC) entered into force 10 years ago and has been ratified by 180 countries; although FCTC parties adopted a protocol on the illicit tobacco trade in 2012, only six countries have ratified it.[34] *Money laundering*: In the European Union (EU), central registers will be set up listing the beneficiary owners of companies and trusts[35]. Britain, France, Denmark and the Netherlands plan to demand full public disclosure of company beneficiary owners. The deal is awaiting formal sign-off by national governments.[36] These demands go beyond what was agreed by the leaders of the Group of 20 largest economies in November 2014. Meanwhile, the Financial Action Task Force,[37] the global standard-setting body to counter money-laundering and the funding of terrorism, has singled out the countries it says are failing to meet international standards.
– In March 2015, a 2012 Executive Order took effect in the US, requiring government contractors to make sure their supply chains did not include forced labourers.[38]

3. *False invoicing to evade tax must be recognized as part of illicit trade*

The mechanisms used to evade tax tend to be the same as those used to shift the proceeds of other illegal activity across international borders. Keeping records of company ownership, as described above, will help curtail both tax evasion and other aspects of illegal trade. Automatic exchange of tax information across borders is another important tool in combating tax evasion. Country-by-country reporting of financial results by multinational corporations, an issue being addressed by the EU, will also help curb tax evasion. The High Level Panel on Illicit Financial Flows from Africa has identified mis-invoicing for the purpose of commercial tax evasion as by far the major mechanism for shifting money out of the continent, a process which stifles economic prosperity and undermines national and regional security. The panel recommends that all African countries and, by implication, all developing countries, should publish real-time world market trade-pricing data, so that imports and exports can be checked for proper pricing, a move which would significantly reduce tax evasion and, therefore, limit the movement of money from other forms of illegal trade.

4. *Contrasting regulatory regimes and identifying effective practices*

It is illuminating to compare and contrast track-and-trace regulatory regimes across countries and industries.
– *Tobacco*: A comparative analysis of the interventions adopted by countries to control illicit tobacco trade yields not only insights into the array of technological applications and the evolution of policy, but also highlights effectiveness and success rates in different markets.[39]
– *Pharmaceuticals*: Markets such as China, India, South Korea, Brazil, the United States and Europe are in the process of adopting drug traceability regimes. A comparative study looking at the technical requirements in each country, and the pace and scope of implementation, could serve as a guide not only for other countries but also for multinational companies.

5. *Extrapolating stakeholder maps and overlaying alliances*

In addition to mapping the involvement of international organizations, private/business associations and key non-government organizations, it would be beneficial to expand stakeholder maps to reflect the role of non-traditional stakeholders and alliances. For example, on 2 December 2014, Pope Francis and 11 other religious leaders made a united call for an end to slavery by 2020 through education, funding and legal reform.[40] Philanthropists are also playing a more visible role in this space. Bill Gates and Michael Bloomberg, for instance, have created a fund to help countries defend themselves against litigation by tobacco firms.[41]

6. Identifying areas of regulatory arbitrage

There are many long-standing examples of regulatory arbitrage, including the sale of "illicit whites"[42] in the underground tobacco industry, but the synthetic drug market is home to some of the most alarming instances of this practice. Laboratory-produced chemical compounds that mimic the effects of popular recreational drugs but that are not yet controlled by international drug conventions are being sold as "legal highs".[43] The rapid emergence of these drugs has forced authorities to play regulatory catch-up to such an extent that the United Kingdom is considering a blanket ban on new psychoactive drugs, rather than banning the drugs one by one.[44] Many of these substances are being produced legally in China[45] and sold cheaply online; in the US, the Drug Enforcement Authority "can't keep up with regulating the drugs, essentially because the research labs in China can change the structure of the chemical and create new versions."[46]

IV. Harnessing technology to fight illicit trade

Illicit trade has long been considered to be something of a parallel universe, with illegal underground markets for everything that is legitimately sold in the global economy. This is truer today than ever before, with the emergence of illicit e-commerce that is "almost as easy as ordering from Amazon or eBay".[47] In just one year, the number of illegal drug listings on the so-called Dark Web or Dark Net — the anonymous portion of the internet — rose from 20,000 to 47,000.[48] Dark Web marketplaces require specialized technology, software such as Tor, allowing people to browse the web while hiding their identities, and a crypto-currency such as bitcoin that lets them transact their business discreetly.[49] Moreover, these Dark Web sites are innovating, introducing search engines, "trending" searches, user ratings and customer-service buttons.[50]

