SUPPORTING INNOVATION, CREATIVITY & ENTERPRISE

CHARTING A PATH AHEAD

U.S. JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT

FY 2017 - 2019

SUPPORTING INNOVATION, CREATIVITY & ENTERPRISE

CHARTING A PATH AHEAD

U.S. JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT

FY 2017 - 2019

TABLE OF CONTENTS

SECTION 1

THE GLOBAL SCALE OF INTELLECTUAL PROPERTY THEFT AND ITS UNLAWFUL EXPLOITATION BY THIRD PARTIES POSES SERIOUS THREATS TO U.S. NATIONAL INTERESTS 17

A. The Economic Scope and Magnitude of Counterfeiting, Commercial Piracy, and Trade Secret Theft: A Global Perspective 19

1. Assessments of the Scale and Economic Impact of Counterfeiting and Commercial Piracy 20
2. Assessments of the Scale and Economic Impact of Trade Secret Theft 21

B. The Complex and Sophisticated Nature of Commercial Piracy, Counterfeiting and Trade Secret Theft in the Modern Era 21

1. Schemes Employed for the Unlawful Exploitation of Digital Content 21
2. Schemes Employed to Facilitate Illicit Trade in Counterfeit Goods 26
3. The Targeting and Theft of Trade Secrets 31

C. The Theft and Unlawful Exploitation of Intellectual Property as Threats to U.S. National Interests 32

1. Undermines Principles of Fair Trade in the Global Economy 32
2. Threatens Consumer Health and Safety 33
   - *Example: Counterfeit Personal Care Products* 33
   - *Example: Counterfeit Consumer Electronics & Electrical Products* 34
   - *Example: Counterfeit Pharmaceuticals* 35
   - *Example: Counterfeit Automotive Parts* 37
3. Threatens the Environment 38
4. Exploits Labor 39
5. Poses Threats to Domestic and International Security 40
   a. The Integrity of Supply Chains and Critical Infrastructures 41
   b. The Convergence between Intellectual Property-Based Crime and the Financing of Criminal and Terror Networks 42

SECTION 2

HELPING TO PROMOTE A SAFE AND SECURE INTERNET: MINIMIZE COUNTERFEITING AND INTELLECTUAL PROPERTY-INFRINGING ACTIVITY ONLINE 61

A. Targeting Financial Support Flowing to Criminals: A "Follow-the-Money" Approach to Combating Online Commercial Piracy and Counterfeiting 61

1. Strengthen Payment Processor Networks' Efforts to Curb Illicit Proceeds 62
2. Strengthen Online Advertising Networks' Efforts to Curb Flow of Illicit Revenue 63
3. Strengthen Foreign Banking Practices to Curb the Financing of Illicit Trade 66

B. In Furtherance of a Healthy Domain Name System....68
1. Assessing the Enforcement Challenge of Domain Name Hopping....68

C. Reducing Online Piracy and Counterfeiting by Increasing the Ability of Consumers to Locate Content and Products Through Lawful Means....69
1. Support Consumers' Identification of Websites Offering Legal Goods or Services....69
2. Support Practices and Policies to Improve DMCA Notice-and-Takedown Processes....70
3. Support Practices and Policies Within Social Media Channels to Curb Intellectual Property Based Illicit Activity....71
4. Support Practices and Polices to Reduce Intellectual Property Infringement Facilitated by Mobile Apps....73
5. Putting the Consumer First: Combatting Operators of Notorious Websites by Way of Consumer Education....74
6. Encourage Efforts that Support Content Platforms Offering Content Legally and Minimize Deceptive Sites That Operate with a Commercial "Look and Feel"....76
7. Opportunities to Curb Sales of Counterfeit and Pirated Goods on E-Commerce Platforms....77

D. Support Responsible 3D Printing Communities and Business Models....79

E. Address Cyber-Enabled Trade Secret Theft....80

SECTION 3

SECURE AND FACILITATE LEGITIMATE CROSS-BORDER TRADE....93

A. Safeguarding Our Borders: Enhancing Identification and Interdiction of Counterfeit and Pirated Goods Bound for the U.S. Market....93
1. Employ an "All-Threats" Approach to Cargo Screening....94
2. Combat the Domestic Assembly and Finishing of Counterfeit Goods....94
3. Address the Surge of Small Parcels in the Express Consignment and International Mail Environments....96
4. Implement Advance Targeting Capabilities in the International Mail Environment to Address Rising Threats in the Global Marketplace....99
5. Assess Scope of, and Respond to, Importer Identity Theft in the Trade Environment....100
6. Enhance Customs Recordation Systems and Public-Private Collaboration on Information Collection....101
7. Invest in Anti-Counterfeiting Technology....102
8. Enhance Interdiction Through Specialized Task Forces....104
9. Enhance Fines, Penalties, and Forfeiture Processes and Practices....104
10. Improve Administration of ITC Exclusion Orders....105
11. Expand and Enhance the Use of Post-Entry Audits....106

B. Working Globally: Efforts to Curb the Movement and Trade of Counterfeit and Pirated Goods Around the World 106
1. Promote Necessary Seizure Authority and Best Practices Around the World 107
2. Curb Illegal Operations Within Free Trade Zones 109
3. Support Modern Recordation Systems in Developing Countries 110
4. Tackle the Growing Costs Associated with the Storage and Destruction of Counterfeit Goods 111
5. Dispose of Infringing Goods in an Environmentally-Friendly Manner 112

SECTION 4

PROMOTE FRAMEWORKS AND POLICIES TO ENHANCE THE EFFECTIVE ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS 121

A. Promote Governmental Frameworks for Coordinated and Effective Intellectual Property Enforcement 121
1. The U.S. Model: A "Whole of Government" Approach to Intellectual Property Enforcement 122
2. The "Specialized Office" Approach to Intellectual Property Enforcement 125

B. Enhance Capacity-Building, Outreach, and Training Programs on Intellectual Property Enforcement in Other Countries 129

C. Promote Enforcement of U.S. Intellectual Property Rights Through Trade Policy Tools 131

D. Supporting Innovation and Technological Advancements: The Need for Tools for Effective and Predictable Patent Protection Domestically and Abroad 134
1. Enhancing Domestic Patent Protection 134
2. Enhancing Domestic Design Protection 136
3. Enhancing the Effectiveness of Patent Systems Abroad 137
a. Reducing Patent Pendency 137
b. Promoting Effective, Transparent, and Predictable Patent Systems 138
c. Enhancing Effectiveness of Design Systems Abroad 139

E. Broader Recognition of the Essential Role Universities Play in Innovation 140

F. Support Strategies that Mitigate the Theft of U.S. Trade Secrets 141

G. Promote Supply-Chain Accountability in Government Acquisitions 142

H. Calls for Research 143



A Reflection on Creativity and the American Spirit

When Walt Whitman wrote, "The United States themselves are essentially the greatest poem," he was not discussing literature. What Whitman praised so prophetically was the vast and transformative creative energy that characterized his young nation and, indeed, democracy itself. The Greek root of *poet* means *one who makes, creates, fashions, composes.* The United States created itself—politically, socially, and culturally—from the pieces of a colonial empire, and that early appetite for growth and experimentation has never been sated. American history is a tapestry of human achievement woven from innumerable threads of individual acts of imagination and innovation.

To be creative and productive, a society must respect the dignity of labor. Whether people work with their hands or their minds, they deserve to benefit from the fruits of their own labor. A product is not less useful because it is intellectual, intangible, sometimes even invisible. It is easier to steal a song than a cow, but a musician needs to earn a living no less than a dairy farmer. The world craves new songs as much as it does fresh butter. The chest a cabinetmaker sells exists in three dimensions as a physical object, and every passerby recognizes its value. A photographic image or pharmaceutical formula can be expressed in only two dimensions on paper or a screen. In such insubstantial form, they may seem negligible until the photograph changes public opinion or the formula saves a patient's life. Intangible products generate tangible value, and their creators should share in those benefits. Value is not expressed in tonnage.

"I hear America singing," Whitman wrote. The song he heard was the melody of workers rapt in the act of creation enlivened by the expectation of enjoying the fruits of their labor. He knew it was a song as diverse as humanity:

> *The carpenter singing his as he measures his plank or beam,*
>
> *The mason singing his as he makes ready for work, or leaves off work,*
>
> *The boatman singing what belongs to him in his boat, the deckhand singing on the steamboat deck,*
>
> *The shoemaker singing as he sits on his bench, the hatter singing as he stands,*
>
> *The wood-cutter's song, the ploughboy's on his way in the morning, or at noon intermission or at sundown,*
>
> *The delicious singing of the mother, or of the young wife at work, or of the girl sewing or washing,*
>
> *Each singing what belongs to him or her and to none else,*

In this famous hymn to labor, Whitman forgot to mention himself and his own enduring song. His words have outlasted the works of the carpenter and mason and still move millions across the world—he sang what belonged to him and no one else.

Dana Gioia

Poet Laureate of California



ABOUT THE OFFICE OF THE INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR & THE U.S. INTERAGENCY STRATEGIC PLANNING COMMITTEES ON INTELLECTUAL PROPERTY ENFORCEMENT

The Office of the Intellectual Property Enforcement Coordinator
Executive Office of the President

Under the Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("PRO-IP Act," or the "Act"), Public Law No. 110-43, the United States Congress created the position of the Intellectual Property Enforcement Coordinator (IPEC) within the Executive Office of the President of the United States. 15 U.S.C. §8111 *et seq*. Under the Act, the scope of intellectual property (IP) enforcement relates to copyrights, patents, trademarks, trade secrets, and other forms of intellectual property both in the United States and abroad, with a focus on combating counterfeit and infringing goods.

The Act outlines the IPEC's duties and includes specific efforts to enhance interagency IP enforcement policy coordination. In brief, the IPEC is directed to: coordinate the development of the Joint Strategic Plan on IP Enforcement, a national strategy for the designated departments and agencies involved in IP enforcement matters; facilitate the issuance of policy guidance to departments and agencies to assure the appropriate coordination of IP enforcement policy and consistency with other law; and report to the President and to Congress regarding domestic and international IP enforcement programs.

The IPEC is tasked with coordinating the development and issuance of two major documents: (i) an *Annual Report* on the progress made towards the effective enforcement of IP rights; and (ii) a *Joint Strategic Plan on IP Enforcement (hereafter the "Joint Strategic Plan," "Strategic Plan," or "Plan")*, issued every three years. The Joint Strategic Plan is delivered to the Committee on the Judiciary and the Committee on Appropriations of the U.S. Senate, and to the Committee on the Judiciary and the Committee on Appropriations of the U.S. House of Representatives. Per the Act, the Joint Strategic Plan is posted for public access on the White House website.

The U.S. Interagency Strategic Planning Committees on IP Enforcement

Pursuant to Federal statute and an Executive Order, the IPEC chairs two separate interagency committees to develop and implement the U.S. Government's IP enforcement priorities. Specifically, the IPEC chairs: (i) a Senior IP Enforcement Advisory Committee and (ii) an IP Enforcement Advisory Committee (collectively and hereinafter, the *"U.S. Interagency Strategic Planning Committees on IP Enforcement"*) in connection with the formation of the Joint Strategic Plan. The responsibilities and members of the committees are as follows:



Senior Advisory Committee
Established pursuant to Executive Order 13565

The Senior Advisory Committee is a cabinet-level committee that advises the IPEC, and is tasked with facilitating the formation and implementation of the Joint Strategic Plan. The designated departments and offices are represented on the committee by the corresponding head (or deputy head) of office.

This Joint Strategic Plan was developed with the support of leadership from the following entities:

1. Department of State;
2. Department of the Treasury;
3. Department of Justice;
4. Department of Agriculture;
5. Department of Commerce;
6. Department of Health and Human Services;
7. Department of Homeland Security;
8. Office of Management and Budget; and
9. Office of the U.S. Trade Representative.

IP Enforcement Advisory Committee
Established pursuant to 15 U.S.C. § 8111(b)(3) and Executive Order 13565

The IP Enforcement Advisory Committee is a sub-cabinet level committee charged with the development of the Joint Strategic Plan. The committee is composed of Senate-confirmed representatives, who are assigned by the respective heads of their designated departments, offices, and agencies.

Per the statute and the executive order, this Joint Strategic Plan was developed with participation and contribution from committee members representing the following entities:

1. Office of Management and Budget;
2. Relevant units within the Department of Justice, including the Criminal Division, the Civil Division, and the Federal Bureau of Investigation;
3. The U.S. Patent and Trademark Office, the International Trade Administration, and other relevant units of the Department of Commerce;
4. Office of the U.S. Trade Representative;
5. Department of State, including the Bureau of Economic, Energy, and Business Affairs, the U.S. Agency for International Development, and the Bureau of International Narcotics and Law Enforcement Affairs;
6. Department of Homeland Security, including U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement;
7. The Food and Drug Administration of the Department of Health and Human Services;
8. Department of Agriculture;
9. Department of the Treasury; and
10. U.S. Copyright Office.

MESSAGE FROM THE INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, AND CHAIR OF THE U.S. INTERAGENCY STRATEGIC PLANNING COMMITTEES



Photo credit: Ralph Alswang

I have been honored to serve as the Intellectual Property Enforcement Coordinator, and as Chair of the U.S. Interagency Strategic Planning Committees on IP Enforcement. On behalf of the Office, and the Federal partners represented on the interagency committees, I am pleased to present the Joint Strategic Plan on Intellectual Property Enforcement (FY 2017-2019), titled "*SUPPORTING INNOVATION, CREATIVITY & ENTERPRISE: CHARTING A PATH AHEAD.*"

The Strategic Plan is a blueprint for the work to be carried out over the next three years by the Federal Government—with opportunities for state and local governments, governments around the world, and the private sector—in support of a healthy and robust intellectual property enforcement policy environment. It starts with an acknowledgement and celebration of the extraordinarily important role that the creative and innovative communities play in our cultural and economic lives: supporting over 45 million U.S. jobs, more than 50 percent of our exports, and incentivizing all forms of dynamic and enriching creative expression.

The mission of the Federal Government in supporting creativity, innovation, and enterprise through the effective enforcement of intellectual property rights must be ambitious. The threats posed by patent, trademark, and copyright infringement, and the misappropriation of trade secrets, are real and multidimensional. Our work must be carried forward with a sense of urgency in order to minimize these threats and the often overlooked attendant harms that flow from IP-based illicit activities.

The protection of intellectual property rights is about promoting economic prosperity and supporting jobs; opening new markets for U.S. goods and services; and fostering innovation and investments in research and development. It is also about standing up for our values at home and abroad. Trade in counterfeit goods, for example, compromises the integrity of domestic and global supply chains, and creates significant public health and safety risks for our citizens. Illicit trade also subverts human rights through reliance on forced and even child labor, and endangers the environment through irresponsible manufacturing and disposal practices. These and other illicit IP-related acts also undermine national security interests when, for example, sensitive trade secrets are targeted for misappropriation; or counterfeit goods enter critical private or governmental supply chains; or when these illicit activities financially support transnational organized crime networks.

These threats are not limited to a single industry, nor do they fall under the purview of a single government agency or even a single country. They are cross-cutting in scope and global in scale. To address these and other concerns, the Strategic Plan lays out four primary, overarching goals during FY 2017-2019: (1) to enhance National understanding of the economic and social impacts flowing from the misappropriation of trade secrets and the infringement of intellectual property rights; (2) to promote a safe and secure Internet by minimizing counterfeiting and IP-infringing activity online; (3) to secure and facilitate lawful trade; and (4) to enhance domestic strategies and global collaboration in support of an effective IP regime.

The Strategic Plan has been prepared to go beyond a compilation of abstract goals or objectives, placing heightened importance on the need for a detailed assessment of the challenges faced by creative, innovative, and law enforcement communities, domestically and overseas, with respect to IPR enforcement. By adding increased attention on the specific dimensions of the evolving IP enforcement challenges before us, we may better advance the development of narrowly-tailored, but strategically-aligned, solutions in the months and years to come. As such, this Strategic Plan represents the beginning of a continuous process, and not the culmination of one.

This Strategic Plan represents a "call for action" for all nations—as well as international organizations, industry, educational institutions, and consumer protection and public interest groups—to provide forward-thinking leadership and a collaborative approach to combatting illicit IP-based activities. Together, we can enhance our enforcement programs and policies for the modern era, and ensure that collective efforts to curb illicit trade in counterfeit and pirated goods, online commercial piracy, trade secret theft, and other acts of IP infringement are maintained as a top priority.



Daniel H. Marti

Intellectual Property Enforcement Coordinator,
Executive Office of the President

INTRODUCTION

IP-intensive industries play a significant role in the U.S. economy, and serve as a primary driver of U.S. economic growth and national competitiveness. These important industries rely on the recognition and effective enforcement of a variety of intangible assets and products of the mind and human intellect, which we refer to collectively as "intellectual property."

IP is comprised of such things as **inventions** (protected under patent law); **literary and artistic works**, such as books, musical compositions, movies, computer programs, and other creative expressions (protected under copyright law); **distinctive symbols, names, and images** which distinguish the goods or services of one undertaking from those of others in the marketplace (protected under trademark and consumer protection laws); and **confidential business information**, including formulas, practices, processes, or methods that are not generally known (protected from improper means of discovery under trade secret law).

IP is found everywhere in the economy, and IP rights are relied upon by and support virtually every U.S. industry. IP-intensive industries represent a major, integral, and growing part of the U.S. economy. The Department of Commerce has reported that IP-intensive industries directly account for 27.9 million American jobs, and indirectly support an additional 17.6 million jobs. Together, this represents approximately 30 percent of all jobs in the U.S., with the total value added by IP-intensive industries amounting to 38 percent of U.S. Gross Domestic Product (GDP).

As the Supreme Court has noted, by "establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas."* Trademark law, on the other hand, serves two purposes, namely, to aid the consumer in differentiating among competing products and second, to protect the producer's investment and goodwill. And a patent is recognized by the Constitution as a means to serve the public purpose of promoting the "progress of science and useful arts."**

** Harper & Row, Pub., Inc. v. Nation Enter., 471 U.S. 539, 558 (1985)*
*** U.S. Const., art. I, § 8.*

Because of their value, IP assets are targets for unlawful appropriation and exploitation by entities pursuing unfair competition and often criminal enterprises. The Federal Government is committed to a balanced and effective intellectual property system, which includes the effective enforcement of intellectual property rights.

A number of U.S. departments, offices, and agencies share responsibility for IP enforcement, making effective *coordination* and *strategy-setting* essential for national effectiveness. The Joint Strategic Plan lays out the work to be carried out over the next three years by the Federal Government—with opportunities for state and local governments, government partners around the globe, and the private sector—to enhance coordination and collaboration in support of the effective enforcement of intellectual property rights.

The protection of intellectual property rights is essential to upholding fair competition in a global marketplace. With enhanced predictability and accountability in the market, IP-intensive industries are better positioned to finance creative and innovative research and development activities that lead, for example, to new technologies, breakthroughs in medicines, and a growing body of creative and innovative works. The attendant harms that flow from the misappropriation and infringement of intellectual property rights are troubling in size and scope, and— as set forth in greater detail throughout the Joint Strategic Plan— directly undermine a number of important national interests, including, at times, national security.

Purpose of the Joint Strategic Plan

Title III of the Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403 (the "PRO-IP Act," or the "Act"), mandates a coordinated approach to intellectual property enforcement policy. The Act requires development of a three-year National plan on enforcement of laws protecting copyrights, patents, trademarks, trade secrets, and other forms of intellectual property, with an emphasis on combatting counterfeit and infringing goods in the domestic and international supply chains.*

* PRO-IP Act §§ 302-303.

The objectives of the Joint Strategic Plan in the PRO-IP Act, are summarized as follows:

1. **Reduce** counterfeit and infringing goods in domestic and international supply chains;
2. **Identify** unjustified impediments to effective enforcement action against the financing, production, trafficking, or sale of counterfeit or infringing goods;
3. **Support** the sharing of information to curb illicit trade;
4. **Disrupt** domestic and international counterfeiting and infringement networks;
5. **Strengthen** the capacity of other countries to protect and enforce intellectual property rights;
6. **Establish** with other governments international standards and policies for the effective protection and enforcement of intellectual property rights; and
7. **Protect** intellectual property rights overseas by enhancing international collaboration and public-private partnerships.[†]

Raising public awareness and developing effective solutions begins with a detailed understanding of the nature of the problem presented.

To advance a detailed understanding, the Act places special emphasis on teasing out the dimensions of the overall problem as part of the strategy-setting process. Specifically, the Act places as a core objective of the Strategic Plan the need to identify "structural weaknesses," "systemic flaws," and other "impediments" to effective IPR enforcement actions against the financing, production, trafficking, or sale of counterfeit or infringing goods.[‡] The need to rigorously identify, define, and understand the dimensions of the problem—weaknesses, flaws, and impediments—have been taken to heart in the development of the Strategic Plan in order to help anchor the policy discussion and direction of proposed goals and objectives. Put differently, the U.S. Interagency Strategic Planning Committees on IP Enforcement did not speed past the nature of the problem in the strategy-setting process, but rather focused on developing a more robust understanding of the nature of the illicit activity in order to improve the enforcement and policy-setting environment on a going-forward basis.