However, technological innovations are also being harnessed in the fight against illicit trade, and some are showing considerable promise. Examples include:

- *Big data to uncover sex traffickers*. Thomson Reuters Foundation and New York prosecutors worked with financial institutions to use data to uncover sex traffickers.[51]
- *Satellite tracking to tackle illegal fishing*. Backed by the Pew Charitable Trusts, project, Eyes on the Seas, uses a "Virtual Watch Room",[52] a digital platform which monitors waters across the world's oceans and can be accessed remotely by governments.
- *Big data to map deforestation*. To track illegal deforestation, Global Forest Watch was created as an online platform combining satellite images, high-tech data processing and crowd-sourcing, to provide near-real-time data on the world's forests.[53]
- *Drones for monitoring*. Drones can be used not only to monitor environmental crimes but also track illegal mining activities and trafficking of humans, wildlife and drugs.
- *DNA analysis*. DNA analysis is being used to detect food fraud[54] based on a genetic library of all life on Earth. DNA analysis is also being deployed to combat the illegal wildlife trade, with forensic laboratories set up to link stolen ivory to specific animals.[55]

Conclusion

We believe that the World Economic Forum is the ideal multistakeholder platform to bring together global leaders to improve the effectiveness of policies designed to prevent and mitigate illicit trade.

Some priorities for action:

- If we are to develop a culture of evidence to facilitate informed decision-making across all sectors, then there is a critical need to develop a common or harmonized data base. This has been the number one demand from key stakeholders and participants in this effort. The Forum could play a role here, as an independent, non-partisan and well-respected convener of knowledge and thought leadership.
- Technological solutions are now more cost effective, can be deployed faster and the latest innovations – applications, smartphones and optics – all make traceability feasible at scale. Businesses should employ technologies that allow an appropriate level of information to be shared with the public and law enforcers, so that legitimate products can easily be distinguished from illegitimate products. More broadly, we need to identify the opportunities presented by technology to fight illicit trade.
- We do not have a global governance regime to deal with illicit trade. The closest we have are “initiatives”, many of which are, or at some point will be, competing with each other. These include the World Customs Organization (WCO), the Office for Harmonization in the Internal Market, and INTERPOL. Confusion over different organizations’ areas of responsibility benefits those involved in illicit trade and, in recognition of this, these three organizations work closely together. Since 2012 they have conducted some 30 joint operational training events and activities, involving 4,000 officers from 85 countries and representing all INTERPOL regions and languages. The WCO has been involved in operations, seminars, mentoring programs, workshops and conferences involving more than 200 stakeholder organizations.
- It is imperative that efforts made by international organizations complement each other and that the focus remains on policy coherence in combating illicit trade. They must also tackle the challenge of aligning fragmented governance with new concepts around the role of business and individuals in the fight against illicit trade.
- By making it clear to governments, businesses and individuals who discover, report and help staunch illicit trade that there are incentives for doing so, we can engage a broader group of stakeholders. Indirect and, where possible, direct financial benefits for those who identify and address illicit activity will encourage involvement.

Governments should support, or be encouraged to support, anti-counterfeiting efforts and the fight against illicit trade, including the FCTC and the World Customs Organization’s Interface Public Members (IPM) platform of tools, with appropriate legislation and awareness campaigns. There is also a need to coordinate and update assessments of the magnitude of different types of illicit trade.
The World Economic Forum Meta Council on the Illicit Economy’s “Illicit Trade Matrix” should be seen as one of its concrete deliverables. Its aim is to increase the awareness and overall understanding of international, government, institutional, social and private efforts - and their results - in the fight against illicit trade. Ultimately, it is hoped it will stimulate consensus on how to address the many challenges involved and stimulate the creation and implementation of new tools that can effectively and pro actively disrupt illicit networks.

Deep Dive: Analysis and Recommendations for Controlling the Illicit Mining and Trading of Minerals

A strategy for limiting or eliminating the contribution of minerals to the illicit economy

Mining operations within the formal, legal economy can drive growth and development. The illicit mining and trade of minerals can, however, be associated with smuggling, human-rights abuses, environmental destruction and other criminal activities. Solutions to these problems must address the complex interplay of political, social, commercial and economic relationships and drivers that feed the illicit economy. A central challenge is how to alter these relationships, transforming illicit mining operations so they become part of the formal economy, where the rule of law prevails and trade can be legitimized. Transparency, enhanced reporting and accountability, reinforcement of host governments' ability to combat illicit activity, and global advocacy are key elements of the necessary reforms.