The Joint Strategic Plan is a forward-looking document, concentrating almost exclusively on the nature of the impediments to effective enforcement and how best to overcome these challenges during the plan's three-year term. The Joint Strategic Plan does not provide a summary of all the progress made in the fulfilment of intellectual property enforcement initiatives over the past few years. There have been numerous accomplishments and initiatives to observe: from increased seizure and enforcement statistics to high-profile arrests and convictions; to the posting of Intellectual Property Law Enforcement Coordinators (IPLECs) and Intellectual Property Attachés around the world; to the bipartisan passage and enactment of the Defend Trade Secrets Act of 2016, Public Law 114-153 (May 11, 2016), to name a few. To learn more about these and many other important accomplishments, please refer to the *Annual Report on Intellectual Property Enforcement* issued by the Office of the Intellectual Property Enforcement Coordinator, and submitted to the Committee on the Judiciary and the Committee on Appropriations of the U.S. Senate, and the Committee on the Judiciary and the Committee on Appropriations of the U.S. House of Representatives, pursuant to Section 304 of the PRO-IP Act, 15 U.S.C. § 8814.[§]

Development of the Strategic Plan

Pursuant to the PRO-IP Act and Executive Order 13565, the Joint Strategic Plan on Intellectual Property Enforcement is developed by the U.S. Interagency Strategic Planning Committees on IP Enforcement, chaired by the IPEC and comprised of a diverse array of Federal departments, offices, and agencies, including the Department of Justice, the Department of Homeland Security, the Department of State, the Department of Commerce, the Department of the Treasury, the Department of Health and Human

[*] PRO-IP Act §§ 302-303.
[†] 15 U.S.C. § 8113.
[‡] *Id.* at § 303(a)(2).
[§] As of the timing of the issuance of this Joint Strategic Plan, the most recent summary of U.S. activities is contained in the Annual Report dated *April 29, 2016* (for Fiscal Year 2015), accessible at https://www.whitehouse.gov/sites/default/files/omb/IPEC/fy2015ipecannualreportchairmangoodlatteletter.pdf.

Services, the Department of Agriculture, the Office of Management and Budget, the Office of the U.S. Trade Representative, and the Copyright Office.*

In preparing this Joint Strategic Plan, the Office of the Intellectual Property Enforcement Coordinator and the members of the U.S. Interagency Strategy Planning Committees on IP Enforcement drew on their respective experience on IP enforcement. The U.S. Interagency Strategic Planning Committees on IP Enforcement are comprised of, and supported by, experts in intellectual property laws and enforcement matters, including the Federal Bureau of Investigation (FBI) and the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice; Customs and Border Protection (CBP); Homeland Security Investigations (HSI) within Immigration and Customs Enforcement (ICE); the Office of International IP Enforcement of the Department of State, and the U.S. Patent and Trademark Office (USPTO), among other offices and agencies.

The Office of the Intellectual Property Enforcement Coordinator and the interagency committees have also developed the Joint Strategic Plan by receiving input, as appropriate, from a wide variety of stakeholders across the Federal Government, along with input received from state and local governments; industry; non-governmental organizations; educational institutions; trade organizations; public interest groups; and others.

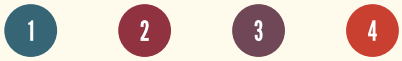
For example, the Office of the Intellectual Property Enforcement Coordinator and members of the U.S. Interagency Strategic Planning Committees on IP Enforcement have consulted with U.S. officials at various U.S. embassies, consulates, and posts around the world who may have extensive experience with intellectual property matters, or are active in supporting contacts with U.S. industries, or maintain regular dialogues with foreign government officials at key ministries and agencies. Such U.S. officials include, for example, Heads of Mission (e.g., Ambassadors and Chargés d'Affaires) and other senior Foreign Service Officers, as well as the agency representatives at post (e.g., Intellectual Property Law Enforcement Coordinators (IPLECs); Intellectual Property Attachés; CBP Attachés; and ICE/HSI Attachés).

Pursuant to Section 303 of the PRO-IP Act, the Office of the Intellectual Property Enforcement Coordinator, as well as members of the U.S. Interagency Strategic Planning Committees on IP Enforcement, also consulted and engaged with foreign governments, international organizations, and law enforcement bodies the world over to understand, for example, the global dimensions around the "financing, production, trafficking or sale of counterfeit and infringing goods," and the opportunities to enhance the effectiveness of intellectual property enforcement in a global market.†

The Joint Strategic Plan has also been developed by consulting with "companies, industry associations, labor unions, and other interested groups" and "private sector experts in intellectual property enforcement," as set forth in the PRO-IP Act.‡ The consultation included formal comments submitted to the Office of the Intellectual Property Enforcement Coordinator in response to its notice in the Federal Register on September 1, 2015, that informed the Federal Government's intellectual property enforcement strategy.§ Lastly, the U.S. Interagency Strategic Planning Committees on IP Enforcement relied on domestic and international reports and studies and congressional testimony and consultations with Members of Congress and their staff during the preparation of this Joint Strategic Plan on Intellectual Property Enforcement.

* For full membership of the *U.S. Interagency Strategy Planning Committees on IP Enforcement,* see page [4].
† *See*, e.g., PRO-IP Act §§ 303(a)(1), (4)-(7) and (f), as examples of statutorily mandated international considerations and engagement.
‡ *See* PRO-IP Act § 303(a)(7)(C) & 303 (c)(2).
§ Public comments and submissions in response to the Federal Register Notice are accessible at https://www.regulations.gov/document?D=OMB-2015-0003-0001.

THE ORGANIZATION OF THE STRATEGIC PLAN



The Strategic Plan is organized and divided into four main sections.

SECTION 1 provides an overview of how intellectual property serves as a material force behind U.S. economic growth, high-paying jobs, economic competitiveness, and creative expression. It also describes in detail the nature and scope of the IP enforcement-related challenges faced by IP-intensive industries and law enforcement communities. The overall dimensions and scale of intellectual property infringement appear to be on the rise, with the global estimate of international trade in counterfeit and pirated hard goods, for example, reported to now be up to *2.5 percent* of world trade or more than $400 billion. For further context and understanding, this section provides illustrative examples to show how business models that rely on unlawful IP infringement operate to target, misappropriate, and exploit IP assets belonging to others. Lastly, this section also includes a meaningful examination of the often overlooked attendant harms that flow from the misappropriation and unlawful infringement of intellectual property. In doing so, Section I outlines how unlawful activities threaten to undermine the rule of law and fair competition in world markets, and how illicit trade in counterfeit and pirated goods, for example, compromises the integrity of domestic and global supply chains, threatens public health and safety, and undermines a number of additional important national interests.

SECTION 2 focuses on illicit IP-based activity in the online (digital) environment. From the operation of stand-alone illicit websites, to unlawful activity on online platforms and services by illicit actors, this section explores opportunities to support and develop enhanced mechanisms to curb a wide-range of illicit online IP-based activity. It includes an examination of a "follow-the-money" approach to disrupt illicit financing (via payment processors and advertising networks). This section also discusses practices and policies aimed at curbing abusive activities that focus on legitimate e-commerce platforms, social media channels, and the search environment.

SECTION 3 focuses on strategies designed to facilitate secure and lawful trade domestically and abroad. Each year, more than 11 million maritime containers arrive at U.S. seaports. At the Nation's land borders, another 10 million shipments arrive by truck, and 3 million arrive by rail. An additional quarter billion cargo, postal, and express consignment packages arrive by air. This section of the Strategic Plan outlines mechanisms to enhance the Nation's ability to stem illicit trade in the form of counterfeit and pirated products by improving identification and interdiction mechanisms, enhancing the operational efficiency of customs authorities, and securing institutional commitments to explore new ways of carrying out day-to-day business. The section advocates the promotion of collaborative efforts among domestic and international stakeholders to maintain pace with the evolution of deceptive tactics used by illicit actors to exploit shipping channels and economically significant trading zones.

SECTION 4 examines broader IP enforcement strategies that bridge both online and trade-based threats, focusing on overarching governmental frameworks and policies that are critical to supporting robust intellectual property enforcement efforts in a rapidly changing environment. As the threats to effective IP enforcement continue to evolve and migrate across borders, opportunities exist to support modern administrative frameworks, such as a "whole of government" model and a "specialized office" approach to IP enforcement, to provide a more effective and agile response to IP-based illicit activity. This section further outlines enhancements to strategic international engagements, including, for example, supporting the capabilities of other governments to engage in effective IP enforcement. This section of the Strategic Plan also highlights the role of effective trade policy and enhanced transparency and predictability in global markets.

While seeking to be thorough, the Strategic Plan does not attempt to provide an exhaustive analysis of all concerns that might be implicated by the unlawful misappropriation or use of intellectual property in all its forms. The issues are vast and constantly evolving in scope and complexity, and additional work will be required to continue to further develop and advance the direction laid out in this Strategic Plan. The U.S. Interagency Strategic Planning Committees on IP Enforcement have focused on collecting information and empirics to fashion and implement effective IP enforcement strategies, so we collectively can do more of what works and less of what does not work. In doing so, we are mindful that the Joint Strategic Plan may identify some problems with no immediately clear or comprehensive solution. In those instances, the problem-definition process should be viewed as a useful step to generate innovative thinking and solutions over the life of the plan.

A Note on Copyright Infringement

The term "piracy" describes the misappropriation and unlawful infringement of protected works, such as movies, television broadcasts, music, books, and other creative works. Without proper context, piracy may be misconstrued in the policy arena. For purposes of this Strategic Plan, discussions around "piracy" in the digital environment are focused on large-scale illicit business models that have been designed to intentionally and unlawfully infringe third-party copyrighted content, often for commercial gain. The Strategic Plan does not propose broad Federal enforcement in order to address any and all acts that may be deemed infringing. Rather, the Strategic Plan focuses more narrowly on actors that engage in a deliberate targeting and unlawful infringement of protected works. The Strategic Plan also calls attention to large-scale infringement on legitimate online platforms by illicit actors, and the need for new strategies and enhanced corporate leadership to address such acts.

Nothing herein should be interpreted as limiting the scope of exceptions and limitations, such as fair use, under U.S. copyright law. To the contrary, the basic principles that have permitted the Internet to thrive must be safeguarded, and the Strategic Plan expressly recognizes and celebrates advancements in technology. The way people use and access content – which has led to new and innovative uses of media (*e.g.*, remixes and mashups involving music, video and the visual arts), and fair use, for example – will undoubtedly continue to evolve. We must work to foster creativity, understanding the role of exceptions and limitations as not only part of our body of laws, but as an important part of our culture. Indeed, it is the combination of strong copyright rights with a balance between the protection of rights and exceptions and limitations that encourages creativity, promotes innovation, and ensures our freedom of speech and creative expression are respected.

IP enforcement options must be crafted to allow for effective measures against actors that unlawfully prey on the works of rights holders, while ensuring that enforcement activities do not affect lawful activity.

Enhanced Private Sector Leadership and Public-Private Collaboration

Legitimate actors in the trade environment operate under the principle that the criminal exploitation of their respective businesses' services or platforms is unacceptable. No business, however, is immune to such exploitation of its services, and no single entity or industry can effectively tackle these threats alone. The digital age has altered the manner in which syndicates can and do work to inflict serious harm (from selling fake medicines or automotive air bags online to delivering malware to unsuspecting online shoppers), including through the exploitation of intermediary services and platforms. In light of the seriousness and magnitude of the illicit activities in the online and traditional environments, enhanced private sector leadership remains important to ensure a sustained and focused approach to minimize these growing threats.

This Strategic Plan has identified numerous circumstances where enhanced non-governmental leadership and public-private sector collaborations may yield beneficial results. Over the past few years, for example, several private-sector-led collaborative partnerships have emerged—comprised of leading Internet service providers, content producers, and brand owners, payment processors, advertisers, and ad networks, domain name registries, and others—with the laudable goal of minimizing the criminal exploitation of a business's services or platforms by syndicates perpetrating consumer frauds and other illicit activities.

The Office of the Intellectual Property Enforcement Coordinator has worked to facilitate and support innovative private partnerships and voluntary stakeholder initiatives such as these. These new and evolving partnerships bring relevant private sector entities together to assess and share achievements realized against third-party exploitative acts, as well as to explore the possibility of strengthened government-private collaboration and industry-led voluntary initiatives in the marketplace. Some examples of these collaborations and initiatives include:

- **An E-Commerce Marketplace Initiative,**[*] a collaboration between the FBI and third-party online marketplaces, payment processors, and online advertising systems and platforms, ensures that appropriate analytical tools and techniques are in place to mitigate the manufacture, distribution, advertising, and sale of counterfeit products.

- **Centers of Excellence and Expertise (Centers),**[†] launched by CBP, support enhanced industry outreach and collaboration on intellectual property and other enforcement matters by focusing on industry-specific issues across ten unique trading environments. The Centers are organized along the following industry sectors: Agriculture & Prepared Products; Apparel, Footwear & Textiles; Automotive & Aerospace; Base Metals; Consumer Products & Mass Merchandising; Electronics; Industrial & Manufacturing Materials; Machinery; Petroleum, Natural Gas & Minerals; and Pharmaceuticals, Health & Chemicals.

- **The Center for Safe Internet Pharmacies (CSIP),**[‡] a nonprofit organization founded in 2011 by a group of Internet service providers and technology companies addresses the global problem of consumer access to illegitimate pharmaceuticals from illegal online pharmacies and other sources. CSIP and its members work to provide consumers and medical professionals with ways to verify online pharmacies, to report illegal online pharmacies or counterfeit pharmaceutical products, and to become educated about these issues. CSIP also collaborates with global law enforcement in support of efforts to end the threat of illegal online pharmacies.

- **Domain Name Registry Best Practices,**[**] launched in partnership with the Motion Picture Association of America (MPAA) and the Donuts and Redix domain name registry platforms, works to promote a safe and secure domain name system. Under the program, a "trusted notifier" system has been established as part of collaborative efforts to mitigate blatant and pervasive illegal online activity in violation of platform terms of service.

- **The Center for Copyright Information (CCI),**[††] a collaboration between the content creators and certain Internet Services Providers (ISPs), seeks to educate consumers about the importance of copyright protection through an innovative Copyright Alert System (CAS) that notifies ISP subscribers when their accounts have been identified as involving illegal activity.

- **Payment Industry Best Practices,**[‡‡] established by leading credit card and payment processing companies, provide an identifiable complaint mechanism and procedures for withdrawing payment services to websites engaged in illicit IP-based activity, including content theft and counterfeiting.

[*] *See* Department of Justice, *"Justice Department Announces New Strategy to Combat Intellectual Property Crimes"* (October 2, 2015), accessed from: https://www.justice.gov/opa/pr/justice-department-announces-new-strategy-combat-intellectual-property-crimes-and-32-million; Federal Bureau of Investigation, "*Countering the Growing Intellectual Property Theft Threat: Enhancing Ties Between Law Enforcement and Business*" (January 22, 2016), accessed from: https://www.fbi.gov/news/stories/countering-the-growing-intellectual-property-theft-threat.

[†] See CBP, "*Centers of Excellence and Expertise,*" accessed from: https://www.cbp.gov/trade/centers-excellence-and-expertise-information.

[‡] For more information, see The Center for Safe Internet Pharmacies at https://safemedsonline.org/.

[**] See, e.g., Castro, Daniel. The Hill. "*Industry Cooperation Takes Another Step In Fighting Online Piracy*" (March 3, 2016), accessed from: http://thehill.com/blogs/pundits-blog/technology/271587-industry-cooperation-takes-another-step-in-fighting-online; see also Motion Picture Association of America, "*Donuts and the MPAA Establish New Partnership to Reduce Online Piracy,*" (February 9, 2016), accessed from http://www.mpaa.org/wp-content/uploads/2016/02/Donuts-and-MPAA-Establish-New-Partnership-2.9.16.pdf, and "*Radix and the MPAA Establish New Partnership to Reduce Online Piracy,*" (May 13, 2016), accessed from http://www.mpaa.org/wp-content/uploads/2016/05/Radix-and-the-MPAA-Establish-New-Partnership-to-Reduce-Online-Piracy.pdf.

[††] For more information, see The Center for Copyright Information at http://www.copyrightinformation.org/.

[‡‡] *See* The White House, "*2013 Joint Strategic Plan on Intellectual Property Enforcement,*" at p. 36, accessed from https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

- **Advertising Best Practices**[§] which have continued to evolve over the past few years, strive to protect the integrity of the digital advertising system as well as third-party content and brands by preventing the flow of advertising dollars to websites that are engaged in illicit activity, including content theft and counterfeiting. Building on pledges made by the advertising community in recent years, a new voluntary initiative has been launched to further reduce advertising revenue from illicit sites.[**] Through this and other industry-led initiatives, many of the world's largest brand advertisers and agencies have committed to taking aggressive steps to keep their digital ads off infringing sites and to better ensure that their brands will not be associated with illicit activity.[††]

These and other collaborations and initiatives operate with a sense of purpose to promote a marketplace that provides an enhanced level of protection to consumers and legitimate businesses. One advantage of voluntary initiatives is their ability to adapt quickly to changes in the rapidly-evolving marketplace and craft agreements and initiatives that are responsive to marketplace developments. By making it more difficult for illicit actors to operate without consequence, these and other initiatives are improving the marketplace.

How Will Solutions be Evaluated and Success Measured?

The Federal Government must strive to implement results-oriented strategies that measure success by documenting progress. The Federal Government must improve agency efficiencies and resource allocations, employ administrative and policy levers to drive more effective evidence-based IP enforcement practices, and enhance public understanding of the dimensions of the issues.

Good government programs use a broad range of analytical and management tools, which collectively comprise an "evidence infrastructure," to learn what works (and what does not), for whom and under what circumstances it works (or does not), as well as to improve results. Evidence can be quantitative or qualitative and may come from a variety of sources, including performance measurement, evaluations, statistical studies, retrospective reviews, and other data analytics and research.[*]

In the IP enforcement environment, there are a number of challenges to measuring progress in minimizing illicit trade in counterfeit and pirated goods, large-scale commercial infringement of copyrights, trade secret misappropriation, and other acts of IP infringement. Attempts to approach the appraisal from a quantitative fashion—that is, by statistics or mathematical techniques—remain important, but can be limiting.

For example, IP misappropriation and other illicit activities are dynamic in nature, rapidly changing and taking different forms, resulting in measurement data that is often of no prospective use by the time it can be collected. With respect to the data itself, there is a need to make more data from the government and private sectors available in order to enhance analysis of the state of the marketplace. Additionally, the multidimensional nature of illicit IPR-based activities complicates marketplace assessments. For example, is an increase in product seizure numbers indicative of higher performance in targeting and interdiction of counterfeit goods; or the result of a higher volume of illicit trade in counterfeit goods; or due to the ineffectiveness of other "upstream" initiatives to reduce illicit trade in the first instance; or all of the above?

[§] *Id.* Since the issuance of the Joint Strategic Plan, leading ad networks announced in July 2013 certain "Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting," and the Interactive Advertising Bureau (IAB) updated its "Network and Exchange Quality Assurance Guidelines" to include a ban on selling ad inventory on "copyright infringement" sites. In June 2014, the IAB also announced its Trustworthy Digital Supply Chain Initiative, identifying fighting online piracy as one of its five objectives, along with eliminating fraudulent traffic, combatting malware, and promoting brand safety. *See* IAB, "*Winning the War on Crime in the Supply Chain*," *available* at http://www.iab.net/iablog/2014/06/Trustworthy-Digital-Supply-Chain.html.

[**] The Trustworthy Accountability Group (TAG) was created by the American Association of Advertising Agencies (4A's), Association of National Advertisers (ANA), and Interactive Advertising Bureau (IAB) to work collaboratively with companies throughout the digital ad supply chain, and combat ad-supported Internet piracy. *See* TAG, http://www.tagtoday.net/aboutus/.

[††] *See* TAG, "*Largest Brands And Agencies Take TAG Pledge To Fight Ad-Supported Piracy For All Digital Ads*," (December 2015), accessed from https://www.tagtoday.net/largest-brands-and-agencies-take-tag-pledge-to-fight-ad-supported-piracy-for-all-digital-ads/ (noting that many of the world's largest brand advertisers and agencies have pledged to require their ad partners "to take aggressive steps to help fight the $2.4 billion lost to pirate sites each year").

[*] To learn more about evidence-based approaches, see The White House, "*2017 Budget of the United States Government: Analytical Perspectives, Chapter 7: Building the Capacity to Produce and Use Evidence*," accessed at https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/ap_7_evidence.pdf.

To address these and other challenges, the U.S. Interagency Strategic Planning Committees on IP Enforcement have issued calls for research both as part of the development process for the Joint Strategic Plan and in the Strategic Plan itself, while encouraging appropriate public disclosure of more data to support evidence-based IP enforcement efforts (see below).

EXCERPT OF FEDERAL REGISTER NOTICE

Request for Public Comments: Development of the Joint Strategic Plan on Intellectual Property Enforcement

"[I]n an effort to aid the development and implementation of well-defined policy decisions, to advance scholarly inquiry, and to bolster transparency and accountability on intellectual property enforcement efforts, IPEC encourages enhanced public access to appropriately generalized information, trend analyses, and case studies related to IP-infringing activities. Both governmental and private entities may be in possession of a wide range of data and other information that would enable researchers, rights holders, industry-at-large, public interests groups, policy makers and others to better gauge the specific nature of the challenges; develop recommendations for well-balanced strategies to effectively and efficiently address those challenges; and measure the effectiveness of strategies that have been or will be adopted and implemented. To further the objective of supporting transparency, accountability, and data-driven governance, IPEC requests identification of possible areas for enhanced information sharing and access, including the identification of relevant data sets, and how best to improve open access to such data."

Source: Federal Register, 80 FR 52800; Doc. No. 2015-21289.

These calls for research and enhanced public availability of data represent a key element of this Joint Strategic Plan, and of the long-term success of an effective IP enforcement regime.

The IPEC, along with the U.S. Interagency Strategic Planning Committees on IP Enforcement, will continue to develop appropriate performance measures to evaluate the impact of Federal initiatives on intellectual property enforcement. Furthermore, the Office of the Intellectual Property Enforcement Coordinator will monitor progress made under the Joint Strategic Plan by way of an *Annual Report on Intellectual Property Enforcement*, to be submitted to the Committee on the Judiciary and the Committee on Appropriations of the U.S. Senate, and the Committee on the Judiciary and the Committee on Appropriations of the U.S. House of Representatives, pursuant to Section 304 of the PRO-IP Act of 2008, 15 U.S.C. § 8814.