Reform measures must be mineral-specific and based on an analysis of specific mineral supply chains. Such measures would span the range of activities from mining through trading to final use, and include safeguards to protect any positive aspects of illicit activity, such as employment. Most measures will focus on Artisanal and Small Mines (ASMs), but will also include guiding principles for large-scale mines, mainly regarding trade.

The ASM Matrix – a risk map for the illicit trade in minerals

Mapping the illicit mining and trade in minerals will support targeted intervention. Recognizing that some minerals cannot be mined or traded illegally because of the scale of investment required, a first step is to identify those whose operations can be undertaken clandestinely. Such a map will cover two distinct mineral categories: precious minerals such as diamonds, gold and rubies, and minerals that require very low capital investment and skill to extract, such as tantalum ores and tin. The map would focus on regions of concern where conditions are most likely to support illicit activity and where certain target minerals are present. It would identify areas of risk for conflict between ASMs and larger scale mining (LSM). The supply and value chain of each target metal can be captured as part of a database.

Annex 1 is a table that offers an example of how this information could be organized. It would inform, expose and reveal pressure points for focused attention and action. A major data gathering exercise is envisaged. It would need a host, such as the World Economic Forum, the Organisation for Economic Cooperation and Development (OECD) or another multi-sector initiative, and should be updated periodically. Protocols, legal safeguards and other administrative arrangements will have to be worked out. This map would form a basis for a global situation analysis. This would help identify appropriate actions for the control of the illicit mineral trade and its migration to the formal economy.

Reform measures

A combination of measures would focus on the pressure points identified on the map. Some of the instruments that could be used are:

- **Certificates and supply-chain assurance for refiners**. Notwithstanding the limitations of track-and-trace mechanisms for certain minerals, assurance systems, such as those using refiner certificates, can bring transparency to supply chains. They can also help target illicit operations, particularly when aimed at key pinch points. A focus on refiners and smelters has proven an effective strategy, allowing downstream companies to know they are sourcing from trusted partners.
- **Legitimate trading, processing and training centres**. Processing, trading and training centres could be introduced in target regions, fuelling development and functioning as a choke point in the way that refiners do. These centres would be accredited by an outside authority to ensure compliance, and training and skills development would be offered. This strategy can shorten the supply chain, bringing more financial value to miners in exchange for the required paperwork. Such centres would also serve as hubs of legal activity, attracting legitimate ASMs.
- **End-user pressure and incentives, including certification**. End-users can play a critical role in raising demand and support for the licit trade in minerals. For jewellery, a water-marked certificate could be designed to accompany all sales of precious stones and gold to consumers. Similarly, dealers and processors such as diamond cutters could be recognized for dealing only in certified stones or gold. Later, individual countries could issue assurance certificates for all sites and sales, and downstream technology companies could assure consumers that they know their minerals do not contribute to conflict. Certification can also bring value to ASM communities and reward better practices, through initiatives such as “development diamonds” and “fair mined jewellery”.
- **Transparency and Advocacy Initiative on ASM (TASM).** Lessons from the Extractive Industries Transparency Initiative (EITI) and the African Peer Review Mechanism (APRM) suggest that a permanent system of advocacy at local and international levels against illicit mining and trading will bring value. A key tool will be the ASM Matrix on illicit minerals (see Annex 1). Regular publication of country-based reports and maps would be combined with widespread publicity to garner global support. Publicity and advocacy would provoke debate and pressure. TASM would be a constructive public and private partnership. Participating countries, companies and organizations would be incentivized to be good actors. Further work is required to determine how and where to initiate and host this measure.
- **Transparency and EITI-type reporting**. The early EITI approach targeted discrepancies between disbursements by companies and official receipts held by the public treasury. This had significant benefits, one of which was increasing awareness of the business money trail. Building on this approach, one possibility would be to oblige all buyers of unprocessed minerals in host countries to disclose their sources of supply, without compromising commercial confidentiality. Voluntary corporate reporting standards could be considered. More detailed home-government reports on volumes and source of imports would be a good starting point.
- **Country case studies and policy reform**. A set of case studies informed by the Matrix and identified by TASM could be established, beginning with countries known to harbour significant illicit mining operations. These could help determine the right combination of tax, market and public-sector incentives to convert illicit entities to formal structures. These case studies would examine the adequacy of legal frameworks, institutional arrangements and overall governance controls. Local knowledge would provide information that could be confirmed using modern technology such as electronic maps, drones and geographic information systems. Harmonizing tariffs on minerals between neighbouring countries would discourage smuggling, which is especially prevalent in Africa. Global action would help to dismantle markets for ores that have been mined illegally.
- **Capacity-building, trade sanctions and development partners**. Capacity-building and donor prioritization would be used to strengthen host-country capacity to enforce laws and regulations in order to retain mining operations within the formal economy. Building on learnings from experience in other markets, sanctions should be designed that are practical and easily monitored. It is important to avoid sanctions that would drive operations back to the illicit economy. Complementary measures would include incentives for ASM miners, such as free services through training and trading centres, which would draw them into the formal economy.
- **Harmonization of international protocols and tools for minerals from conflict zones.** The incentives for illicit activities are probably highest in conflict zones. Here, the adoption of protocols to be observed globally, such as those developed by the OECD, is a good way forward. Harmonization should be sought across both policy tools and voluntary initiatives, such as the World Gold Council conflict-free tool. This would support adoption by host and trading countries, as well as companies in mineral supply chains.