SECTION

1

THE GLOBAL SCALE OF INTELLECTUAL PROPERTY THEFT AND ITS UNLAWFUL EXPLOITATION BY THIRD PARTIES POSES SERIOUS THREATS TO U.S. NATIONAL INTERESTS.



SECTION 1 CONTENTS

THE GLOBAL SCALE OF INTELLECTUAL PROPERTY THEFT AND ITS UNLAWFUL EXPLOITATION BY THIRD PARTIES POSES SERIOUS THREATS TO U.S. NATIONAL INTERESTS

A. The Economic Scope and Magnitude of Counterfeiting, Commercial Piracy, and Trade Secret Theft: A Global Perspective 19

1. Assessments of the Scale and Economic Impact of Counterfeiting and Commercial Piracy 20
2. Assessments of the Scale and Economic Impact of Trade Secret Theft 21

B. The Complex and Sophisticated Nature of Commercial Piracy, Counterfeiting and Trade Secret Theft in the Modern Era 21

1. Schemes Employed for the Unlawful Exploitation of Digital Content 21
2. Schemes Employed to Facilitate Illicit Trade in Counterfeit Goods 26
3. The Targeting and Theft of Trade Secrets 31

C. The Theft and Unlawful Exploitation of Intellectual Property as Threats to U.S. National Interests 32

1. Undermines Principles of Fair Trade in the Global Economy 32
2. Threatens Consumer Health and Safety 33
   - *Example: Counterfeit Personal Care Products* 33
   - *Example: Counterfeit Consumer Electronics & Electrical Products* 34
   - *Example: Counterfeit Pharmaceuticals* 35
   - *Example: Counterfeit Automotive Parts* 37
3. Threatens the Environment 38
4. Exploits Labor 39
5. Poses Threats to Domestic and International Security 40
   - a. The Integrity of Supply Chains and Critical Infrastructures 41
   - b. The Convergence between Intellectual Property-Based Crime and the Financing of Criminal and Terror Networks 42



INTRODUCTION

The story of intellectual property (IP) is a story of economic growth, high-paying jobs, economic competitiveness, innovation and creative expression. "The entire U.S. economy relies on some form of IP, because virtually every industry either produces or uses it."[1] According to a 2016 U.S. Department of Commerce report[2] on the role of IP in the U.S. economy, IP-intensive industries:

Account for **$6.6 trillion in value added**, or more than **38 percent of U.S. GDP**

Account for over **52 percent** of all U.S. merchandise exports

Support directly over 27 million jobs, and indirectly over 17 million jobs, for a **total of 45.5 million jobs** or **30 percent of all U.S. employment**

Support average weekly wages that are **46% higher** than in other industries. (In patent and copyright industries, wages were 74 and 90 percent higher, respectively)

Source: U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: 2016 Update" (Sept. 2016)

These figures demonstrate the extraordinary role of IP in our economy.

In addition to being a major driver of U.S. economic growth, IP provides the incentive to create, invest in, and commercialize new inventions, products, and services, while supporting artists and authors in disseminating their works, be it literary, artistic, musical, cinematic, or other creative forms of human expression. As President Obama stated on World Intellectual Property Day in 2016, "Whether through the music or movies that inspire us, the literature that moves us, or the technologies we rely on each day, ingenuity and innovation serve as the foundations upon which we will continue to grow our economies and bridge our cultural identities."[3] Together, innovation and creativity, and the IP structure that appropriately balances the creation of new works with

the protection of existing ones, are critical to our economic and cultural life.

Along with this remarkably positive story of economic growth, ingenuity, and creative expression is the growing scope of IP theft and the harms that flow from the unlawful exploitation of IP by third parties. This introductory section of the Joint Strategic Plan on Intellectual Property Enforcement ("JSP" or "Strategic Plan" or "Plan") provides an overview of the current landscape of IP enforcement challenges that the creative and innovative communities—as well as policymakers and law enforcement authorities—face.[4]

This national strategy on intellectual property enforcement—the Joint Strategic Plan—is required by Federal statute.[5] That statute makes explicit that one of the key objectives of the Plan is **"[i]dentifying and addressing structural weaknesses, systemic flaws, or other unjustified impediments to effective enforcement action against the financing, production, trafficking, or sale of counterfeit or infringing goods."**[6] This Strategic Plan seeks to do that in detail.

Understanding these threats and impediments to effective IP enforcement at the macro-level—that is, their global scope and magnitude—and at the micro level—the nature of the complex schemes used by illicit actors to accomplish IP theft on a commercial scale—is essential. That understanding is important for the development and implementation of an effective strategy to minimize the unlawful exploitation and theft of IP and the harms that stem from such activities. The nature of these threats and harms should be well-documented, and our knowledge of them must continue to grow through research, information-sharing, and data analysis with each issuance of a new Joint Strategic Plan over the years to come. In this sense, the Plan represents part of a continuous process. Moreover, as technology continues to evolve, the Federal Government remains attentive to ensuring that lawful activities are not inadvertently captured by an otherwise necessary and robust IP enforcement system.[7] A system that encourages innovation and minimizes unintended consequences as technology evolves also helps to identify the illicit actors who might seek to exploit IP and infringe American products.

As discussed below, the collective weight of research and reporting establishes that the global scope and magnitude of counterfeiting, commercial piracy, and trade secret theft are staggering. As discussed below, one international organization estimates that international trade in counterfeit and pirated goods now constitutes 2.5 percent of world trade, while the recent targeting and theft of trade secrets from American industry has been described as representing "the single greatest transfer of wealth in history."[8]

> "[T]he value of theft of intellectual property from American industry… represents the single greatest transfer of wealth in history."
>
> *Gen. Keith Alexander (Ret.), former Director, National Security Agency, and Commander, U.S. Cyber Command*

An investigation into the schemes and tactics used by the illicit actor may tell us what the overall size of the problem represents. At the micro-level, it is important to understand that entities that target and exploit IP rights employ a wide range of complex schemes to generate illicit profits and evade law enforcement detection.

For example, illicit business models that infringe and exploit copyrighted content are often deliberately structured to conceal identities; to create redundancies so as to ensure operational resiliency in the face of enforcement actions; and to maximize dissemination of the unauthorized third-party content by various means described below. Business models centered on counterfeit trade often rely on manufacturing "safe havens;" the manipulation of trade routes with circuitous intermediary transit points; exploitation of Free Trade Zones; adoption of product concealment methods; fraudulent sales tactics; and opaque distribution structures, in order to deliver fake products to the market.

> Today, everything that can be faked, is being faked—*from food and beverages to personal care products; automotive parts to medicines; fertilizers to consumer electronics; software to footwear and apparel; toys to critical technologies*—subjecting consumers to greater instances of fraud and risks to health and safety than ever before.

And as these dynamic threats continue to evolve and migrate across borders, we must not overlook the

attendant harms and adverse social impacts that flow from the unlawful exploitation and theft of IP assets. Too often, the harm of unlawful exploitation and theft of IP is mischaracterized as limited to a narrow private interest, such as a loss of a potential sale, loss of corporate goodwill, or loss of a technological or competitive advantage. These harms are not the full picture. **The theft and unauthorized exploitation of intellectual property rights by operators of illicit businesses evokes a host of broader negative impacts to the national economy and the general public welfare.** These attendant financial and social harms must be a part of the analysis and understanding of the harms tied to the unauthorized exploitation and theft of IP.

When IP-based exploitative practices go unabated in the aggregate, fair competition in world markets is undermined, productivity is jeopardized, investment in research and development is dis-incentivized, the job market is threatened, and the creative and innovative sectors are weakened. Trade in counterfeit and pirated goods also compromises the integrity of domestic and global supply chains; introduces significant public health and safety risks; contributes to corruption of government institutions; subverts human rights by reliance on forced labor, child labor, and unsafe working conditions; and generates environmental harms caused by unregulated manufacturing practices or the use of substandard products. The growth in IP crime is fueled by sophisticated criminal syndicates exploiting new technologies and lack of effective coordination among governments.[9] The impact of these and other harms are not limited to developed economies, rather they are often disproportionately felt by developing countries (for example, manufacturers of counterfeit medicines and other goods target countries with less developed regulatory structures), necessitating leadership and collaboration from the international community—both from the public and private sectors—to address effectively these serious threats.[10]

Raising public awareness and elevating a common understanding of the issues through a detailed and empirically-based message that provides a clear understanding of the issues is a prerequisite to constructing and implementing an effective solution to the problem. Thus, the Strategic Plan begins with a detailed account of the landscape of the problem so that the policies and proposed responses detailed in the remaining sections of the Plan can be read in proper context.

A. THE ECONOMIC SCOPE AND MAGNITUDE OF COUNTERFEITING, COMMERCIAL PIRACY, AND TRADE SECRET THEFT: A GLOBAL PERSPECTIVE.

Precise quantification and measurement of the global reach and economic scale of counterfeiting and commercial piracy, and the losses attributable to trade secret theft, can prove elusive. Such assessments have proven challenging because counterfeiting and commercial-scale piracy are illicit activities, making data on such activities and their impact inherently difficult to obtain. Furthermore, the Government Accountability Office (GAO) identified the inherent difficulties in measuring the monetary value of non-public, sensitive information in its report *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods.*[11] Both the GAO and Congressional Research Service found that victims of trade secret theft often do not report the theft, thereby limiting the amount of available information that might allow researchers to quantify the impact of trade secret theft.[12]

> "[E]ven if precise assessments [of illicit activities] 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."
>
> *Source: World Economic Forum's Global Agenda State of the Illicit Economy (October 2015)*

Over the years, industry, researchers, and policymakers alike have made efforts to address these challenges by assessing developments and trends across various sectors and economies and by establishing a more rigorous analytical framework to improve economic modeling to measure the overall magnitude of counterfeiting, piracy, and trade secret theft. Further study, however, remains necessary and analysts have not identified any single approach that quantifies these activities fully; Section IV of this Joint Strategic Plan calls for additional research into this and many other topics

in IP enforcement. Still, the collective weight of research and reporting to date establishes that the global scope and costs of counterfeiting, commercial piracy, and trade secret theft are staggering, and continue to threaten substantial national interests.

1. Assessments of the Scale and Economic Impact of Counterfeiting and Commercial Piracy.

One of the most comprehensive attempts to quantify the impact of counterfeiting and pirated goods from the past decade was issued in 2008, and updated in 2009, by the Organization for Economic Cooperation and Development (OECD), an international organization comprised of the United States and 33 other countries from North and South America, Europe, and Asia-Pacific. The OECD report focused on trade involving counterfeit and pirated tangible (hard) goods. In its 2008 Report, the OECD estimated that "international trade in counterfeit and pirated goods could have accounted for up to USD 200 billion in 2005," and in the 2009 Update, the OECD stated that "counterfeit and pirated goods in international trade could have amounted for up [to] USD 250 billion in 2007."[13]

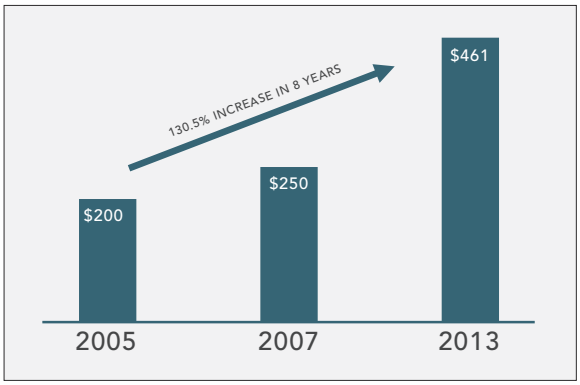
In 2016, with improved methodologies based on updated data sets and seizure statistics from various customs agencies, the OECD issued a new report revising the global estimate of international trade in counterfeit and pirated goods. The 2016 OECD Report stated that "**as much as 2.5% of total world trade in 2013 was in counterfeit and pirated products.**" This was "a significant higher volume" than the percentage of counterfeit and pirated goods in 2005 (1.9% of world trade) and in 2007 (1.8% of world trade). And, in some countries, the percentage of counterfeit and pirated products was higher.[14]

More specifically, the 2016 OECD Report concluded that "[t]he best estimates of this study, based on the data provided by customs authorities, indicate that **counterfeit and pirated products accounted for as much as USD 461 billion in world trade in 2013.**"[15]

A comparison of the 2008/2009 and 2016 OECD Reports demonstrates that the magnitude of the problem is large and growing. Indeed, as the 2016 OECD Report indicates, trade in counterfeits now represents a significant portion of total international trade.

These figures, as significant as they are, represent only a part of a larger problem. As noted above, the

FIG. 1: Annual Est. Max. Value of Counterfeited and Pirated Goods ($ billions).



Source: OECD Reports (2008. 2009, and 2016)

quantitative estimates in the 2008/2009 and 2016 OECD Reports do not include (1) any domestically-produced-and- consumed counterfeit or pirated products, and (2) digital trade in pirated products (online piracy). According to the 2008 OECD Report, if these categories were also included, "the total magnitude of counterfeiting and piracy worldwide could well be several hundred billion dollars more."[16]

Another oft-cited report, published in 2011 by the International Chamber of Commerce (ICC), estimated the total global economic value of counterfeit and pirated products to be **as high as $650 billion** in 2008, when including the categories that had been excluded in the 2008 OECD report. Furthermore, the 2011 ICC report posited that international trade may account for more than half of the estimated value of counterfeiting and piracy (between $285-$360 billion), with domestic production and consumption adding between $140-$215 billion, and digitally-pirated music, movies, and software adding another $30-$75 billion in losses to the creative and innovative industries. Looking ahead, the 2011 ICC report projected that, in 2015, the total magnitude of counterfeiting and piracy could be **between $1.22 trillion and $1.77 trillion**.[17]

Considering that the 2016 OECD report places the international trade in counterfeit and pirated goods at nearly half a trillion dollars annually (excluding all domestically-produced-and-consumed counterfeit and pirated goods, as well as online piracy), the OECD and ICC estimates together suggest that the total magnitude of counterfeiting and piracy worldwide in all forms appears to be approaching, if not surpassing, the trillion dollar mark.

2. Assessments of the Scale and Economic Impact of Trade Secret Theft.

The protection of trade secrets is critical to protecting the fruits of American labor, ensuring that American businesses have an incentive to innovate, and enabling continued economic prosperity in a technology-driven age.[18] Trade secrets are estimated to be worth $5 trillion to American businesses.[19]

The magnitude of trade secret theft is substantial, and the frequency appears to be increasing. The Center for Responsible Enterprise and Trade, for example, conducted a study relying on surrogate indicators and leveraged multiple studies on illicit economic activity in an effort to quantify the impact of trade secret theft. It estimated the theft to be in the range of 1 to 3 percent of U.S. GDP.[20] Reports from the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Commission on the Theft of American Intellectual Property have placed the estimated losses to the U.S. economy from trade secret theft at tens to hundreds of billions of dollars annually.[21]

According to the U.S. Department of Justice, "billions of U.S. dollars are lost annually to foreign competitors who pursue unlawful commercial short cuts" by stealing U.S. innovation and technology.[22] Notwithstanding the difficulties of criminal and civil prosecution due to the international dimensions often associated with trade secret theft, cases that have been successfully prosecuted to completion (*see sidebar* as an example) give an insight as to the significant damages to which U.S. businesses may be exposed when their trade secrets are targeted.

United States v. Kolon

In 2015, Kolon Industries Inc., a South Korean industrial company, pleaded guilty to conspiracy to steal E.I. DuPont de Nemours & Co.'s trade secrets for making Kevlar, a high-strength, para-aramid synthetic fiber that is used for a wide range of commercial applications such as body armor, fiber optic cables, and automotive and industrial products. The defendant was sentenced to pay $360,000,000 in criminal fines and restitution.

Source: United States v. Kolon, Case No. 3:12-cr-00137 (E.D. Va)

Beyond the direct economic losses that may result to businesses and the economy, *cyber-enabled* trade secret theft poses a number of additional dangers and accompanying costs. For example, personally identifiable information (PII), payment data, and personal health information (PHI) may be compromised along with intellectual property assets that are targets of cyber-enabled espionage. In these circumstances, a wide range of direct and intangible costs may increase the overall impact of the cyber incident. These may include so-called "above the surface" costs—such as costs associated with technical investigations, customer breach notifications, post-breach customer protection, regulatory compliance, public relations, *etc.*—to "beneath the surface costs"—such as insurance premium increases, operational disruptions, damage to customer relationships, value of lost contract revenue, increased cost to raise debt, *etc.*[23]

The theft of trade secrets adversely affects entities of all sizes, including small- and medium-sized enterprises (SMEs). In fact, SMEs may rely more heavily on trade secrets than on other forms of intellectual property, as the costs of obtaining and maintaining a patent, coupled with the costs of patent litigation, often make it more financially viable for smaller businesses to depend primarily on trade secrets.[24]

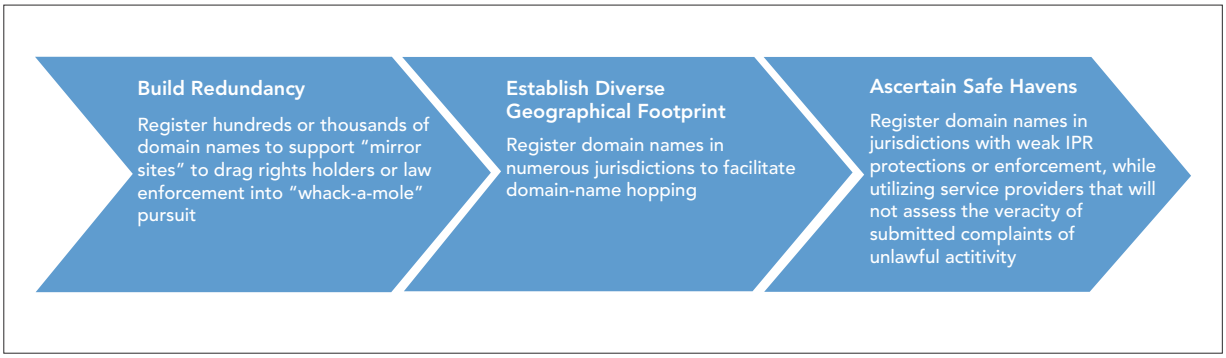
B. THE COMPLEX AND SOPHISTICATED NATURE OF COMMERCIAL PIRACY, COUNTERFEITING AND TRADE SECRET THEFT IN THE MODERN ERA.

In addition to understanding the economic impact of IP theft, effective IP enforcement policy—for the protection of rights holders and consumers alike—requires an understanding of the schemes and day-to-day tactics used by those who unlawfully exploit copyrighted content, brands, patented inventions, and trade secrets.

1. Schemes Employed for the Unlawful Exploitation of Digital Content.

Public reporting offers a window into the various methods entities employ to unlawfully exploit copyrighted content such as movies, music, video games, books, and software in the digital environment to minimize detection and to generate commercial profit.

FIG. 2: IPR-Infringing Websites: Tactics Used to Build Resilience Against Enforcement Activity.



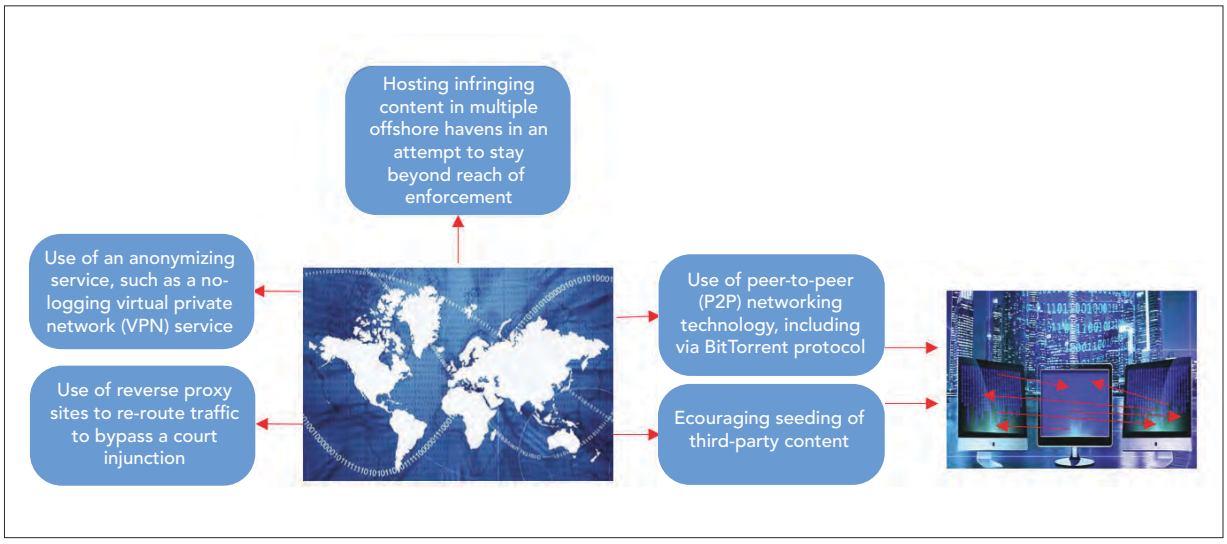
For example, a study commissioned by the European Union Intellectual Property Office (EUIPO), through the European Observatory on Infringements of Intellectual Property Rights, identified various infringement-based business models employed to intentionally benefit from and exploit copyrighted digital content on the Internet, including by way of linking, torrent, streaming, and cyberlocker sites.[25] The illicit online business models appear to be structured to achieve three primary objectives: (i) to shield and conceal identities; (ii) to establish operational redundancies so as to ensure resiliency in the face of enforcement actions; and (iii) to maximize dissemination of infringing third-party content. Examples of some of the tactics employed to realize these objectives are summarized below.