- **Alternative and supplementary livelihoods**. This is arguably the most difficult of areas to address, but there are lessons from the experience of the coca farmers of Latin America that can be customized for the minerals sector. Admittedly, farming, the obvious alternative to mining, is sometimes unattractive to those undertaking ASM activity. There is no immediate return, workers tend to be subject to traditional hierarchical controls, regular revenues are absent and farmers must await harvest for income, and missing is the gambler's possibility of windfall returns. Nevertheless, there are success stories, and these should serve as models for pilot programmes. Donor coordination to support these strategies is critical.
- **Clean ASM Finance Fund**. ASM miners are sometimes lured into the illegal economy because of the availability of finance provided by the illicit sector. A Clean ASM Finance Fund could be established and tested in target regions to help break this link.
- **LSM-ASM intervention experts**. Given that they are increasingly working in the same regions, conflicts between LSMs and ASMs are likely to increase. With the demise of the World Bank's Communities And Small Scale Mining (CASM) programme, there is now a gap in expertise and research. It is time to re-establish a global network of accredited experts who can address LSM-ASM conflicts.
- **Upstream data-gathering and ASM-to-market pilots**: We should encourage technological innovation to support data gathering on ASM miners and sources. Where possible, this data should be linked to mid- and up-stream data sets and reform initiatives, including those incentivizing participation in ethical product markets.

Finally, we see a world where technology, big data and transparency will combine to enable consumers to use their smartphones to support ethical buying.

Conclusion—the way forward

We recommend the following:

- The World Economic Forum, OECD and RESOLVE's Public Private Alliance for Responsible Minerals Trade should organize an international experts' meeting to prioritize and develop an action plan. This should include discussion on the design and launch of TASM, promote donor coordination, and support harmonization of law and voluntary instruments.
- The ASM Matrix should be designed and launched.
- A working group should be set up to define and extend the current transparency architecture, focused on promoting licit minerals, such as the CFSP and WGC. This would have a mandate to build an interactive information or data-sharing platform on illicit operations in minerals, including LSM.

Annex 1. Value Chain Matrix for Tantalum Ores

Source countries (b)	Centres			Potential pressure points				
	Concentrating (c-1)	Exporting (c-2)	Processing (Refining) (c–3)	Mining[1] (d)	Transport[2] (e)	Trade (f)	Processing (Refining) (g)	End User/ Retailer (h)
DRC Rwanda Burundi Rep. Congo	DRC* Rwanda Burundi Rep. Congo	DRC* Tanzania South Africa	China US					
Brazil	Brazil	Brazil	China US					
Columbia	Columbia	Columbia	China US					
Australia	Australia	Australia	China US					

Known Uses: Capacitors, super alloys, etc.
Destinations: (primary known use product producer locations) USA, EU, China, etc.
* known illicit transfers out of country for prior to and after concentrating steps occur

(Footnotes)
[1] Information on precise locations and who are involved (Women, children, youths, Illegal armed groups)
[2] Illegal agents, shipping companies, uncertified movements

Endnotes

1. ICC-BASCAP study done by Frontier Economics http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/
2. World Trade Organization Press Release, 14 April 2015 https://www.wto.org/english/news_e/pres15_e/pr739_e.htm
3. United Nations News Service, 31 May 2015 http://www.un.org/apps/news/story.asp?NewsID=51010#.VXvL2ut0afQ
4. A study from a special issue of the American Journal of Tropical Medicine and Hygiene published April 2015 as cited in the New York Times editorial, "Stemming the Tide of Fake Medicines," 18 May 2015 http://www.nytimes.com/2015/05/18/opinion/stemming-the-tide-of-fake-medicines.html
5. International Policy Network Link, cited in UN's Africa Renewal May 2013 http://www.un.org/africarenewal/magazine/may-2013/counterfeit-drugs-raise-africa%E2%80%99s-temperature
6. International Policy Network Link, cited in UN's Africa Renewal May 2013 http://www.un.org/africarenewal/magazine/may-2013/counterfeit-drugs-raise-africa%E2%80%99s-temperature
7. May 2014 report of ILO Link; also cited in BBC News, 20 May 2014 "Forced labour 'making $150bn profit' - ILO report" http://www.bbc.com/news/world-europe-27480896
8. World Bank, "Labour Force Total," 2014 http://data.worldbank.org/indicator/SL.TLF.TOTL.IN/countries
9. National Post, "Mark Vlasic: Illicit trade in looted antiquities helps finance ISIS terror network," 15 September 2014, http://news.nationalpost.com/full-comment/mark-vlasic-illicit-trade-in-looted-antiquities-helps-finance-isis-terror-network
10. BBC News, "Islamic State and the 'blood antique' trade," 2 April 2015 http://www.bbc.com/culture/story/20150402-is-and-the-blood-antique-trade
11. United Nations Environment Programme and Interpol, "The Environmental Crime Crisis" 2014, http://www.unep.org/unea/docs/RRAcrimecrisis.pdf also cited in VICE News 26 June 2014, "The Illicit Wildlife and Resource Trade Is Financing Militias and Terrorists" https://news.vice.com/article/the-illicit-wildlife-and-resource-trade-is-financing-militias-and-terrorists
12. OECD press release 8 April 2015, http://www.oecd.org/dac/stats/documentupload/ODA%202014%20Technical%20Note.pdf
13. The Guardian, "$213bn illegal wildlife and charcoal trade 'funding global terror groups'," 24 June 2014 http://www.theguardian.com/environment/2014/jun/24/illegal-wildlife-charcoal-trade-funding-global-terror-groups
14. United Nations Office on Drugs & Crime, "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes," (2011) https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
15. An example is the World Customs Organization's press release for its first "Illicit Trade Report" referencing the GAC on Illicit Trade http://www.wcoomd.org/en/media/newsroom/2013/june/wco-publishes-its-first-illicit-trade-report.aspx
16. Global Agenda Council on Illicit Trade & Organized Crime 2012-2014 http://www3.weforum.org/docs/GAC/2013/Connect/WEF_GAC_Illicit_Trade_and_Organized_Crime_2012-2014_Connect.pdf
17. United Nations Office on Drugs and Crime, "World Drug Report," 2010: 12, accessed October 1, 2010. http://www.unodc.org/documents/wdr/WDR_2010/World_Drug_Report_2010_lo-res.pdf
18. OECD "Magnitude of Counterfeiting and Piracy of Tangible Products: An Update."
19. Belser, Patrick, "Forced Labour and Human Trafficking: Estimating the Profits," ILO, March 2005.
20. Baker, Raymond, "Capitalism's Achilles Heel: Dirty Money and How to Renew the Free-Market System" (Hoboken: Wiley, 2005), 167.
21. GFI Interview with Hollis Cummers, Coalition Against Wildlife Trafficking (CAWT) Director, June 12, 2009