Entities engaged in the unlawful exploitation of copyrighted content are reported to conceal or otherwise mask identifying information by providing false or inaccurate registration information when registering a domain name.[26] An operator of a website engaged in illicit activity may also employ one or more evasive registration tactics (FIG. 2,3) such as the registration of hundreds of names across various jurisdictions, in order to increase resilience against any enforcement actions directed at the illicit enterprise.[27]

Once domain names have been secured, reporting suggests that the entity seeking to exploit unlicensed third-party content for commercial profit often employs various additional hosting and operational schemes (FIG. 3) in an attempt to shield the illicit enterprise from effective enforcement.

Illicit actors use legitimate encrypted technologies and proxy connections such as the TOR browser and virtual private networks (VPNs to "cover the tracks" of traffic to an IPR-infringement-based site, attracting individuals seeking to obtain pirated content undetected.

FIG. 3: Evasive Tactics Used to Offer or Access Unlicensed Content.

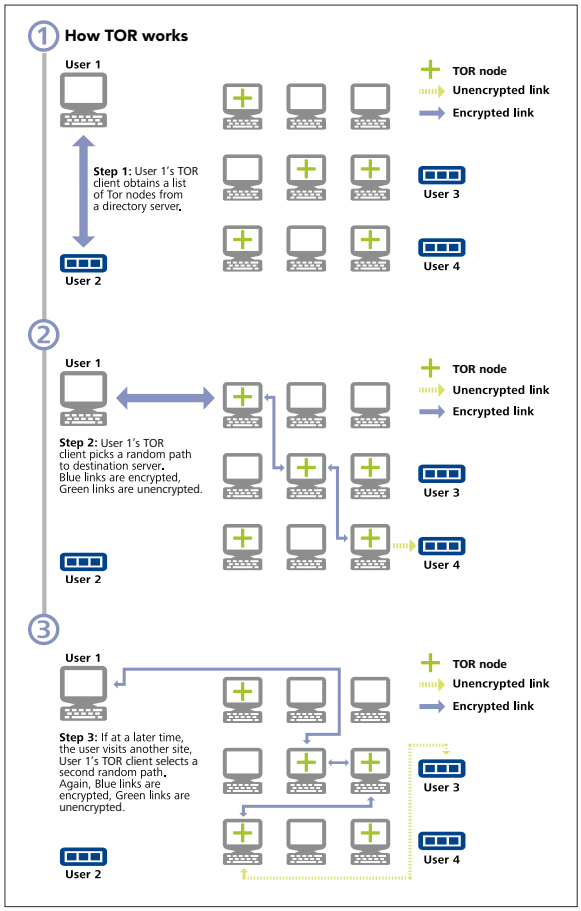


Dedicated IPR-infringing websites have widely promoted torrent VPNs, for example, to anonymize Internet protocol addresses and fake or hide a web user's actual location when accessing libraries of infringing content in violation of applicable laws.[28] Platform operators who facilitate business models predicated on stolen content also develop their business models specifically to evade arrest or civil liability, increase enforcement costs, entice illicit traffic, and generate unreported income for the enterprise and its operators. For these and other reasons, law enforcement actions are often focused on the facilitating platform operator.

These unlawful businesses generate income through a variety of payment methods, including: premium subscription fees and donations; payments in digital virtual currencies (such as Bitcoin, which commercial-scale IP infringers often use to hide the proceeds of crime from the authorities); and revenue from advertisement and pay-per-click services.[29]

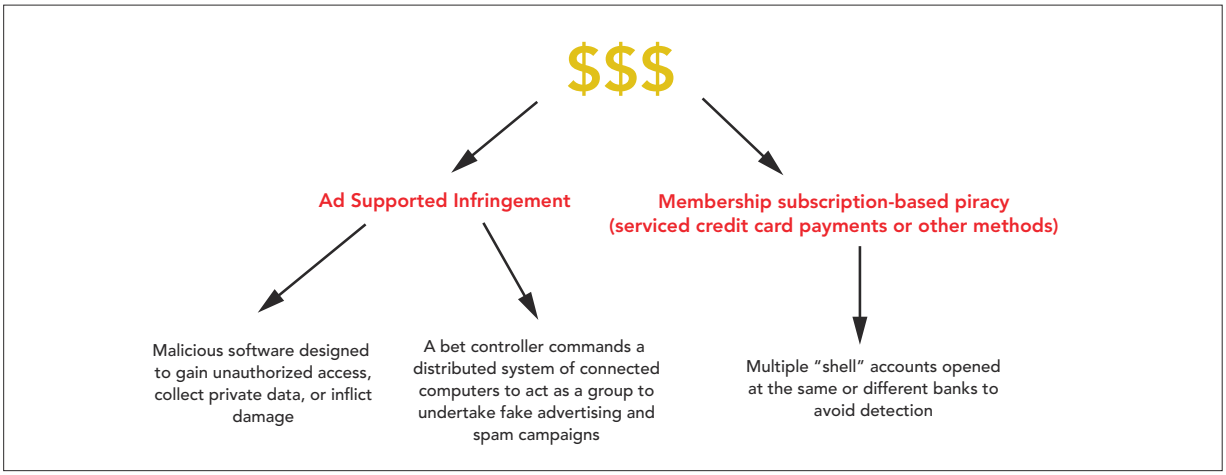
Operators of illicit sites deploy additional strategies to maximize income opportunities and safeguard revenue streams for those seeking to exploit unlicensed content on a commercial scale. For example, websites dedicated to profiting illegally from third-party content have been reported to generate hundreds of millions of dollars each year by exploiting payment processing and advertising network platforms in violation of law, and in material breach of the service provider's and platform's respective "Terms of Service."[30] A number of piracy sites are reported to use the stolen content (such as a hit movie) to lure consumers and then infect consumers' computers with malware in order to conduct other illegal schemes to further augment illicit revenue from the exploited content. Such other schemes include spam and phishing campaigns, accessing personally identifiable data, generation of fake advertising traffic, and the serving of pop-ups and other ads.

FIG. 4: How TOR works.



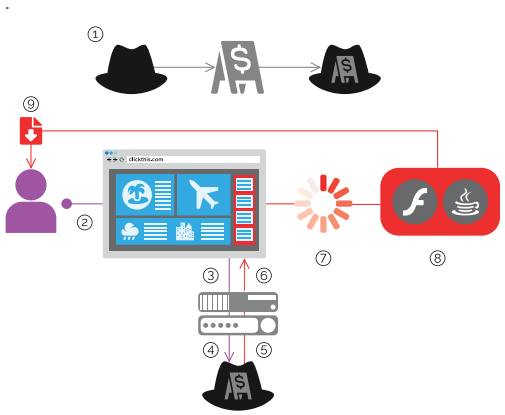
Source: EU IPO, Research on Online Business Models Infringing Intellectual Property Rights (July 2016)

FIG. 5: The Financing of a Commercial Piracy Enterprise.



One recent study, for example, probed a sample of 800 websites dedicated to distributing pirated movies and television shows, and found that *one out of every three* content theft sites contained malware, including delivering adware[31] and botnets.[32] The study found that consumers are *28 times more likely to get malware* from a content theft site than from similarly visited licensed content providers.[33] As such, it has been suggested the unscrupulous website operators exploit IP to "the detriment of society, businesses and the ordinary user of the Internet."[34]

FIG. 6: How Malvertising Works.



1. Attacker registers as an Advertiser with Self-Service Ad Platform
2. User visits website
3. User Targeting Data sent to Ad Platform
4. Impression sold to Attacker
5. Malvertisement served to Ad Platform
6. Malvertisement served to Website
7. Exploit kit loads
8. Vulnerable browser plugins discovered
9. Malware installed on User's device

Source: Digital Citizens Alliance (December 2015)

As an example of how these tactics all come together to perpetrate fraud and permit an actor to engage in commercial-scale criminal exploitation of copyrighted works (FIG. 7): One global organized crime ring registered domain names in 22 different countries in connection with the operation of approximately 10,000 websites, which in turn were hosted in 18 countries around the world, including Canada, Hong Kong, Romania, and the United Arab Emirates.[35] Host locations changed every few minutes by use of an underground service that rotated the websites on computers that were part of a botnet of 450,000 "trojaned" systems, making a single website appear to be hosted in the United States at one moment, only to then appear to be hosted in Singapore at the next moment.[36]

FIG. 7: Example of Global Software Piracy Operation.

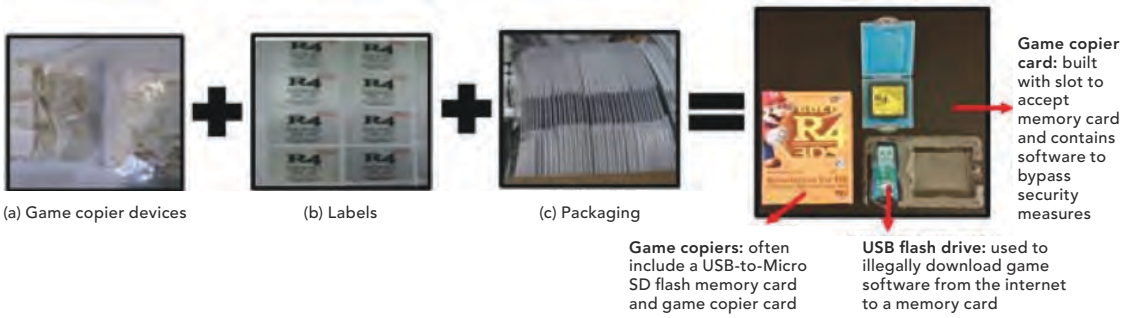


Similarly, the Office of the U.S. Trade Representative (USTR) has noted that Internet-enabled piracy within many countries includes: "pirate servers…that allow users to play unauthorized versions of cloud-based entertainment software; online distribution of software and devices that allow for the circumvention of technological protection measures (TPMs), including 'game copiers' and mod chips that allow users to play pirated games on physical consoles; and set-top or media boxes preloaded with large volumes of pirated content or configured with apps to facilitate access to infringing websites. Piracy facilitated by Internet-based services presents unique enforcement challenges for right holders."[37]

"Game copiers," for example, are unlawful devices openly and knowingly advertised for the purpose of allowing users to make and play unauthorized copies of video games (FIG. 8), depicting popular video game character, on right).

The circumvention devices may be transported to markets around the world through elaborate and deceptive schemes, including by shipping "game

FIG. 8: Example Distribution Tactics of Circumvention Devices to Evade Customs Control.



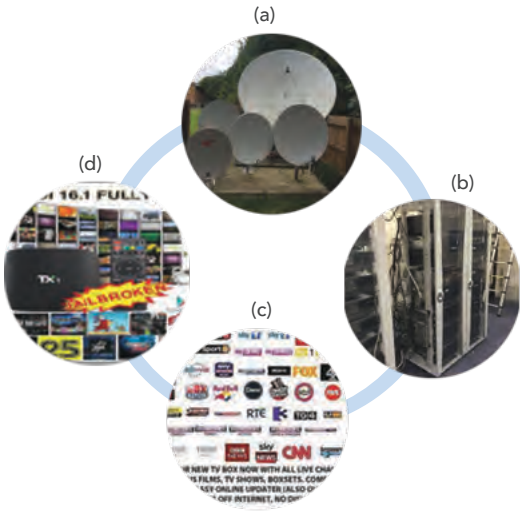
copier" devices in an unmarked, non-labeled condition (FIG. 8, (a)) to minimize detection at the border, with labels and packaging shipped separately (FIG. 8, (b)-(c)), relying on in-country assembly and distribution. These and other deceptive distribution tactics complicate enforcement measures, requiring a combination of enhanced online and global border enforcement strategies.

Emerging trends in the illicit exploitation of television content are equally concerning. Although video content piracy has existed for years in various forms, such as signal piracy and peer-to-peer (P2P) piracy, these activities have historically required some level of technical skill or have been unable to replicate the "lean-back" experience viewers get from watching licensed television programming in their living rooms.[38] Today, plug-and-play devices are readily available, inexpensive, and capable of streaming unauthorized content to one's living room television for an experience virtually identical to watching licensed TV programs.

The market for legitimate premium content via cable, satellite, or Internet television is valued at hundreds of billions of dollars worldwide. This content is delivered via broadband networks, subscription and video-on-demand (SVOD and VOD) providers, such as Netflix, HBO, and Amazon Prime, and pay-per-view sporting and live broadcast events.[39] Criminal networks have begun marketing piracy-enabled set-top boxes (or Internet Protocol Television (IPTV) services) to tap into legitimate content delivery systems while delivering a "lean-back" viewer experience. These set-top boxes are modified with illegal software to enable them to access paid subscription-only channels, including pay-per-view sports, the latest movies, and broadcast television programs; the set-top box operator charges subscribers to access the pirated content at a rate lower than the legitimate content provider (FIG. 9). Consumers have a difficult time identifying piratical IPTV services since many employ professional-looking electronic program guides, artwork, and even free updates.

FIG. 9: Set-Top Box (IPTV) Piracy.

In August 2016, a City of London Police investigation uncovered a large commercial piracy operation involving the worldwide distribution of thousands of illegally modified set-top boxes. The scheme relied on a highly resourced operation employing dozens of satellite dishes (a) and servers (b) to unlawfully scrape and retransmit TV content from broadcast channels (c) to the "pirate" set-top boxes (d).



Sources: See, e.g,, City of London Police Intellectual Property Crime Unit (PIPCU) Press Release, Police Pull The Plug On Illegal International TV Streaming Hub Based In The U.K., August 16, 2016, accessed from: https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Police-pull-the-plug-on-illegal-international-TV-streaming-hub.aspx; See also BBC News, Sale of Kodi "Fully Loaded" Streaming Boxes Faces Legal Test (2016), accessed from: http://www. bbc.com/news/technology-37474595

Piracy continues to evolve with technology, and illicit actors have adapted to continue to evade law enforcement tactics, subjecting artists and the creative communities to economic losses and other harms. As technology continues to advance, new and different forms of digital piracy will likely emerge, generating more problems for copyright owners and creating new technological and legal issues unless appropriate and agile strategic actions are commenced.[40]

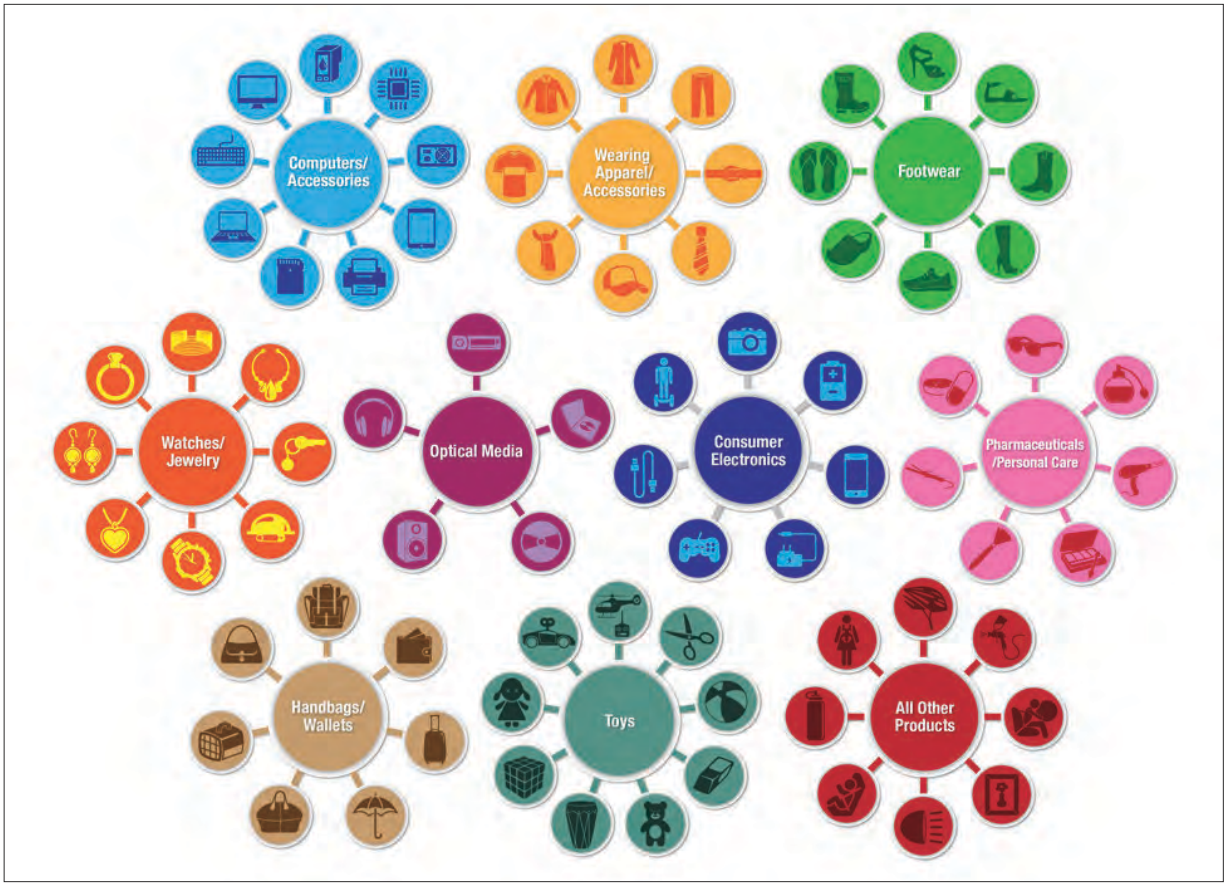
2. Schemes Employed to Facilitate Illicit Trade in Counterfeit Goods.

Whether the intellectual property right at issue is a trademark, copyrighted content, a patented invention or design, a trade secret, or a combination of one or more rights, the illicit trader seeks to misappropriate another's right and investment by producing and/or selling products as if they were genuine (*e.g.*, originating from the rights holder or otherwise authorized, such as by a license agreement).

Along with the advent and many benefits of new technologies, advanced methods of manufacturing and distribution, and the rise of e-commerce, these developments have also enabled counterfeit and pirated goods to become increasingly sophisticated, prevalent, and hard to detect.[41] Counterfeiters invest their resources in high-value products, affecting everyone along the supply chain, from manufacturer, to distributor, to retailer, and ultimately to the consumer.

Products from every industry—from food to personal care products, automotive parts to medicines, electronics to footwear, extension cords to sunglasses, software to jewelry—are being counterfeited today.[42] The U.S. Department of Homeland Security (DHS) seizes counterfeit products in more than 600 different product categories (FIG.10). **Everything that can be faked is being faked, and consumers are often helpless to discern legitimate products from illegitimate ones based on photos on e-commerce sites, or even with the product in hand in traditional brick-and-mortar stores.**

FIG. 10: Diversity of Counterfeit Products in the Marketplace.



Over the past two decades, the supply of counterfeit goods has proliferated, and shifted away from so-called "underground" or secondary markets (e.g., street corners, flea markets) to primary markets, including e-commerce platforms, corporate and government supply chains, traditional retail stores, and other marketplaces where consumers generally pay retail prices and feel confident that they are purchasing genuine goods.[43] Where consumers once were able to identify counterfeit products by relying on "red flag" indicators—such as suspicious location of the seller, sales condition, atypical pricing, or poor quality packaging—consumers are now increasingly exposed to counterfeit products in settings and under conditions where the articles appear genuine.[44] In the primary market, including within the online environment, counterfeit goods so closely resemble the genuine articles that the two are often indistinguishable to the consumer.[45]

Given the complex nature of counterfeiting operations, successful interdiction of smuggled counterfeit goods is difficult and takes time. During that time, the international supply chains are vulnerable. As bad actors continue to adapt to a changing commercial environment, counterfeit activity in all sectors poses risks to industries and governments around the world.

As with the copyright piracy examples discussed above, entities engaged in the trade of fake goods similarly employ a range of intricate methods to drive illicit profits and to attempt to evade detection. The complexity of the networks involved in the manufacturing, distribution, marketing, and sale of fake goods has made IP enforcement difficult. Nonetheless, the consequences of detection are sufficiently great that traders of illicit products in the form of counterfeit goods take calculated measures to reduce risks. Below is a description of a variety of methods syndicates use to facilitate the trade of illicit goods in the form of counterfeit products at various points along the supply chain, from manufacturing to final sale.

Manufacturing

To reduce the risk of having their contraband seized, counterfeiters conduct "just in time" production, minimizing inventories, while storing any finished products ready for shipment in remote warehouses registered to front (sham) companies.[46] Counterfeiters and illicit traders, often with the tacit consent of local government officials, take advantage of "safe haven"-like conditions to manufacture and source a wide variety of fake products.

FIG. 11: Example of False Covering.



During manufacture, counterfeit goods are often disguised by covering over the well-known logo with a peel-away patch or outer covering in order to make it look like a product produced by a lesser-known manufacturer (FIG. 11); by using decoy boxes; or shipping the "blank" product separate and apart from the branded labels, hang tags and similar articles, so that they can be "finished" in the country of consumption, after clearance through customs.[47]

Source/Provenance Economies.