22. High Seas Task Force, "Closing the net: Stopping illegal fishing on the high seas," Governments of Australia, Canada, Chile, Namibia, New Zealand, and the United Kingdom, WWF, IUCN and the Earth Institute at Columbia University (2006): 18 http://www.illegal-fishing.info/uploads/HSTFFINALweb.pdf.
23. "'Illegal' Logging and Global Wood Markets: The Competitive Impacts on the U.S. Wood Products Industry." Seneca Creek Associates, LLC and Wood Resources International (November 2009) pg. 4, http://www.illegal-logging.info/uploads/%20afandpa.pdf
24. Idriss, Manar, Manon Jendly, Jacqui Karn, and Massimiliano Mulone, "International Report on Crime Prevention and Community Safety: Trends and Perspectives," International Centre for the Prevention of Crime, 2010, pg. 52.
25. "The Globalization of Crime: A Transnational Organized Crime Threat Assessment," United Nations Office on Drugs and Crime (2010) p. 263, accessed September 22, 2010, http://www.unodc.org/documents/data-and-analysis/tocta/11.Regions_under_stress.pdf
26. Hurd, Emma, "Sky Exclusive: Cops And Gold Smugglers," Sky News, February 27, 2008.
27. Morante, Thor, "Illegal gold mining destroying Peru's Madre de Dios jungle."
28. Interlandi, Jeneen, "Not Just Urban Legend," Newsweek, January 10, 2009
29. Stohl, Rachel, "Fighting the Illicit Trafficking of Small Arms," Center for Defense Information (13 May 2005)
30. "Annual Summary Charts: 2008," Kimberley Process: Rough Diamond Statistics. Kimberley Process.
31. Los Angeles Times (Associated Press), "Chinese banks a haven for Web counterfeits," 11 May 2015 http://www.latimes.com/business/la-fi-china-banks-counterfeiting-20150511-story.html
44. Interpol has an annual budget of roughly $75 million, which was increased through donations from the tobacco industry.
32. Bloomberg, 16 January 2015, "One Thing Gangs Smuggling Latin Migrants Over the Border Can't Do Without: Big U.S. Banks," http://www.bloomberg.com/news/articles/2015-01-16/one-thing-gangs-smuggling-latin-migrants-over-the-border-can-t-do-without-big-u-s-banks
45. Wall Street Journal, 1 April 2015 "China Tries to Clean Up E-Commerce" http://www.wsj.com/articles/china-tries-to-clean-up-e-commerce-1427894413
34. Reuters, 16 May 2015, "Alibaba sued in U.S. by luxury brands over counterfeit goods," http://www.reuters.com/article/2015/05/16/us-alibaba-lawsuit-fake-idUSKBN0O02E120150516
35. Bloomberg, 16 May 2015, "Etsy Counterfeit Problems Grow as Investors Allege Fraud," http://www.bloomberg.com/news/articles/2015-05-15/etsy-counterfeit-problems-grow-as-investors-allege-fraud
36. Bloomberg, 6 May 2015, "Nuclear Smugglers Abusing Alibaba Listings Challenge Iran Deal," http://www.bloomberg.com/news/articles/2015-05-05/nuclear-smugglers-abusing-alibaba-listings-challenge-iran-deal
37. Financial Times, 26 September 2014, "Alibaba: Weapons of mass ecommerce," http://www.ft.com/intl/cms/s/0/2a19e07c-43ef-11e4-8abd-00144feabdc0.html
38. Wall Street Journal, 17 November 2014, "Google to Spend $250 Million to Boost Ad Compliance Plan," http://www.wsj.com/articles/google-to-spend-250-million-to-boost-ad-compliance-plan-1416229758
39. Bloomberg, 24 July 2014, "Google Targeted in State Crackdown on Illicit Drug Ads," http://www.bloomberg.com/news/articles/2014-07-24/google-targeted-in-state-crackdown-on-illicit-drug-ads
40. Bloomberg, 28 November 2014, "China's Web Stimulates Illegal Trade in Endangered Species," http://www.bloomberg.com/bw/articles/2014-11-28/buy-and-sell-endangered-species-on-the-chinese-internet
41. IFAW Report, "Elephant vs Mouse: An investigation of the Ivory Trade on Craigslist," 2015 http://www.ifaw.org/sites/default/files/IFAW-craigslist-ivory-report-2015.pdf
42. The Telegraph, 9 December 2014, "People smugglers using Facebook to recruit migrants," http://www.telegraph.co.uk/news/worldnews/europe/italy/11282264/People-smugglers-using-Facebook-to-recruit-migrants.html