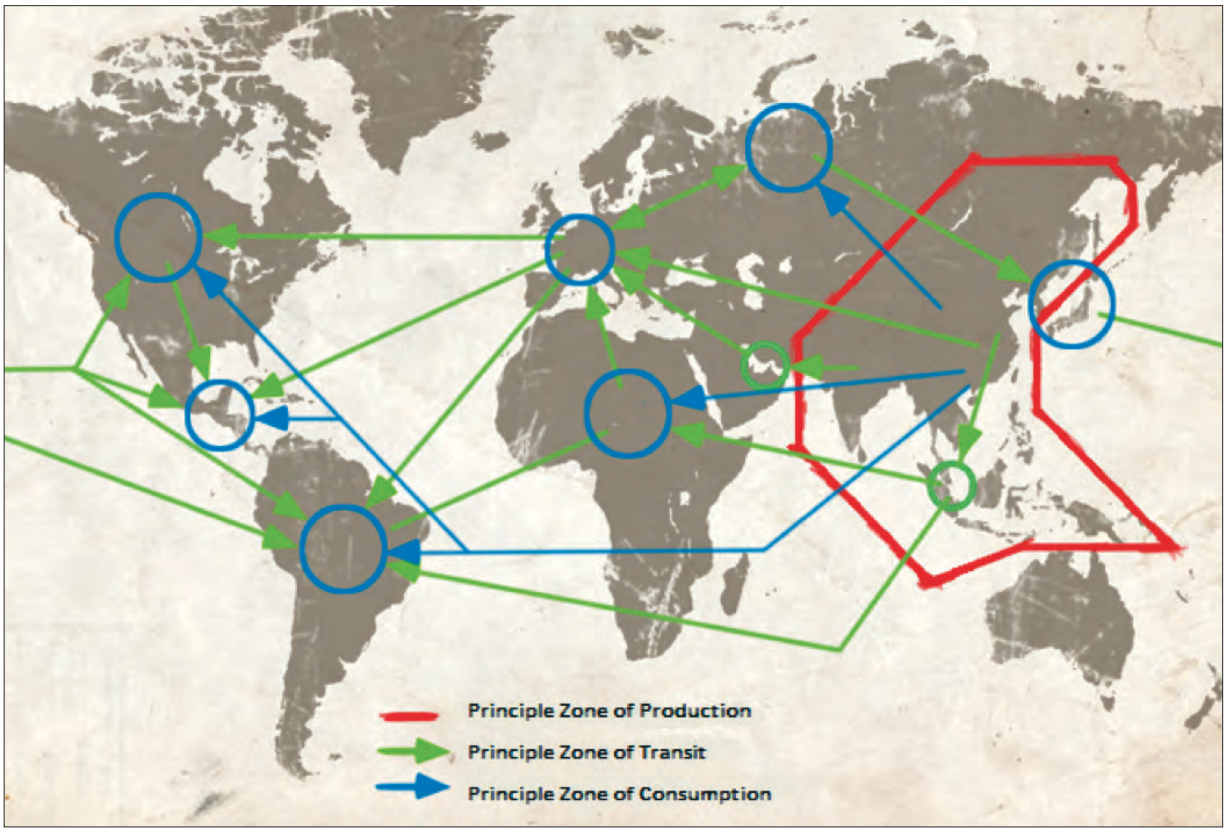
A small handful of "provenance economies" constitute the largest suppliers of counterfeit products to the U.S. and European Union (EU) economies. Counterfeit products originating from the People's Republic of China and Hong Kong (often as a transit route for Chinese goods) constitute 87 percent (by dollar value) of all goods seized by CBP.[48] Customs authorities in the European Union have reported similarly high percentages, with 79 percent of seized goods (by value)

FIG. 12: Fiscal year 2015 IPR Seizure Statistics.



Source: CBP, Office of Trade (2016)

FIG. 13: Source and complex transport routes.



Source: Unifab 2016.

originating from China and Hong Kong.[49] Additional provenance economies of significant global scale include: India, Turkey, United Arab Emirates, Singapore, Bangladesh, Thailand, and Indonesia.[50]

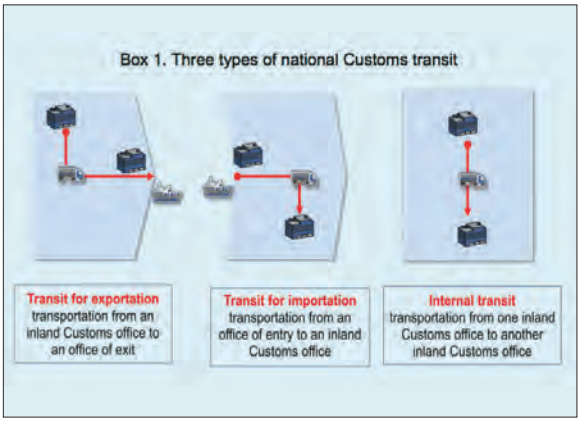
Distribution: Global Transport and Logistics.

Following production in provenance economies, illicit traders turn to global logistics networks and complex transit routes to move massive volumes of illicit goods. The volume of trade in counterfeits is approaching, if not surpassing, half a trillion U.S. dollars annually. Counterfeiters rely on frequent manipulation of trade routes, with circuitous intermediary and seasonal transit points (FIG. 13), to deliver fake products to markets under disguised and falsified conditions.[51]

Some of these transit points, such as Hong Kong or Singapore, are central and often exploited as hubs of international trade in illicit goods. Other transit points are attractive to illicit operators because poor governance or the prevalence of organized crime or terrorist network operations result in reduced scrutiny at the border (*e.g.*, Afghanistan or Syria).[52] Analysis from the OECD, for example, shows significant changes in transit routes from year to year, as illicit traders exploit new governance gaps. This in turn reflects the ability of counterfeiters, and the criminal networks that support the trafficking in fake goods, to identify weak points of enforcement quickly and consequently to minimize the risk of detection.[53]

Illicit traders tend to pass counterfeits through transit points in jurisdictions with little risk of IP-related enforcement actions both to move products closer to ultimate zones of consumption (e.g., end-market destinations), but also as part of a larger scheme to evade detection. As reported by the World Economic Forum (WEF), "[C]ounterfeiters use the transit or trans-shipment of goods through multiple, geographically diverse ports as a means to disguise the nature of the product and make it more difficult for law enforcement to track their activity."[54] Likewise, Europol notes that, "As the declared point of origin of goods is often the key risk indicator for Customs administrations, counterfeiters will use trans-shipment points to change and re-document container loads."[55]

FIG. 14: Three Types of National Customs Transit.



Source: WCO, Transit Handbook (2014)

In-transit counterfeit and piratical goods are less likely to be intercepted internationally by law enforcement personnel, who target imports but who may have limited authority to take action against goods transiting through their territory.[56] During this often overlooked "in transit" stage, reporting indicates that illicit traders will:

- Engage in a "cleansing" of transport documents in order to falsify and conceal the original point of production/departure;
- Establish decentralized distribution centers for counterfeit goods, often in free trade zones (FTZs), in order to ship "cleared" goods into smaller orders to final destination points; and/or
- Finish production, also often in an FTZ environment, by adding counterfeit trademarks and/or repackaging or re-labeling goods.[57]

With respect to FTZs, the WEF Global Agenda Council on Organized Crime singles out FTZs as a significant enabler for organized crime, and compares FTZs to offshore tax havens.[58] Several reports analyzing the exploitation of FTZs by counterfeiters highlight the lack of coordination between customs administration and FTZ administration, allowing criminals to re-document shipments by concealing the origin, contents, and destinations of shipments.[59]

In addition to the adoption of diverse trafficking routes and exploitation of FTZs, counterfeiters employ further transit-based concealment methods in order to evade customs controls, adding yet another dimension to an already complicated detection and enforcement environment. Counterfeit and pirated goods are concealed by way of false customs declarations and

> "Evidence suggests that organized crime groups frequently use FTZs to transship, label and obscure the port of origin of illegal goods. There are approximately 3,000 FTZs in 135 countries."
>
> *Source: Europol (2015 Situation Report on Counterfeiting, p. 16)*

shipping manifests such as invoices and bills of lading. Small products—such as counterfeit medicines in the form of anti-malarial and anti-parasitic drugs, antibiotics, and analgesics—have been found concealed inside air-conditioning equipment, music speakers, and sports balls.[60] The illicit trader often mixes and intersperses counterfeit goods among a variety of other counterfeit and legitimate products, or behind a false cover load, to minimize detection. The vast diversity of illicit trade is well-illustrated by an example of a reported seizure in the Port of Chonburi in Thailand: there were 36 different commodity types (e.g., watches, textiles, mobile phones) represented in a single container, with a combined total count of 42,068 counterfeit units.[61]

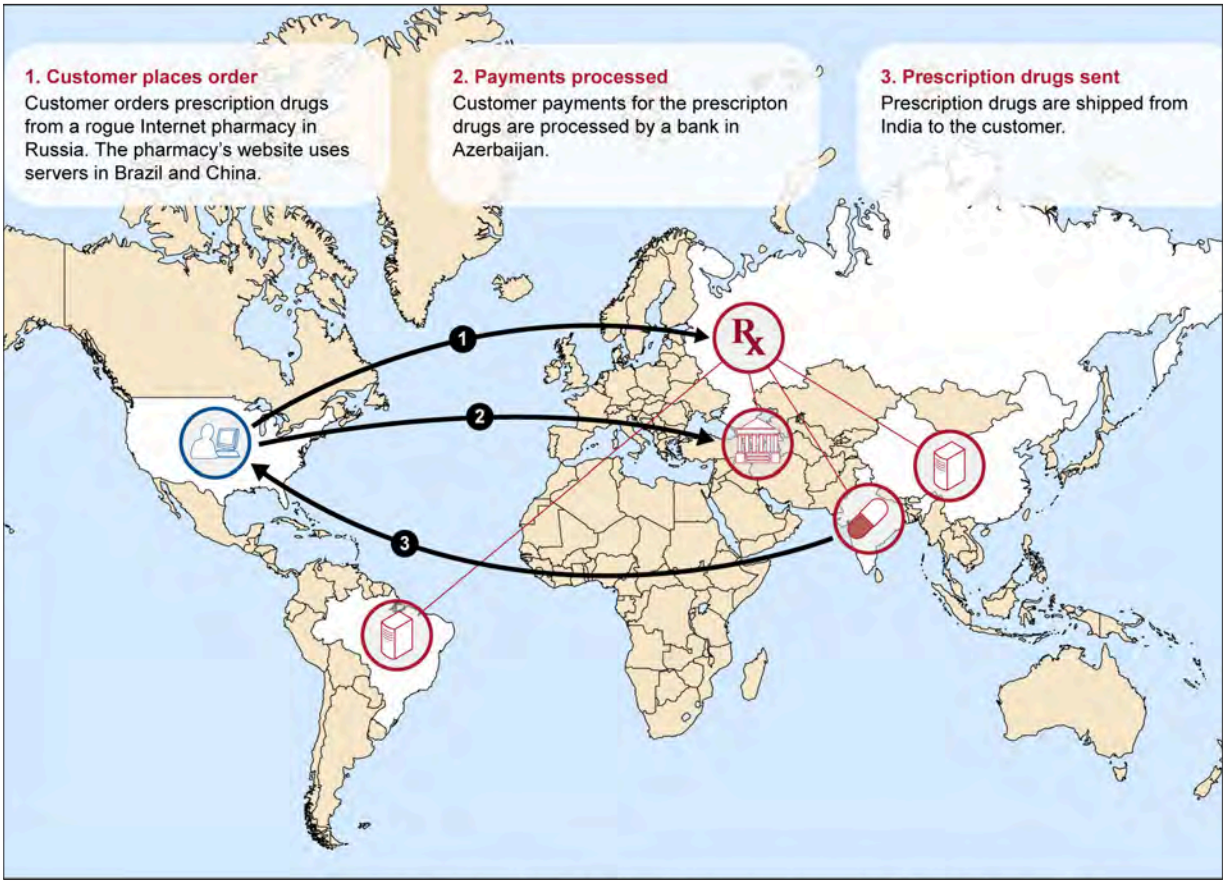
Traffickers of fake products have also turned to "small shipments," mostly by postage or by express shipment services, as a way to avoid detection and minimize the risk of loss or penalties. As set forth in greater detail in Section III.A, small shipments now represent a majority of all IPR seizures, adding a new and troubling dimension to securing domestic and global supply chains from infiltration by fraudulent products.

FIG. 15: Number of Seizures of Illicit Goods by Shipment Method (FY 2015).



Source: U.S. CBP, Office of Trade (2016)

FIG. 16: Example of International Framework Utilized by Rogue Internet Pharmacy Operators.



Source: GAO, "Internet Pharmacies: Federal Agencies and States Face Challenges Combating Rogue Sites, Particularly Those Abroad" (July 2013)

Sales Mechanisms and Tactics.

Counterfeiters are also adopting intricate sales and distribution structures to infiltrate global supply chains. It is not uncommon to see complex international sales and distribution frameworks (FIG. 16) where, for example, a consumer accessing a website purporting to be a "Canadian pharmacy" will in fact access one of numerous "mirror" counterfeiting sites managed from Russia, with web servers in Brazil and China, with payment processing operations run out of a bank in Azerbaijan, with bulk products shipped from India or China, transiting through Hong Kong, then sent by air to the United Arab Emirates, passing through London Heathrow airport, and with counterfeit inventory to be finished (packaged) in the Bahamas, before being delivered to a customer in the United States or elsewhere.[62]

Similar to the piracy business models discussed in the preceding section above, traffickers of counterfeit tangible goods reportedly often engage in systematic misuse of DNS by registering domain names for commercial services behind false or otherwise misleading contact information in order to perpetrate fraud as well as market and sell counterfeit goods on one or more websites, including by cybersquatting and pretending to be a legitimate website (*i.e.*, web page spoofing; FIG. 17).[63] Additionally, commercial-scale counterfeiters exploit social media platforms to generate web traffic and to direct consumers to rogue e-commerce websites selling illicit goods. They do so in a variety of ways, including by utilizing "buy-now"-type buttons that enable purchases directly from page posts and ads; and by posting pseudonymous product reviews, blog entries, and fabricated social media profiles to create an aura of legitimacy around their website.[64]

FIG. 17: Example of Website Spoofing Associated with Sale of Counterfeit Goods Online.



Source: EUROPOL IP Crime Coordinated Coalition

FIG. 18: Example of Multidimensional Industry Enforcement Dilemma.



The fronts on which the rights holder is fighting the illicit trade war are many and varied. A U.S. rights holder whose rights are infringed faces a complex, global enforcement scenario subject to a number of challenges (FIG.18). These challenges typically include the need to stem the manufacturing and flow of illicit products from provenance economies with inadequate enforcement mechanisms; to coordinate customs authorities across one or more continents to share information that may aid in the interdiction and seizure of counterfeit goods; to curb cybersquatting and other fraudulent tactics employed to move illicit content via the Internet; and to safeguard legitimate supply chains from infiltration by counterfeits. Once illicit products have entered supply chains, the products are sold to consumers who think they are buying legitimate products, either through well-known e-commerce sites or established brick-and-mortar businesses, compounding the economic loss to the rights holder with the potential for reputational loss through dissemination of defective and substandard products.

3. The Targeting and Theft of Trade Secrets.

Today, with technology enabling convenient global access to and instantaneous transmission of information, a malicious actor need not rely on physical access to a document to steal it, copy it, or photograph it.[65] Trade secrets exist in multiple forms and there are a myriad of ways in which they can be stolen, including through cyber infiltration and employee misappropriation.[66]

Critically, the targeting of U.S. trade secrets for commercial gain, when directed by nation-state actors, has emerged as an especially serious threat to the U.S. economy.[67] U.S.-based businesses, academic institutions, defense contractors, service providers such as law firms, and other entities are purposefully targeted for economic espionage and theft of trade secrets by state-sponsored foreign entities for commercial gain because these entities are "leader[s] in the development of new

technologies and central player[s] in global finance and trade networks" and thus "foreign attempts to collect U.S. technological and economic information… represent[s] a growing and persistent threat to U.S. economic security."[68]

Trade secret theft does not discriminate and affects all industries. It will continue to rise as methods for stealing become more sophisticated and, in some cases, easier due to technological advancements. In 2015, the United States achived important political commitments bilaterally with China, followed by a similar commitment with the G20, that "no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[69] While some improvements have been made to thwart these efforts, including increased legal protections, companies must remain vigilant. Stakeholders need to work together to protect American innovation and creativity, pillars of our global economy, by continuously monitoring emerging threats and addressing vulnerabilities expeditiously.

C. THE THEFT AND UNLAWFUL EXPLOITATION OF INTELLECTUAL PROPERTY AS THREATS TO U.S. NATIONAL INTERESTS.

The preceding sections describe the overall scope, magnitude and level of complexity and sophistication behind the unlawful exploitation of intellectual property rights, including copyright interests, trademarks, patents, and trade secrets. This section seeks to highlight the often-overlooked types of harms caused by the unlawful exploitation of intellectual property interests. It is important that the theft of IP be seen in the larger context of its attendant economic, social, and ethical impacts. This perspective will help to advance public understanding of these matters, as well as providing enhanced clarity and purpose in policymaking.

If ever it was, it certainly is no longer accurate to view IP theft as a "soft crime" affecting only narrow private interests. The entities engaged in commercial-scale piracy, counterfeiting, or trade secret theft harm the economic competitiveness of our businesses, the livelihood of our creative and innovative communities, the health and safety of the public, workers' rights, the environment, and domestic and international security.

> "Nearly any illicit market involves criminal activities that impact the security of citizens, undermine the authority of states, erode the social fabric, criminalize society, and generate an overall cost of crime that must be borne by society."
>
> *Source: Convergence: Illicit Networks and National Security in the Age of Globalization (2013).*

1. Undermines Principles of Fair Trade in the Global Economy.

IP-intensive industries are an engine of economic growth for the United States and other countries. Success in the global marketplace is premised upon a company's ability to innovate and compete in any free-market environment that upholds the rule of law. Entrepreneurs and rights holders invest enormous resources in creating products, content and know-how, and in strengthening their businesses through innovation and creativity. They are denied a rightful return on these investments when the integrity of the marketplace—that is, rules supporting fair competition—are violated. The development and distribution of counterfeit goods, commercial-scale piracy, trade secret theft, and the erosion of patent protection are all means to gain unearned (and unlawful) economic competitive advantage or profit. These acts, particularly at the scale being widely reported, tend in aggregate to decrease the stability and efficiency of the global economy by discouraging the creativity, investment, and innovation that improve quality of life and support well-paying jobs.[70]

Misappropriation of IP can deter critical foreign investment that would create more opportunities for American businesses abroad while simultaneously improving the economies of our trading partners. For instance, the cost of doing business in countries with poor IPR enforcement continues to increase, as companies are forced to budget for additional enforcement costs and lower sales revenue when they cannot combat the entry of counterfeits into the global supply chain. Put simply, poor IP enforcement (like all incursions on the rule of law) dampens domestic and foreign investment and the attendant benefits that flow from such investments.

As noted at the outset, IP-intensive industries in the United States alone create and support tens of millions

FIG. 19: The harms flowing from counterfeiting, commercial piracy, and trade secret theft are widely felt.[71]

Consumers	Legitimate Businesses	Governments	Global Trading Partners
• Exposed to low quality products that are unregulated and often unsafe • Misled and defrauded • Exposed to theft of private information	• Lost sales • Decreased profits • Loss of brand trust • Opportunity cost of increased spending on IP protection	• Undermines rule of law • Decreased tax revenues • Increased spending on welfare, health services, law enforcement and crime prevention • Undermines fair competition in world markets • Labor exploitation	• Decreased or delayed investments of U.S. companies overseas • Undermines political, financial, and security institutions in states by corruption • Financing of criminal syndicates

of jobs, contribute trillions of dollars in value, represent more than 38 percent of U.S. GDP, and account for more than 50 percent of all U.S. merchandise exports.[72] When IP is stolen or unlawfully exploited, it not only hurts our artists, innovators, and businesses all over the world that rely on these protections, but presents a real and significant threat to an enormous driver of U.S. economic growth (FIG. 19).

Without a comprehensive plan to continue to address the root causes of these harms, the magnitude of the impact on our economies, our people (both consumers and workers), the environment, and our political institutions will compound and increase. Indeed, the interdependence of countries resulting from the increasing integration of trade and finance, and the exchange of people and ideas in one global marketplace—driven, in part, by the digital revolution, along with continuing improvements in manufacturing methods and transportation infrastructure—have lowered barriers to entry and vastly expanded a commercial enterprise's potential customer base. These and other factors are attracting more people into the commercial marketplace, including, unfortunately criminal actors relying on unlawful shortcuts by way of IP-exploitative activities.

2. Threatens Consumer Health and Safety.

The threats to the health and safety of the American public from counterfeit goods is significant, and may be on the rise due to the growing diversity of counterfeit products entering the United States. CBP seizure statistics reveal a diverse set of products, including personal care products, pharmaceuticals, critical technology components, automotive parts, electrical components, aviation parts, medical devices, children's toys, and foods and beverages that are routinely counterfeited and pose dangers to consumer health and safety.[73] However, there has not been a systematic analysis of the magnitude of the health and safety risk to U.S. interests from these and other categories of goods, and more data and research are critically required, as detailed in the Call for Research at the conclusion of Section IV of this Strategic Plan.

For illustrative purposes, and to enhance public understanding and awareness, below are a series of case studies across four counterfeit product categories that pose significant threats to the health and safety of the public, namely: (1) personal care products; (2) pharmaceuticals; (3) consumer electronics and electrical components; and (4) automotive parts. While these case studies are instructive, there remains ample opportunity to enhance our understanding of the nature and scope of the problem across these and other product categories where counterfeiting is proliferating.

Example: Counterfeit Personal Care Products.