43. Financial Times, 21 October 2014 "IT and the trade in conflict minerals," http://www.ft.com/intl/cms/s/0/34c46212-4f99-11e4-908e-00144feab7de.html

33. Wall Street Journal, 27 October 2014, "Icann, Regulators Clash Over Illegal Online Drug Sales," http://www.wsj.com/articles/icann-regulators-clash-over-illegal-internet-drug-sales-1414463403

46. The Australian, 24 April 2015, "Casting a wide net for criminals," http://www.theaustralian.com.au/news/features/casting-a-wide-net-for-criminals/story-e6frg6z6-1227317775501

47. Council on Foreign Relations, 27 February 2015, "The Tobacco Treaty Turns 10" http://www.cfr.org/health-policy-and-initiatives/tobacco-treaty-turns-ten/p36192?cid=rss-analysisbriefbackgroundersexp-the_tobacco_treaty_turns_ten-022715

48. Reuters, 17 December 2014, "EU shines light on dirty money with central registers," http://www.reuters.com/article/2014/12/17/eu-moneylaundering-lawmaking-idUSL6N0U11HZ20141217

49. Wall Street Journal, 17 December 2014, "EU Moves to Counter Money Laundering," http://www.wsj.com/articles/eu-rules-to-require-listing-of-company-owners-on-national-registers-1418825431

50. Financial Action Task Force, 24 October 2014, "High Risk and non-cooperative jurisdictions" Public Statement http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/public-statement-oct2014.html

51. Wall Street Journal, Risk & Compliance blog, 30 March 2015, "Supply Chain Slavery Comes Into Focus for Companies," http://blogs.wsj.com/riskandcompliance/2015/03/30/supply-chain-slavery-comes-into-focus-for-companies/

52. Hana Ross, "Controlling Illicit Tobacco Trade: International Experience." Economics of Tobacco Control Project, 28 May 2015 http://tobacconomics.org/wp-content/uploads/2015/05/Ross_International_experience_05.28.15.pdf

53. Reuters, 2 December 2014, "World religious leaders pledge to fight modern slavery," http://blogs.reuters.com/faithworld/2014/12/02/world-religious-leaders-pledge-to-fight-modern-slavery/

54. Reuters, 18 March 2015, "Gates and Bloomberg create $4 million fund to fight Big Tobacco," http://www.reuters.com/article/2015/03/18/us-health-tobacco-fund-idUSKBN0ME24C20150318

55. "Illicit whites are cigarettes that may be produced legally but, as KPMG puts it, are "typically not sold legally anywhere and are often made exclusively for smuggling" as cited in BBC News, 23 January 2015, "The cigarettes that worry tobacco firms," http://www.bbc.com/news/blogs-magazine-monitor-30949434

56. AFP/Business Insider 26 May 2015, "Meth consumption in Asia is booming as wealth rises" http://www.businessinsider.com/afp-meth-seizures-quadruple-across-much-of-asia-pacific-un-2015-5

57. The Telegraph, 27 May 2015, "Blanket ban on 'legal highs' will see dealers face seven years in jail" http://www.telegraph.co.uk/news/politics/queens-speech/11633825/Blanket-ban-on-legal-highs-will-see-dealers-face-seven-years-in-jail.html

58. The Guardian, 1 May 2015, "'Our purity is above 99%': the Chinese labs churning out legal highs for the west," http://www.theguardian.com/society/2015/may/01/chinese-labs-legal-highs-west-drugs

59. Tech.Mic 27 May, 2015, "It's Ridiculously Easy to Buy Flakka, the New Street Drug That's Devastating Florida," http://mic.com/articles/119280/it-s-ridiculously-easy-to-buy-flakka-the-new-street-drug-that-s-devastating-florida

60. Washington Post Wonkblog, 24 November 2014, "The not-so-secret place on the Web that sells drugs, uranium…"http://www.washingtonpost.com/blogs/wonkblog/wp/2014/11/22/a-complete-tally-of-the-weird-disturbing-and-hilarious-things-for-sale-on-the-internets-largest-black-market/

61. Wired, 27 October 2014, "NY Senator calls for renewed crackdown on dark web drug sales," http://www.wired.com/2014/10/schumer-crackdown-on-dark-web-drug-sales/

62. Economist, 1 November 2014, "The Amazons of the dark net," http://www.economist.com/news/international/21629417-business-thriving-anonymous-internet-despite-efforts-law-enforcers

63. The Guardian, 5 October 2014, "Dark net markets: the eBay of drug dealing," http://www.theguardian.com/society/2014/oct/05/dark-net-markets-drugs-dealing-ebay

64. Reuters, 18 November 2014, "US data war on sex trafficking to reach Europe," http://www.reuters.com/article/2014/11/18/women-conference-vance-idUSL6N0T74AB20141118

65. Economist, 24 January 2015, "Combating Illegal Fishing: Dragnet," http://www.economist.com/news/science-and-technology/21640306-new-satellite-based-surveillance-system-will-keep-sharp-eye-those

66. The Guardian, 2 October 2014, "Counting trees to save the woods," http://www.theguardian.com/global-development-professionals-network/2014/oct/02/counting-trees-to-save-the-woods-using-big-data-to-map-deforestation

67. Scientific American, 4 February 2014, "Quick DNA Scans Could Ensure Food Is Safe to Eat," http://www.scientificamerican.com/article/quick-dna-scans-could-ensure-food-is-safe-to-eat/

68. BBC 8 May 2015, "Kenya opens anti-poaching forensic laboratory," http://www.bbc.com/news/world-africa-32651578

69. The ILO states in their 2012 study's executive summary that "human trafficking can also be regarded as forced labour," and the 20.9 million "estimate captures the full realm of human trafficking for labour and sexual exploitation or what some call 'modern-day slavery.'" This figure does not include trafficking for organ removal and forced marriage/ adoption unless leading to forced labour and sexual exploitation. International Labour Organization, "Global estimate of forced labour: Executive summary," 2012, pg. 1. http://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_182004.pdf

70. Ibid.

71. Shelley, L., Human Trafficking: A Global Perspective, Cambridge University Press, 2010.

72. Verité, "Forced Labor in the Production of Electronic Goods in Malaysia: A Comprehensive Study of Scope and Characteristics," 2014. http://www.verite.org/sites/default/files/images/VeriteForcedLaborMalaysianElectronics_2014_0.pdf

73. Verité, "Strengthening Protections Against Trafficking in Persons in Corporate and Federal Supply Chains," 2015. http://www.verite.org/sites/default/files/images/Verite-Executive_Order_13627.pdf

Members of Meta-Council on the Illicit Economy

Adam Blackwell (Chair)
Ambassador in residence, William J. Perry Center for Hemispheric Defense and Security Studies (NDU), National Defense University, USA

Christina Bain
Director, Initiative on Human Trafficking and Modern Slavery, Babson College

Jay Cziraky
Chief Executive Officer, North Degrees

Raymond Baker
President, Global Financial Integrity

Steven Simske
HP Fellow and Director, Content Solutions, Hewlett-Packard Company

Steven Broad
Executive Director, TRAFFIC International

Gaozhang Zhu
Director, Compliance and Facilitation, World Customs Organization (WCO)

Hans J. Schwab
Managing Director, Tech Trace SA

Linah K. Mohohlo (Vice-Chair)
Governor and Chairman of the Board, Bank of Botswana

Dimitri Vlassis
Chief, Corruption and Economic Crime Branch (UNODC), United Nations Office on Drugs and Crime

Anton Plessis
Managing Director, Institute for Security Studies (ISS)

Wolfgang Goetz
Director, European Monitoring Centre for Drugs and Drug, Addiction (EMCDDA)

Rolf Alter
Director, Public Governance and Territorial Development, Organisation for Economic Co-operation and Development (OECD)

Laura Lane
President, Global Public Affairs, UPS

Jean-Paul Laborde
Executive Director, Counter- Terrorism Executive Directorate (CTED), United Nations

Alan D. Cohn
Adjunct Professor, Georgetown University Law Center

Ashifi Gogo
Chief Executive Officer, Sproxil

Paul Boon Hui Khoo
Senior Adviser, Ministry of Home Affairs of Singapore

World Economic Forum

Jean-Luc Vez
Managing Director, Head of Public Security Policy and Security Affairs Member of the Management Committee, World Economic Forum

Karen Wong, Council Manager of Meta-Council on the Illicit Economy
Community Specialist, Global Crime and Public Security, World Economic Forum

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum – committed to improving the state of the world – is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org