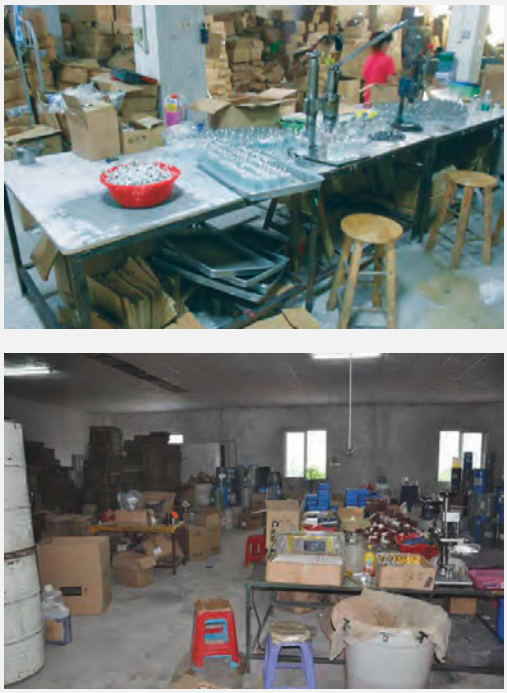
With increased seizures reported each year, counterfeit personal care products—such as perfume, soap, toothpaste, contact lenses, condoms, sanitary pads, deodorant, shampoo, lip balms, petroleum jelly, baby oil, hair curlers, and cosmetics—are on the rise and becoming one of the most-seized product categories.[74]

Over the last two years, the number of personal care products seized by U.S. authorities has tripled.[75] Illustrative of scale, a single joint operation between U.S. and French customs authorities conducted from April

FIG. 20: Real Ingredients and Consequences of Counterfeit Personal Care Products.

Counterfeit Item	Danger(s)/Containments Detected
Sunscreen	No SPF protection
Cosmetics (eyeliner, mascara, lipstick, foundation)	Carcinogens like arsenic, aluminum, lead, bacteria
Perfume	Urine, contaminated water, carcinogens

FIG. 21: Working Conditions of a Counterfeit Perfume Factory Exposed.



8, 2015 to May 4, 2015, resulted in the seizure of more than 31,000 counterfeit personal care products, with a combined manufacturer's suggested retail price of $541,000.[76]

Counterfeit personal care products are reported as being produced in highly unsanitary conditions (FIG. 21), with little regard for the safety of the consumer. Unlike authentic personal care products that go through rigorous development and testing procedures, counterfeit personal care items are not subject to the same strict safety and effectiveness requirements as genuine articles, including, for example, under the Federal Food, Drug and Cosmetic Act (FD&C Act).[77]

These products have been found to contain substandard and dangerous substances, or otherwise fail to perform as advertised, causing adverse physical reactions such as rashes, acne, psoriasis, and eye infections,[78] burning, and ineffectual family planning protection to the consumer.[79]

While counterfeiters may have targeted "high-end" products in the past, seizure data and criminal prosecutions confirm that counterfeit personal care products have evolved to include everyday health and beauty items.[80] Counterfeits within this product category pose significant dangers to consumer health and safety, and also undermine consumer trust in the quality and safety of branded products in the marketplace.

Example: Counterfeit Consumer Electronics & Electrical Products.

Counterfeit electrical products pose high risks to public health and safety as these products are often manufactured with inferior materials through sub-standard processes, without regard for any labeled ratings, certifications, or customer safety requirements, leading to increased risk of malfunctions that may cause serious injuries, including electrical shock and death.

According to recent CBP figures, counterfeit electrical products have grown to now represent 18 percent of all seizures, with approximately $135 million in seized fake products destined to consumers in the U.S. market.[81] From personal electronics such as headphones to smartphones and related accessories like power adapters and charging cords and devices, consumers are unknowingly at increasing risk of bringing home dangerous devices.[82]

FIG. 22: Overheated Counterfeit Extension Cord.



Source: Underwriters Laboratories (UL) (Fake cord caught on fire when plugged in and put under a heavy electrical load)

One technical investigation administered by Underwriters Laboratories (UL) subjected 400 counterfeit mobile phone adapters to safety testing, and the results were literally shocking.[83] The overall failure rate exceeded 99 percent, and the counterfeit adapters were found to present significant fire and shock hazards.[84] Indeed, 22 samples were immediately damaged during the tests, and 12 additional samples were found to be so poorly designed and constructed that they presented a risk of lethal electrocution to the user.[85]

This fast-growing criminal trade in counterfeit electronic components has resulted in millions of counterfeit electrical products entering supply chains the world over, including recent examples of: circuit breakers that did not trip when overloaded; extension cords with undersized wiring that overheated; batteries and chargers without a safety device in the circuitry to prevent overcharging; holiday lights that posed fire hazards; small appliances that lacked ground-fault circuit interrupters that protect users against electrical shock; and ineffective surge protectors.[86]

The diverse avenues through which counterfeit electronics can reach consumers is particularly worrisome. Sometimes, a counterfeit reaches the consumer in the form of a complete counterfeit product, while other times they enter the supply chain as fraudulent component parts that are inadvertently incorporated into legitimate goods.[87] For example, as of June 2016, CBP had facilitated the seizure of over 100,000 hoverboards, valued at $45 million, following reports of fires caused by substandard and counterfeit lithium ion batteries used to power the hoverboards (FIG. 23).[88]

FIG. 23: Overheated Counterfeit Hover Board.



Source: U.S. Consumer Product Safety Commission

Manufacturers of counterfeit electrical products have their sights set on the attractive U.S. market. As an example of the scale of the issue, a single joint operation between Chinese and U.S. customs offices during a one-month period resulted in the seizure of a quarter of a million counterfeit electronics, including globally known legitimate brands.[89] Criminal enterprises exploit these and other popular, legitimate brands to further their illicit enterprises. Counterfeiters are becoming sufficiently sophisticated that even complex technologies are successfully manufactured, falsely branded, and sold into the U.S. supply chain.

Example: Counterfeit Pharmaceuticals.

Among all counterfeit goods, counterfeit pharmaceuticals pose one of the most serious and pervasive health and safety threats. As noted by The Economist, "[s]alesmen have peddled worthless cures for millennia. But the 21st century is turning into a golden age for bad drugs.... For criminals, fake pharma is lucrative and the penalties are usually low. Indeed, the drug supply-chain is a cheat's paradise."[90]

Counterfeit drugs circumvent all of the standards and protections built into the regulated closed system of distribution for genuine pharmaceuticals in the United States. They may contain too little, too much, or no active primary ingredients, or various dangerous contaminants.[91]

Counterfeit drugs are not produced under safe manufacturing conditions, nor are they inspected by regulatory authorities. Reports confirm that many counterfeit drugs include ingredients that are toxic to patients and processed under poorly controlled and unsanitary conditions.[92] Organizations and independent traffickers often acquire counterfeit oxycodone and other pharmaceutical drugs through the darkweb. Consequently, these drugs resemble actual pharmaceutical drugs including the marking on the pills. However, lab results often determine these purported pharmaceutical drugs contain other illicit drugs such as heroin.

FIG. 24: Ingredients found in counterfeit medicines.

Heavy Metals	Actual poison	Contaminants	Common household items	No drugs at all
mercury	PCBs	road paint	aminotadalafil	dextrose
aluminum	benzopyrenes	wall paint	homosildenafil	dextrin
lead	rat poison	brick dust	xanthoanthrafil	lactose
cadmium	boric acid	floor wax	pseudovardenafil	starch
arsenic	antifreeze	sheet rock	hongdenafil	saline
chrome		paint thinner	sibutramine	sald
uranium			haloperidol	
strontium				
selenium				

Source: Adapted from the Partnership for Safe Medicines

FIG. 25: Examples of Counterfeit Pharmaceutical Manufacturing Conditions.[95]

Facilities in Columbia



Source: International Intellectual Property Institute

Facilities in Pakistan



Source: CNN

The medicines produced in (FIG. 24) for example, were reported to contain no active ingredient, and tested positive for such compounds as boric acid, brick dust, and paint.[93]

To date, millions of counterfeit pharmaceutical products have been identified and seized in global markets.[94] Assessing the total size of the problem has proven difficult, but recent enforcement operations and surveys suggest that the problem is world-wide, requiring enhanced international attention and determination to eliminate illicit trade in medicines.

In a 2007 report on counterfeiting and piracy, the OECD provided an extensive but non-exhaustive list of medicinal products that have been counterfeited, which included: medicines used for treating cancer; human immunodefiency virus (HIV); malaria; osteoporosis;

FIG. 26: Can you tell which ones are fake drugs in each of these pairs?*



Source: Partnership for Safe Medicines

**counterfeits on right*

diabetes; hypertension; cholesterol; cardiovascular disease; obesity; infectious diseases; Alzheimer's disease; prostate disease; erectile dysfunction; asthma and fungal infections; antibiotics; anti-psychotic products; steroids; anti-inflammatory tablets; pain medicines; cough medicines; hormones and vitamins; and treatments for hair and weight loss.[96]

In 2013, the World Health Organization (WHO) launched a global surveillance and monitoring system to encourage countries to report "substandard, spurious, falsely labelled, falsified and counterfeit" (SSFFC) medical products in order to help develop a more accurate and validated assessment of the scope, scale, and harm caused by this issue.[97] **Over 920 different medical products have been reported so far**, representing every region of the world, affecting medical products from all main therapeutic categories, and representing both innovator and generic medicines.[98]

Using intelligence from enforcement operations, INTERPOL coordinated a worldwide operation during a single week in 2015 resulting in a **record 20.7 million fake and illicit medicines seized**—including blood pressure medication, erectile dysfunction pills, cancer medication and nutritional supplements—and more than 2,410 rogue websites taken offline.[99] Ninety-seven percent of all counterfeit pharmaceuticals seized at the U.S. border in FY 2015 were shipped from four economies: China, Hong Kong, India, and Singapore.[100]

Counterfeit drugs are manufactured to closely resemble the real thing, often making it virtually impossible for consumers to detect whether the medicinal products they are ingesting are genuine or counterfeit (FIG. 26). This can be especially dangerous if the counterfeit product appears as commonly prescribed opioid pain medication, such as oxycodone or hydrocone, yet the counterfeit actually contains illicitly produced fentanyl, a significantly more powerful synthetic opioid, because fentanyl can plunge users into overdose quickly.

With a growing number of individuals shopping online for affordable medicine, consumers are now confronted with an alarming number of rogue internet pharmacy sites.[101] Criminal networks have become increasingly sophisticated, stocking rogue pharmacies with counterfeit medicines made all over the world and posing as legitimate pharmacies.[102] Yet, a review by the National Association of Boards of Pharmacy (NABP) has shown that as **few as three percent (3%) of websites** selling prescription drugs are legitimate pharmacies.[103]

Counterfeit Automotive Parts.

The circulation of counterfeit automotive parts in the United States and around the world gives rise to serious public safety concerns.[104] These illegal products are not made to the specifications of the original manufacturer, are not subject to quality control tests, and fail to perform as intended, resulting in catastrophic failures with potentially fatal consequences.

Some of the most dangerous counterfeit products involve air bags that, during testing from U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA), demonstrated consistent malfunctioning of the air bag (FIG.27) ranging from non-deployment, to under-deployment, to over-deployment accompanied by an explosion of metal shrapnel.[105]

FIG. 27: NHTSA Test of Counterfeit Air Bag.

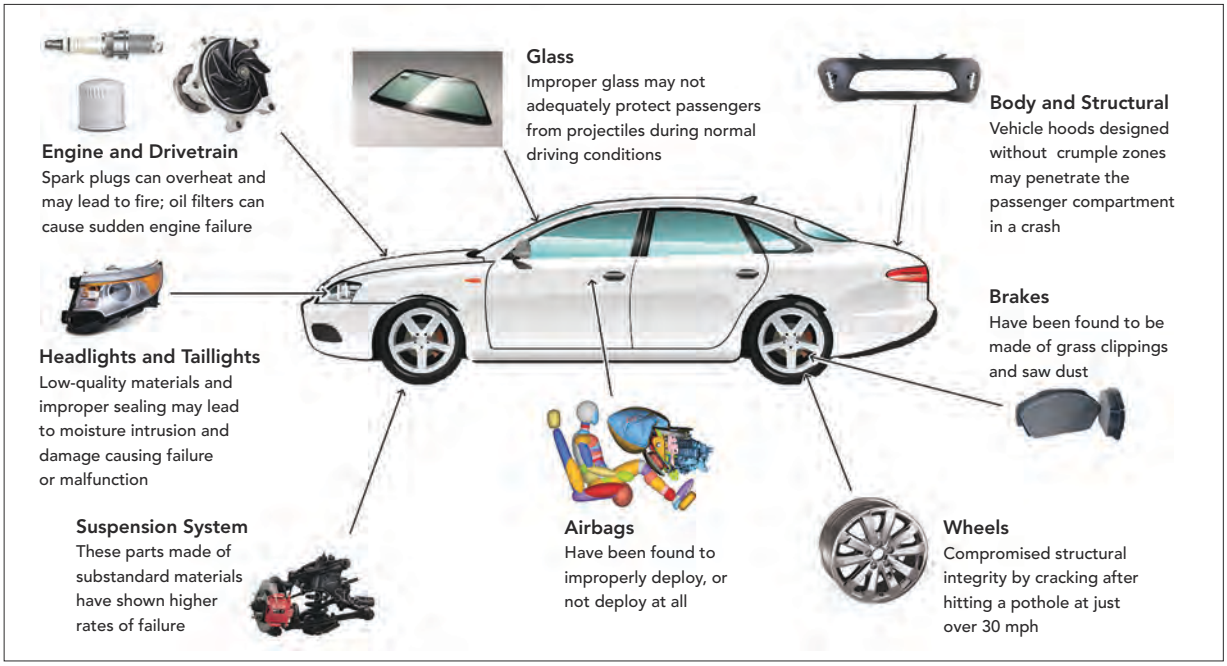


Source: NHTSA

A wide variety of auto parts have been seized by law enforcement over the years.[106] While counterfeit auto parts may have been historically limited to "cosmetic" items like hood ornaments and decals, customs seizure statistics reveal that counterfeit safety components like brake pads, air bags, wheels, and suspension parts are becoming increasingly common.

Additional counterfeit parts reported to have been seized by law enforcement include: seat belts, oil and air filters, brake rotors, control arms, windshields, bearings, steering linkages, ignition coils, microchips, spark plugs, solenoids, clutch housing, crankshafts, diagnostic equipment, suspension parts and oil pumps.[107] **Put simply, almost every type of auto part can be and has been counterfeited** (FIG 28).

FIG. 28: Examples of Seized Counterfeit Automotive Parts.



Source: a2c2

Recent enforcement operations suggest that the counterfeit auto part trade is large and growing.[108] During one inspection at Florida's Port Everglades on May 8, 2015, CBP officers and import specialists seized more than 3,260 counterfeit automobile parts, comprised of a diverse collection of over 180 different types of vehicle parts ranging from small fuses to entire front ends.[109]

As these industry examples illustrate, entities behind the manufacture, distribution, advertising, and sale of counterfeit products are not concerned about public health and safety. These entities share a devotion to generating illicit profits at all costs, while remaining recklessly indifferent to the actual injuries and potential risks to life that can come from their imitation of personal care products, pharmaceuticals, consumer electronics and electrical components, and automotive parts.

3. Threatens the Environment.

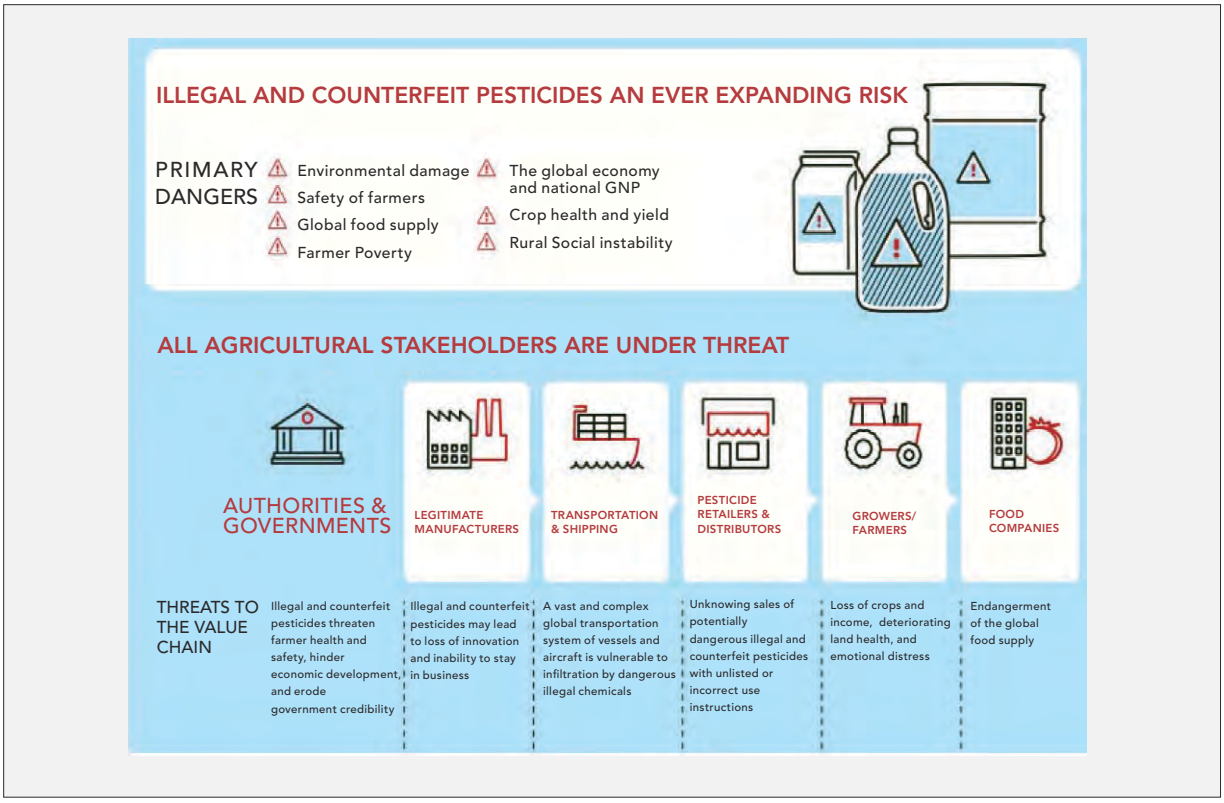
Environmental offenses are often treated in isolation from other types of serious crimes, including trade in counterfeit goods. That may be due in part to separate agencies having responsibility for the protection and conservation of the environment, trade enforcement, and national security. A broader view and greater coordination would be beneficial to adapt to today's more sophisticated environment of global illicit trade.

The environmental costs of counterfeiting are often understated, but cannot be ignored. Counterfeit products are often accompanied by environmentally-damaging consequences, either at the time of manufacture, the time of use, or the time of disposal. With respect to counterfeit manufacturing practices, the United Nations Office on Drugs and Crime (UNODC) has reported that while responsible manufacturers try to improve their environmental impact standards, "counterfeiters enjoy the cost savings of dirty production. In short, anywhere that the international community attempts to establish good practice standards for industry, counterfeiters undercut them."[110]

Furthermore, the use of counterfeit agrochemical products appear to be significant and on the rise.[111] Unregulated fertilizers or pesticides have destroyed harvests and poisoned farmland.[112] These products pose serious environmental risks, including infecting food chains and harming ecosystems. For example, counterfeit fertilizers have been reported to have caused serious damage and destruction of harvests in large areas in China, Russia, Ukraine, and Italy.

Counterfeit pesticides exported from China and India have been found to include toxic ingredients such as nicotine sulphate, which is deadly to humans, and has been distributed to unknowing buyers throughout

FIG. 29: The Growing Global Threat of Counterfeit Pesticide Use.



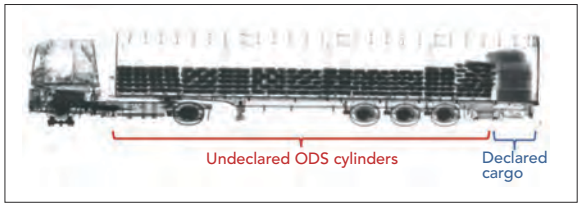
Source: Croplife International

Europe.[113] It is estimated that more than 25 percent of the pesticides in circulation in parts of Europe may be illicit or counterfeit.[114]

Additionally, illicit trade-based operations have been associated with the mishandling of toxic chemicals, including outlawed chemicals and toxic dyes. This contributes to the emission of greenhouse gases polluting the air, as well as polluting soil and water systems.[115]

Lastly, the improper disposal of seized counterfeits containing unknown chemicals is also posing a growing risk and challenge.[116] Manufacturing waste, including electronic waste, may implicate more than 1,000 different substances, including toxic heavy metals. When disposed of improperly, this waste can cause significant pollution problems and create health hazards.[117] As the counterfeit trade continues to increase, so will logistical challenges for determining how best to dispose of its waste while ensuring no environmental harms.[118]

FIG. 30: Customs x-ray of a truck involved in waste trafficking and transshipment fraud. The x-ray reveals the method of double layering to conceal cylinders containing ozone depleting substances behind declared cargo.



Source: INTERPOL[119]

4. Exploits Labor.

The behind-the-scenes production of counterfeit goods often involves human rights violations, including the use of child labor, forced labor, human trafficking, long hours and dangerous "sweatshop" working conditions, and payment of unlawfully low wages that do not cover living expenses.[120] Although they read as if taken from a horror novel, reports from the field are all too real, describing labor practices that are contrary to the most basic principles of respect for human rights. Put simply, the safety and security of the laborer are ignored.

Illegal counterfeit enterprises often exploit the

most vulnerable individuals in society that find their way to these positions on the 'sweatshop' floor, where they are not granted the same form of protection available to the legitimate employment market.[121] With a workforce comprised of individuals with little to no means—including migrants who have been smuggled into a country or immigrant workers who have had their identity papers confiscated—these are often 'dead-end' positions from which it is difficult to free oneself.

> "I remember walking into an assembly plant in Thailand a couple of years ago and seeing six or seven little children, all under 10 years old, sitting on the floor assembling counterfeit leather handbags. The owners had broken the children's legs and tied the lower leg to the thigh so the bones wouldn't mend. [They] did it because the children said they wanted to go outside and play."
>
> *Source: Dana Thomas, Harper's Bazaar, "The Fight Against Fakes," exerpt from "Delux: How Luxury Lost its Luster."*

Labor and human rights violations extend beyond the point of manufacture to the time of sale, where individuals are exploited by human traffickers and illicit traders. For example, illegal immigrants—often from Africa or Asia—are reported to have been smuggled into countries and coerced by their facilitators to engage in street sales of counterfeits.[122] Although street sales operations may not appear to be under forced circumstances, reports confirm that many of these street sales and unlicensed markets are often controlled by organized crime groups and other illicit actors.[123]

These types of exploitative acts and violations are not confined to foreign countries, as reports demonstrate that individuals in the United States have engaged in human trafficking and forced labor in connection with the distribution and sale of counterfeit and pirated goods.[124] As the U.S. Attorney for the Southern District of Texas noted in connection with one criminal case that was prosecuted to conviction: "Driven by greed, these defendants mistreated and abused the victims of human trafficking after enticing them to come…with promises of employment and a better life. Forced to sell counterfeit goods to repay their smuggling fees and earn their freedom, bootleg CDs and DVDs became the shackles of the victims of this modern day slavery."[125]

5. Poses Threats to Domestic and International Security.

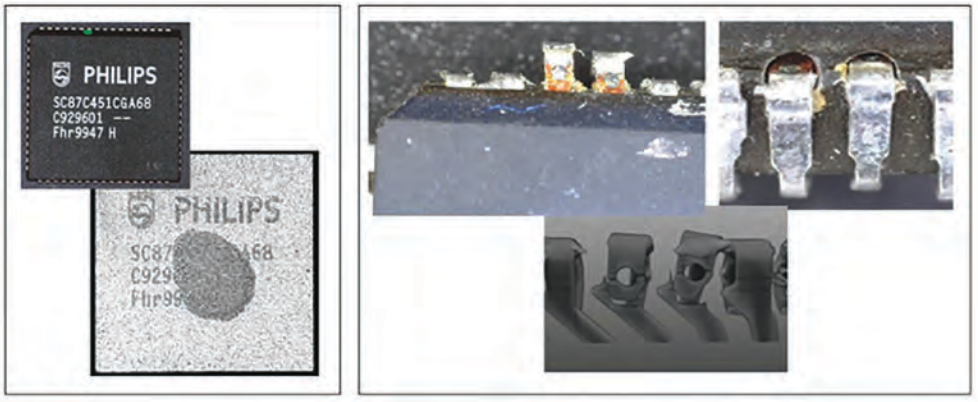
In addition to the various risks and consequences flowing from the unlawful exploitation of intellectual property rights discussed above, these same illicit activities may also give rise to far-reaching and serious threats to domestic and international security. Although these threats may be closely linked to, and converge with, one or more of the threats summarized above, the risks to national security interests must be better understood.

The U.S. is a key player in the global financial and trade networks and a leader in producing valuable intellectual property. Therefore, it continues to remain a prime target for counterfeiting and piracy networks. As a target, the United States is both seen as a main *source* of critical technology, life-saving medicines, and other innovative and creative works to be stolen or otherwise misappropriated, as well as an attractive *receiver* or destination of incoming illicit goods due to market size. Put simply, the dual nature of the threat—*incoming* illicit goods and *outgoing* misappropriated IP—gives rise to unique national security concerns.

> "Illicit networks seek to navigate, infiltrate, and/or dominate global supply chains to further their activities and enhance their power. They actually thrive in open societies with the free flow of goods, people, and capital. Just like licit businesses, illicit networks are matching the supply and demand for goods, services, capital, and information for their clients. Illicit actors utilize and…seek to control or co-opt supply chains around the world[.]"
>
> *Source: Convergence: Illicit Networks and National Security in the Age of Globalization (2013).*

This section highlights two particularly acute threats in which illicit IPR activities may also impact security concerns: namely, when illicit goods infiltrate critical supply chains (such as military and civilian computer network systems) and when intellectual property-based crimes are used to finance and support criminal syndicates around the world.

FIG. 31: Examples of Tests to Detect Suspect Counterfeit Electronic Parts.



An acoustic microscopy test identified that the center of the part contained a different material that was otherwise undetectable upon visual inspection.

Visual inspection and X-ray revealed part leads that were replaced and covered up.

Source: Naval Surface Warfare Center Crane Division | GA-16-236

a. The Integrity of Supply Chains and Critical Infrastructures.

When counterfeit computer and networking devices enter the supply chain, for example, they directly "undermine the reliability of our communications and transportation networks and create national security vulnerabilities. In addition, nation states target U.S. civilian industries for trade secret theft to obtain information that can be used to advance their domestic industries and military capabilities."[126]

There are particularly significant consequences when the supply chain is one operated for the benefit of the U.S. Department of Defense (DOD). The existence of counterfeit parts in the DOD supply chain can, for example, delay or threaten military and intelligence missions, affect the integrity of sensitive data and secure networks, cause weapon or other system failures, and ultimately endanger the lives of service members. Almost anything is at risk of being counterfeited, including microelectronics used in fighter jets and missile guidance systems, fasteners used in aircraft, and materials used in engine mounts.[127]

The DOD supply chain is vast, covering over 4.7 million parts that are used in, for example, communication and weapon systems, at a cost of approximately $100 billion.[128] "DOD draws from a large number of suppliers in a global supply chain—in both the acquisition phase and throughout a system's operational and sustainment phases—providing multiple opportunities for the risk of counterfeit parts into these systems."[129] In particular, contractors rely on thousands of subcontractors and suppliers, including the original component manufacturers that assemble microcircuits and the mid-level manufacturers subcontracted to develop the individual subsystems that make up a complete system or supply.

United States of America v. Peter Picone
Case No. 3:13-cr-oo128 (D. Conn.)

In October 2015, an individual was convicted for conspiring with suppliers in **China and Hong Kong** to sell thousands of **counterfeit integrated circuits**, bearing the trademarks of approximately 35 major electronics manufacturers, intended for use in nuclear submarines by the U.S. Navy.

Source: IPEC FY 2015 Annual Report

Based on an audit of reports submitted through the Government-Industry Data Exchange Program (GIDEP)—a program that allows government and industry participants to share information on nonconforming parts, including suspect counterfeit parts, via a web-based database—the Government

Accountability Office found that 526 reports of suspected counterfeit parts were entered for fiscal years 2011 through 2015.[130]

Similarly, private supply chains are being infiltrated, resulting in counterfeit products unknowingly being passed along and sold directly to industries and consumers alike. With respect to industrial supply chains, the U.S. has identified sixteen (16) critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, National economic security, National public health or safety, or any combination thereof.[131] These critical infrastructure sectors span across various industries, including for example, information technology; critical manufacturing (e.g., electrical equipment, transportation equipment, etc.); food and agriculture; healthcare and public health; and energy.

The diversity of counterfeit and faulty goods not only creates extra costs for businesses and consumers, but can also corrupt critical infrastructure sectors and jeopardize public safety. From counterfeit electronic components used in information technology systems to counterfeit automotive parts; from counterfeit pharmaceuticals to counterfeit fertilizers and pesticides that contaminate food supplies, these and other products and components introduce potential problems along the supply spectrum, posing a growing threat to governments, industry and consumers.

b. The Convergence between Intellectual Property-Based Crime and the Financing of Criminal and Terror Networks.

The growth in illicit trade is being fueled by smart and sophisticated organized criminal networks that understand how to exploit new technology, and use the differences among national regulatory regimes and links between the global economic, financial, and transportation systems for their own gain. There is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures and the crimes they commit also vary.[132] These networks generate illicit profits that may be used for other criminal activities, such as drug trafficking, people smuggling, bribery, money laundering and terrorism.[133]

> "The link between organized crime groups and counterfeit goods is well established. But INTERPOL is sounding the alarm that Intellectual Property Crime is becoming the preferred method of funding for a number of terrorist groups.
>
> There are enough examples now of the funding of terrorist groups in this way for us to worry about the threat to public safety. We must take preventative measures now."
>
> *Former Secretary General, INTERPOL, Hon. Ronald K. Noble*

There are a number of publicly available examples—stemming from U.S. prosecutions and reports; international organizations and law enforcement bodies; and the news media—that illustrate the growing convergence between IP-based crimes, TOC, and terrorism. With respect to the latter, there is evidence supporting *links* between intellectual property crime (IPC) and various terror groups, but as succinctly noted by INTERPOL, "most terrorist groups do not take responsibility for the development and control of counterfeit production and distribution; rather they

FIG. 32



benefit indirectly from funds remitted to them from sympathizers and militants involved in IPC."[134]

For purposes of discussion within the context of this Strategic Plan, this distinction may provide a practical interpretative guide, meaning that that reported terror "links" should be understood largely in the context of *indirect* funding at this time. However, in light of our Nation's commitment to "prevent collaboration between criminal and terrorist networks and deprive them of their critical resources" and to "break[] the financial strength of criminal and terrorist networks," even indirect financial support represents a material concern when speaking of terror groups.[135]

As summarized by the White House "Strategy To Combat Transnational Organized Crime," it has been reported that TOC networks are engaged in the theft of critical U.S. intellectual property, including through intrusions into corporate and proprietary computer networks; piracy of movies, music, and video games; counterfeiting of popular and trusted brand names; and the infringement of patented high-tech devices and other assets.[136]

The United Nations and other entities have similarly reported that organized criminal networks—such as the Mafia in the Americas, the Colombian and Mexican drug cartels, the Russian Mafia, the Neapolitan Camorra in Europe, and the Triads and Yakuza in Asia—have diversified into the illicit trafficking of counterfeit and pirated goods, including counterfeit medicines, luxury apparel and accessories, DVDs and CDs, and other goods.[137] "Much, if not most, of the trade in pirated and counterfeit goods in Mexico is controlled by [TOCs]."[138]

The nexus between organized criminal activity and terrorist groups remains a threat requiring renewed attention. INTERPOL and other entities have reported that a wide range of terrorism-linked entities—including al-Qaeda and affiliated groups; North African radical fundamentalists terrorists in Europe; Hezbollah; Chechen separatists; ethnic Albanian extremist groups; and paramilitaries in Northern Ireland—have been linked with the smuggling and sale of a broad array of counterfeit goods, including counterfeit cigarettes; medicines; personal care products (such as shampoos, creams, cologne and perfume); auto parts; shoes and apparel; and pirated music, movies, computer software, and video games.[139]

OPERATION JUPITER VII

Coordinated by INTERPOL, police and customs officers across South America took part in an operation aimed at disrupting the organized crime networks behind illicit trade and the production and distribution of counterfeit goods in the region and beyond. Operation Jupiter VII was conducted on August 15 – 31, 2015, and involved 2,000 raids in 11 countries.

The operation led to the seizure of 800,000 fake goods worth approximately $130 million, with 805 people either arrested or placed under investigation. Counterfeit goods seized included: clothing, fertilizers, windshields, alcoholic beverages, cigarettes, cosmetics, electric and electronic components, mobile phones, accessories, fuel, and construction materials.

Federal Brazilian Police seized 300,000 fake car windshields during the operation.



Source (Photo): INTERPOL Gallery 2015-137

"Initiatives such as Operation Jupiter VII show a clear link can be drawn between traddicking in illicit goods and transnational organized crime, which makes enforcement operations of this nature of utmost importance," sid INTERPOL Executive Director of Police Services.

Source: INTERPOL Press Release, Sept. 21, 2015)

According to additional reports, a number of TOCs and terrorism-linked entities have established, benefited from, or were otherwise associated with, a complex financial network supported by a diversity of criminal activities, including specifically illicit trade in counterfeit goods. Those entities include, for example, the Irish Republican Army (IRA), which has been linked to the sale of various counterfeit products, including counterfeit veterinary medicine; Hamas, which has been linked to counterfeit footwear and sports apparel; the Basque separatist group Euskadi Ta Askatasuna (ETA), which has been linked to counterfeit apparel,

Statement on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea"

"We take seriously North Korea's attack that aimed to create destructive financial effects on a U.S. company and to threaten artists and other individuals with the goal of restricting their right to free expression."

The White House (Jan. 2, 2015)

bags and cigarettes; the Revolutionary Armed Forces of Colombia (the FARC), which reportedly found the sale of pirated discs more profitable than the ransom kidnappings for which it is more notorious; and across the tribal belt of Pakistan, it is reported that Taliban militias collect money from cigarette smugglers in exchange for allowing counterfeit and illicit tobacco into Afghanistan and China.[140,141]

The convergence of intellectual property crime and illicit actors is not just limited to TOC or terrorist-affiliated groups, but also extends to nation-state actors. For example, it was widely reported that North Korea facilitated the distribution of large volumes of counterfeit pharmaceuticals and cigarettes as a means to generate hard currency due to the state of sanctions; the country was also identified as sponsoring the crippling cyber-attacks against Sony Pictures Entertainment in 2014—an attack that deleted files from corporate hard drives, uploaded several unreleased films to the Internet, and leaked sensitive personal information regarding thousands of Sony employees.[142]

When state-sponsored malicious cyber actors target confidential business information and proprietary works and technologies for commercial gain, they put businesses and our national interests at risk. Similarly, when counterfeit goods such as fake computer and networking devices infiltrate global supply chains, they place the reliability of our communications and transportation networks at risk and introduce threats and vulnerabilities that could impact national security, while fake pharmaceuticals, electrical components, aircraft and automobile parts and other goods undermine public safety and other National interests.[143]

At this time, interested stakeholders such as industry associations, international organizations, news media, public interest groups, and academia may not be in a position to assess how widespread the convergence may be between intellectual property crime and TOC and/or terror-supporting entities. As a result, there is an opportunity to systematically collect and make more of this type of information available, in an appropriate manner, in order to raise awareness and understanding of IP crime and its links to serious crime and terror organizations, and to facilitate and improve the exchange of information and intelligence on IP crimes such as counterfeiting and piracy between the public and private sectors. See the Call for Research at the end of Section IV of this Strategic Plan for further discussion of related data and research needs.

The convergence between intellectual property-based crimes, transnational organized crime, and terrorist financing undermines the strength and security of democratic regimes by allowing illicit actors, for example, to forge alliances with corrupt foreign government officials, or otherwise destabilize political, financial, and security institutions in fragile states. Terrorists and insurgents increasingly turn to these criminal networks to generate funding and acquire logistical support.[144] Put simply, the exploitation of intellectual property rights by criminal syndicates appears to be posing an increasing threat to National and global security interests.

This Strategic Plan addresses the issues discussed above by proposing improvements to the enforcement of domestic IP rights, cooperation with foreign governments, use of trade tools, and voluntary private-sector best practices (consistent with the antitrust laws), to name a few, while being mindful that these issues are complex and ever-changing. The following sections seek to build on what already has been accomplished, while continuing to look ahead. Now, more than ever, it is important that the public, law enforcement officials, policy makers, and all other stakeholders remain vigilant against the mounting threats from entities that seek to unlawfully misappropriate and exploit the intellectual property interests belonging to others.

THIS PAGE IS INTENTIONALLY LEFT BLANK

ENDNOTES

[1] U.S. Department of Commerce, *"Intellectual Property and the U.S. Economy: Industries in Focus"* (March 2012), accessed from https://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf.

[2] *See* U.S. Department of Commerce, *"Intellectual Property and the U.S. Economy: 2016 Update,"* (September 2016), accessed from https://www.uspto.gov/sites/default/files/documents/IP-andtheUSEconomySept2016.pdf.

[3] Message by President Obama on World Intellectual Property Day (April 26, 2016), accessed from https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Documents/EMessage%20World%20Intellectual%20Property%20Day.pdf.

[4] Copyrights and trademarks are the most commonly violated intellectual property rights for both hard goods and online content. As a result, this Section emphasizes these intellectual property interests. Of course, there are certain activities or products that may constitute an infringement of patent rights independent from, or in combination with, one or more other intellectual property right(s). For example, a counterfeit electronic device such as a smartphone may implicate the infringement of a trademark, a copyright, and a patent right. Patent interests that are independent of counterfeiting and piracy are addressed more extensively in Section IV of this Plan.

[5] *See* Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("PRO-IP Act"), Pub. L. No. 110-403, 122 Stat. 4256 (2008).

[6] Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("PRO-IP Act"), Pub. L. No. 110-403, 122 Stat. 4256 (2008) (emphasis added).

[7] An example that illustrates the importance of the Federal Government being aware of and seeking to keep up with technological innovations and new business models is the case of cell phone unlocking. When cell phone unlocking lost exemption status under the Digital Millennium Copyright Act, consumers lost the ability to shop for a mobile phone provider using the device they had purchased because "unlocking" a device would circumvent technical access mechanisms that are often used to protect copyright. After over 100 thousand Americans petitioned the Federal Government to restore the exemption, the U.S. Congress and the Executive Branch acted and the Unlocking Consumer Choice and Wireless Competition Act, Pub. L. No. 113-144, 128 Stat. 1751 (2014), was passed, so that the strong protections that prevent illicit actors from stealing copyrighted works would not create unintended consequences that lessened the ability for a consumer to take their business where they choose.

[8] General Keith Alexander (ret.), while Director of the National Security Agency and Commander of U.S. Cyber Command, estimated that U.S. companies lose approximately $250 billion per year due to the theft of their intellectual property. *See* Rogin, Josh, "*NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history*," The Cable (July 9, 2012), accessed from http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

[9] *See* Section I.

[10] *See* Section III.

[11] *See* U.S. Government Accountability Office ("GAO"), "*Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*" (April 2010), at p.16, accessed from http://www.gao.gov/assets/310/303057.pdf.

[12] *See* Congressional Research Service, "*Protection of Trade Secrets: Overview of Current Law and Legislation*" (April 22, 2016) at pp.13-14, accessed from http://www.fas.org/sgp/crs/secrecy/R43714.pdf (listing a number of factors impeding more precise calculation of the economic impact of trade secret theft, including: (1) the fact that companies may not realize that their sensitive information has been stolen until years after the theft; (2) the belief that reporting security breaches to law enforcement could harm the company's reputation and stock prices, or damage its corporate relationships; (3) fear of offending potential customers or business partners by publicly accusing a foreign government or business competitor of trade secret theft; and (4) difficulty in measuring the monetary value of some forms of sensitive information). *See also* Department of Justice, American Journal Of Trial Advocacy, "*Your Secrets Are Safe With Us: How Prosecutors Protect Trade Secrets During Investigation and Prosecution*," Vol. 38:461 (2016) at p.463, accessed from http://www.justice.gov/criminal-ccips/file/640271/download (observing, "Despite the potential advantages of federal prosecution, some victims of trade secret theft have been reluctant to involve the Justice Department when investigating suspected thefts. Among other reasons, victims have expressed concern that inviting a criminal investigation and prosecution will increase the likelihood of the trade secret becoming publicly revealed during investigation or at trial.").

[13] *See* Organization for Economic Cooperation and Development (OECD), "*The Economic Impact of Counterfeiting and Piracy*" (2008) (hereinafter "2008 OECD Report"), accessed from http://www.oecd.org/sti/ind/theeconomicimpactofcounterfeitingandpiracy.htm, as updated by OECD, "*Magnitude of Counterfeiting and Piracy of Tangible Products: An Update*" (November 2009) (hereinafter "2009 OECD Report Update"), accessed from http://www.oecd.org/sti/ind/44088872.pdf. The quotations, regarding the estimates in the 2008 Report and the 2009 Update, are in the 2009 Update at pp. 1 and 3. In the 2008 Report, the estimate is at p.13 ("Analysis carried out in this report indicates that international trade in counterfeit and pirated products could have been up to USD 200 billion in 2005.").

[14] *See* OECD/European Union Intellectual Property Office, "*Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*" (2016) (hereinafter "2016 OECD Report") at p.68 (emphasis in the original), accessed from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Mapping_the_Economic_Impact_study/Mapping_the_Economic_Impact_en.pdf. In addition, the 2016 OECD Report estimated that **"as much as 5.1% of EU imports in 2013 was in counterfeit and pirated products."** *Id.* at p.76 (emphasis in original) ("this number represents an upper limit of counterfeit imports to the EU . . . the maximum possible amount of imports of counterfeit goods"). The 2016 OECD Report also indicated that, for at least one product category, the percentage of counterfeit goods could be significantly higher ("for some EU members, the incoming flows of counterfeit footwear from China tends to reach 27% of the total incoming trade in that product category . . . [this] represents the upper level of potential trade in

counterfeits, meaning that within the HS64 [footwear] category imported from China by some EU members, the share of counterfeits was reaching 27% in some years"). *Id.* at p.67.

[15] 2016 OECD Report at p.68 (emphasis in original). The Report explained that "[t]he term 'as much as' is crucial in this context as it refers to the upper boundary of counterfeit trade."

[16] 2008 OECD Report at p.13. *See also* 2009 OECD Report Update at p.1 ("Based on the framework developed in OECD (2008) this short report updates the quantitative results of that study by utilising more recent international trade statistics for the calendar years 2000 to 2007. This report does not, however, update the customs interception data on which the original framework was constructed and relies on the same, aggregated customs interception data (*i.e.* for 1999-2005).").

[17] *See* International Chamber of Commerce, "*Estimating the global economic and social impacts of counterfeiting and piracy*" (February 2011) at pp. 5 (2008 estimates and 2015 projection) and 50 (2015 projection), accessed from http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/.

[18] *See, e.g.*, Office of the National Counterintelligence Executive, "*Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*," (October 2011) at p.3, ("The theft of trade secrets from US companies by foreign economic rivals undermines the corporate sector's ability to create jobs, generate revenues, foster innovation, and lay the economic foundation for prosperity and national security"), accessed from https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[19] *See* Rowe, Elizabeth A., "Contributory Negligence, Technology, and Trade Secrets," 17 *George Mason L. Rev.*, 1, 5 (2009), accessed from http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1060&context=facultypub. https://www.uschamber.com/sites/default/files/legacy/international/files/Final TPP Trade Secrets 8_0.pdf *See also* Politico.com, Op-Ed by Senators Orrin Hatch and Chris Coons, "A Better Way To Protect Trade Secrets" (April 4, 2016), ("According to some estimates, trade secrets are worth $5 trillion to the U.S. economy, on par with patents"), accessed from http://www.politico.com/agenda/story/2016/04/a-better-way-to-protect-trade-secrets-000081#ixzz4DpHlmVNQ.

[20] *See* The Center for Responsible Enterprise And Trade and PricewaterhouseCoopers LLP, "*Economic Impact of Trade Secret Theft*" (February 2014) at p.3, accessed from https://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf.

[21] General Keith Alexander (ret.), while Director of the National Security Agency and Commander of U.S. Cyber Command, estimated that U.S. companies lose approximately $250 billion per year due to the theft of their intellectual property. *See* Rogin, Josh, "*NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history*," The Cable (July 9, 2012), accessed from http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history. *See also* Testimony of Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism (May 13, 2014), ("The Office of the National Counterintelligence Executive, using estimates from academic literature, has estimated losses from economic espionage to be in the tens or even hundreds of billions of dollars annually to the American economy"), accessed from https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft; *see also* The National Bureau of Asian Research, "*The Report of the Commission on the Theft of American Intellectual Property*," (May 2013) ("The USITC reported that in 2009 U.S. firms in the IP-intensive economy lost roughly $1.1 billion from the misappropriation of trade secrets to China alone," *citing* U.S. International Trade Commission, "*China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*," no. 332-519, USITC Publication 4226 (May 2011) at pp.3-37, accessed from: https://www.usitc.gov/publications/332/pub4226.pdf), accessed from http://www.ipcommission.org/report/ip_commission_report_052213.pdf; *see also* American Intellectual Property Law Association, "*Response to Request for Public Comments for 'Trade Secret Theft Strategy Legislative Review' (78 Fed. Reg. 16875)*" (April 22, 2013) at p.1, ("Last year, the National Security Agency described trade secret theft as the greatest transfer of wealth in history, estimating the losses of trade secret theft and cyber breaches to be in excess of $334 billion per year"), accessed from http://www.aipla.org/advocacy/executive/Documents/AIPLA%20Letter%20to%20IPEC%20on%20Trade%20Secrets%20-%204.22.13.pdf.

[22] *See* United States Department of Justice, Office of Public Affairs, "*Kolon Industries Inc. Pleads Guilty for Conspiring to Steal DuPont Trade Secrets Involving Kevlar Technology*" (April 30, 2015) (*quoting* Special Agent in Charge Lee: "each year, billions of U.S. dollars are lost to foreign competitors who pursue illegal commercial short cuts by stealing valuable advanced technologies. This case demonstrates the FBI's ability to penetrate these highly sophisticated criminal schemes and bring their perpetrators to justice. Its outcome should send a clear message to foreign commercial actors who seek to illegally exploit American companies and steal our nation's innovation and technology."), accessed from https://www.justice.gov/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar.

[23] *See*, Deloitte, "*Beneath the Surface of a Cyberattack – A Deeper Look at Business Impacts*" (2016) at p.2, ("The costs commonly associated with data breaches are only the most widely understood impacts, the damage seen above the surface. But theft of PII is not always an attacker's objective. Rarely brought into full view are cases of intellectual property (IP) theft, espionage, data destruction, attacks on core operations, or attempts to disable critical infrastructure. Beneath the surface, these attacks can have a much more significant impact on organizations. But the tolls they take are not broadly understood and are much more difficult to quantify"), accessed from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-gra-beneath-the-surface.pdf.

[24] *See* International Chamber of Commerce, "*Enhancing Intellectual Property Management and Appropriation by Innovative SMEs*," (October 2013) at pp.14–15, accessed from http://www.iccwbo.org/Advocacy-Codes-and-Rules/Areas-of-work/Intellectual-Property/Innovation-and-intellectual-property/.

[25] European Union Intellectual Property Office, *"Research on Online Business Models Infringing Intellectual Property Rights: Phase 1 - Establishing an Overview of Online Business Models Infringing Intellectual Property Rights"* (July 2016) at p.7 *et seq.*, accessed from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf.

[26] *See, e.g.*, Europol, "*The Internet Organised Crime Threat Assessment - Overview*" (2014) ("Criminals can misuse/abuse WHOIS data in a number of ways" including "[g]iving false WHOIS credentials to Registrars to avoid identification, in order to conduct illegal or harmful Internet activities" and "[u]sing of the private domain registration (domain names registered via privacy or proxy services or offshore) to obscure the perpetrator's identity"), accessed from https://www.europol.europa.eu/iocta/2014/chap-4-3-view1.html. *See also* European Union Intellectual Property Office, "*Research on Online Business Models Infringing Intellectual Property Rights: Phase 1 - Establishing an Overview of Online Business Models Infringing Intellectual Property Rights*" (July 2016) at p. 9 ("operators behind the IPR-infringing activities often either conceal their identities by using privacy shield services for the registration of their domain names or provide inadequate, false or otherwise misleading contact details on the website thus hampering or even precluding enforcement actions"), accessed from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf.

[27] *See* Europol and Office for Harmonization in the Internal Market, "*2015 Situation Report on Counterfeiting in the European Union*," (April 2015) at p.33, accessed from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/publications/2015+Situation+Report+on+Counterfeiting+in+the+EU.pdf. *See also* European Union Intellectual Property Office, "*Research on Online Business Models Infringing Intellectual Property Rights: Phase 1 - Establishing an Overview of Online Business Models Infringing Intellectual Property Rights*," (July 2016) at p. 9.

[28] Both Popcorn Time and The Pirate Bay—entities that have been included by the Office of the U.S. Trade Representative as representative "Notorious Markets" in the Out-of-Cycle Notorious Markets Review—have advertised and promoted anonymizing services alongside their respective listing of free movies, music and other content. *See* Office of the U.S. Trade Representative, "*2014 Out-of-Cycle Review of Notorious Markets*," (March 5, 2015) at pp. 5 and 17, accessed from https://ustr.gov/sites/default/files/2014%20Notorious%20Markets%20List%20-%20Published_0.pdf. *See also* Robertson, Adi, "*Popcorn Time's Best-known App Comes Back to Life,*" The Verge (February 26, 2016) (reporting that torrent streaming application Popcorn Time added "a paid VPN anonymizing service alongside its free movies"), accessed from http://www.theverge.com/2016/2/26/11119290/popcorn-time-io-movie-streaming-piracy-back-online. *See also* Stone, Jeff. "*The Pirate Bay Pushing Free VPN Amid Blockade, Torrent Site Facing New International Scrutiny,*" International Business Times (October 25, 2014) ("Swedish torrent site Pirate Bay in the past few days prominently featured advertisements for a free virtual-private network, or VPN"), accessed from http://www.ibtimes.com/pirate-bay-pushing-free-vpn-amid-blockade-torrent-site-facing-new-international-scrutiny-1713144.

[29] European Union Intellectual Property Office, *"Research on Online Business Models Infringing Intellectual Property Rights: Phase 1 - Establishing an Overview of Online Business Models Infringing Intellectual Property Rights"* (July 2016) at pp.31-37, accessed from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf.

[30] *See* Section II.

[31] In this context, adware is designed to co-opt the consumer's computer into advertising fraud schemes. It is highly invasive software, running the background, designed to make money by serving pop-ups to the user even when s/he is not browsing, and by collecting the user's personal data to identify and target delivery of the most profitable ads relevant to that user.

[32] *See* Digital Citizens Alliance, "*Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data,*" (December 2015) at p.9 *et seq.*, ("A botnet is a system of connected computers acting as a group at the command of a 'Bot controller,' who directs the enslaved computers to accomplish certain tasks, such as to carry out spam and phishing campaigns and to fake advertising traffic"), accessed from https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf.

[33] Digital Citizens Alliance, "*Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data,*" (December 2015) at p.1 ("the cyber security firm RiskIQ found that one out of every three content theft sites contained malware. The study found that consumers are 28 times more likely to get malware from a content theft site than on similarly visited mainstream websites or licensed content providers"), accessed from https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf. *See also* Federal Bureau of Investigation, "*Consumer Alert: Pirated Software May Contain Malware,*" (August 1, 2013) ("Our collective experience has shown this to be true, both through the complaints we've received and through our investigations. It's also been validated by industry studies, which show that an increasing amount of software installed on computers around the world—including in the U.S.—is pirated and that this software often contains malware"), accessed from https://www.fbi.gov/news/stories/pirated-software-may-contain-malware1; Ernst & Young, "*IAB U.S. Benchmarking Study: What is an untrustworthy supply costing the US digital advertising industry?*" (November 2015) (finding that fraudulent impressions, infringed content, and malvertising cost the U.S. digital marketing, advertising, and media industry $8.2 billion annually), accessed from http://www.iab.com/wp-content/uploads/2015/11/IAB_EY_Report.pdf; European Union Intellectual Property Office, "*Digital Advertising on Suspected Infringing Websites,*" (January 2016) at pp.23-24 (discussing the relative prevalence of click generators and malware in "high risk sector" online advertisements in the EU), accessed from https://euipo.europa.eu/ohimportal/documents/11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites; European Union Intellectual Property Office (EU IPO), *"Research on Online Business Models Infringing Intellectual Property Rights,"* (July 2016) at p.4 ("IPR is also being used to disseminate malware, carry out illegal phishing and simple fraud"), accessed from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf.

[34] European Union Intellectual Property Office (EU IPO), "*Research on Online Business Models Infringing Intellectual Property Rights*: Phase 1 - Establishing an Overview of Online Business Models Intellectual Property Rights" (July 2016) at p.4, accessed

from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf.

[35] *See* Microsoft.com, "*Breaking New Ground to Fight Online Piracy*" (March 5, 2013), accessed from http://blogs.microsoft.com/on-the-issues/2013/03/05/breaking-new-ground-to-fight-online-piracy/.

[36] *See* Microsoft.com, "*Breaking New Ground to Fight Online Piracy*" (March 5, 2013), accessed from http://blogs.microsoft.com/on-the-issues/2013/03/05/breaking-new-ground-to-fight-online-piracy/.

[37] Office of the United States Trade Representative, "*2016 Special 301 Report*," (2016) pp.19-20, accessed from https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.

[38] *See, e.g.*, Schouten, Christopher, *et. al.*, "*The New Face of Pay-TV Piracy and How to Fight It*," (2016) pp.3-5 (summarizing evolution of piracy, from signal piracy, to P2P and web piracy, to IPTV piracy), accessed from https://www.kudelskisecurity.com/sites/default/files/files/Kudelski%20Security_The%20New%20Face%20of%20Pay-TV%20Piracy%20and%20How%20to%20Fight%20it_White%20Paper.pdf.

[39] *See, e.g.*, Deloitte, *"Television's Business Model: Fit for a Digital World"* (2014), accessed from http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-ibc-report-2014.pdf. Increasingly, "over the top" (OTT) content providers like Netflix and Amazon are producing original programming for distribution, integrating the content production and distribution streams. *See, e.g.*, Huddleston, Jr., Tom, "*Netflix Could Win Big at the 2016 Emmys,*" (Fortune: Sept. 16, 2016) ("The company is spending a reported $5 billion this year on its ever-expanding roster of original series and films. It plans to churn out roughly 600 hours of original programming in 2016"), accessed from http://fortune.com/2016/09/16/emmys-preview-netflix/.

[40] *See, e.g.*, U.K. Intellectual Property Office, "*Protecting Creativity, Supporting Innovation: IP Enforcement 2020"* (2016) at p.20, accessed from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/522847/IP-Enforcement-Strategy.pdf.

[41] *See, e.g.*, National Intellectual Property Rights Coordination Center, "*Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad*," (November 2011) at p. iv, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/.

[42] *See, e.g.*, National Intellectual Property Rights Coordination Center, *"Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad,"* (November 2011) at p.iv, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/. *See also* U.S. Government Accountability Office, "*Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*," (April 2010) at p.10 ("counterfeiters have increasingly diversified beyond their traditional products, such as luxury goods, to more functional products such as baby shampoo and household cleaners, and will continue to expand their product portfolios since the profit incentives are large"), accessed from http://gao.gov/new.items/d10423.pdf.

[43] *See* National Intellectual Property Rights Coordination Center, "*Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad*," (November 2011) at pp.iv,18, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/.

[44] *See* Organization for Economic Co-operation and Development, "*The Economic Impact of Counterfeiting and Piracy: Executive Summary*," (2007) at p. 5, accessed from https://www.oecd.org/sti/38707619.pdf.

[45] *See* International Trademark Association (INTA), "*Fact Sheet: Protecting a Trademark*," (April 2015) ("To deceive consumers into thinking that a product sold online at a discounted price is the real thing, online sellers of counterfeits often advertise the discounted product under a nice photo of the real product. Only after the consumer has received the product in the mail will that consumer realize that he or she has been tricked into buying a counterfeit."), accessed from http://www.inta.org/TrademarkBasics/FactSheets/Pages/Counterfeiting.aspx [subscription required]. *See also*, Jacobs, Deborah, "*Online Scams Lure Shoppers With 'Luxury' Handbag Ripoffs*," (Forbes.com: April 17, 2014) ("The proliferation of online sites…makes it easier than ever to get snookered. Some have professional sounding names; include pictures that look like the real thing…and price merchandise so it seems like they're discounting the real thing, rather than overcharging for a knockoff."), accessed from http://www.forbes.com/sites/deborahljacobs/2014/04/17/online-scams-lure-shoppers-with-luxury-handbag-ripoffs/#73f780b129fe; City of London Police, *"Two Arrested in 'Wake Up—Don't Fake Up!' Campaign,"* (May 21, 2015) accessed from https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Two-arrested-in-'Wake-up-—-don't-fake-up!'-campaign.aspx.

[46] *See* United Nations Office on Drugs and Crime, "*Transnational Organized Crime in East Asia and the Pacific: A Threat Assessment*" (2013) at p.125, accessed from https://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_EAP_web.pdf.

[47] *See* McNiff, Eamon, *et al.*, "*Counterfeiter Tricks of the Trade: How Fake Goods Might Get Past Inspectors*," (ABC News: May 13, 2015), accessed from http://abcnews.go.com/US/counterfeiter-tricks-trade-fake-goods-past-inspectors/story?id=30961441. *See also* Section III.

[48] United States Department of Homeland Security, Customs and Border Protection, "*Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,*" (April 2016) at p.10 (stating that, by dollar value, 52 percent of goods seized by CBP in FY 2015 originated in China, and 35 percent in Hong Kong), accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Apr/FY%202015%20IPR%20Stats%20Presentation.pdf.

[49] *See* European Union, "*Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border 2015,*" (2016) at p.19 (stating that, by dollar value, 58.37 percent of goods seized by EU customs in FY 2015 originated in China, and 20.23 percent in Hong Kong), accessed from https://ec.europa.eu/taxation_customs/sites/taxation/files/2016_ipr_statistics.pdf.

[50] *See* United States Department of Homeland Security, Customs and Border Protection, "*Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,*" (April 2016) at p.10, accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Apr/FY%202015%20IPR%20Stats%20Presentation.pdf. *See also* United States Trade Representative, "*2015 Special 301 Report,*"

(2015) accessed from https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf; World Customs Organization (WCO), "*Illicit Trade Report 2014*," (December 2015) at p.66, accessed from http://www.wcoomd.org/en/media/newsroom/2015/december/~/media/6FDFF08E365E49D49C0B6DC375C492B5.ashx.

[51] 2016 OECD Report, at pp.13, 43.

[52] 2016 OECD Report, at p.13.

[53] 2016 OECD Report, at pp.13, 43.

[54] World Economic Forum "*Global Agenda Council on Organized Crime: Organized Crime Enablers*," (July 2012) at p.21, accessed from http://www3.weforum.org/docs/WEF_GAC_OrganizedCrimeEnablers_Report_2012.pdf.

[55] Europol and the Office for Harmonization in the Internal Market, "*2015 Situation Report on Counterfeiting in the European Union*," (April 2015) at p.16, accessed from https://www.europol.europa.eu/content/2015-situation-report-counterfeiting-european-union.

[56] *See*, 2016 OECD Report, at p.76.

[57] *See*, 2016 OECD Report, at p.61.

[58] *See* World Economic Forum "*Global Agenda Council on Organized Crime: Organized Crime Enablers*," (July 2012) at p.5, accessed from http://www3.weforum.org/docs/WEF_GAC_OrganizedCrimeEnablers_Report_2012.pdf.

[59] Europol and the Office for Harmonization in the Internal Market "*2015 Situation Report on Counterfeiting in the European Union*," (April 2015) at p.16, accessed from https://www.europol.europa.eu/content/2015-situation-report-counterfeiting-european-union; International Chamber of Commerce Business Action to Stop Counterfeiting and Piracy (BASCAP), "*Controlling the Zone: Balancing Facilitation and Control to Combat Illicit Trade in the World's Free Trade Zones*" (May 2013) at p.1, accessed from http://www.iccwbo.org/advocacy-codes-and-rules/bascap/international-engagement-and-advocacy/free-trade-zones/. *See also* International Trademark Association (INTA) "*Resolution of the Anti-Counterfeiting & Enforcement Committee (ACEC): Role of Free Trade Zones and Free Ports in the Transshipment and Transit of Counterfeit Goods*," (November 2006), accessed from http://www.inta.org/Advocacy/Pages/RoleofFreeTradeZonesandFreePortsintheTransshipmentandTransitofCounterfeitGoods.aspx.

[60] World Customs Organization, "*Illicit Trade Report 2014*," (2015) at p. 71, accessed from http://www.wcoomd.org/en/media/newsroom/2015/december/~/media/6FDFF08E365E49D49C0B6DC375C492B5.ashx.

[61] United Nationals Office on Drugs and Crime (UNODC) and World Customs Organization, "*Global Container Analysis Report 2008*," (2008) at p.50, accessed from http://www.mcmullinpublishers.com/downloads/OMDrcEN08.pdf.

[62] *See, e.g.*, United States Government Accountability Office, "*GAO-13-560: Internet Pharmacies: Federal Agencies and States Face Challenges Combating Rogue Sites, Particularly Those Abroad*," (July 2013) at pp.19-20, accessed from http://www.gao.gov/assets/660/655751.pdf. See also Toscano, Paul, "*The Dangerous World of Counterfeit Prescription Drugs*" (CNBC: October 4, 2011), accessed from http://www.cnbc.com/id/44759526 (reporting that in one case that led to seizures, "counterfeit drugs produced in China were transported by road to Hong Kong, sent by air to Dubai, passing through London Heathrow on the way to the Bahamas, where the organization kept a warehouse fulfillment center. From there, the drugs were sent to another organization in the U.K., which eventually sent the packages to the U.S."). *See also* Kovacs, Laszlo, European Commissioner for Taxation and Customs Union, "*Press Conference: EU Customs' fight against the dangers of counterfeiting*" (October 11, 2006) at pp.2-3 ("earlier this year, a shipment of 350 kg of fake pharmaceuticals, which were stopped in the UK, were dispatched from China transiting through the United Arab Emirates, and then UK with a final destination in the Bahamas. The process is even more complicated because this was an internet order placed from Canada"), accessed from https://ec.europa.eu/taxation_customs/sites/taxation/files/docs/body/counterfeit_statistics2005_2006_11_10.pdf. *See also* Bogdanich, Walt, "*Counterfeit Drugs' Path Eased by Free Trade Zones*" (The New York Times: December 17, 2007) ("[A]n examination of the case reveals its link to a complex supply chain of fake drugs that ran from China through Hong Kong, the United Arab Emirates, Britain and the Bahamas, ultimately leading to an Internet pharmacy whose American customers believed they were buying medicine from Canada, according to interviews with regulators and drug company investigators in six countries."), accessed from http://www.nytimes.com/2007/12/17/world/middleeast/17freezone.html?_r=0.

[63] *See* Section II. *See also* European Union Intellectual Property Office, "*Research on Online Business Models Infringing Intellectual Property Rights:* Phase 1 - Establishing an Overview of Online Business Models Intellectual Property Rights" *(Phase 1)*" (July 2016) at pp. 4-9, accessed from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf.

[64] *See* Section II.

[65] *See* Statement of Randall C. Coleman, Assistant Director Counterintelligence Division, Federal Bureau of Investigation, before the U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, "*Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?*" (May 13, 2014), accessed from https://www.judiciary.senate.gov/imo/media/doc/05-13-14ColemanTestimony.pdf.

[66] *See. e.g,* United States Department of Justice, Federal Bureau of Investigation, "*The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*," accessed from https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

[67] *See* Office of the Press Secretary, The White House, "*Fact Sheet: Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*," (April 1, 2015), accessed from https://www.whitehouse.gov/the-press-office/2015/04/01/fact-sheet-executive-order-blocking-property-certain-persons-engaging-si.

[68] *See* United States Office of the National Counterintelligence Executive, "*Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*," (October 2011) at p.i, accessed from https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[69] G20 Leaders' Communique, Antalya, Turkey, (November 16, 2015), accessed from http://pm.gc.ca/eng/news/2015/11/16/g20-leaders-communique.

[70] *See* The White House, "*Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*," (July 2011), accessed from https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf

[71] *See, e.g.*, International Chamber of Commerce Business Action to Stop Counterfeiting and Piracy (BASCAP) and Frontier Economics, "*Estimating the global economic and social impacts of counterfeiting and piracy*," (February 2011), accessed from http://www.iccwbo.org/Data/Documents/Bascap/Global-Impacts-Study---Full-Report/; United States Government Accountability Office, *"GAO-10-423: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods,"* (April 2010), accessed from http://www.gao.gov/assets/310/303057.pdf.

[72] *See* United States Department of Commerce, "Intellectual Property and the U.S. Economy: 2016 Update" (September 2016), accessed from https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.

[73] *See* United States Department of Homeland Security, "*Intellectual Property Rights Seizure Statistics: Fiscal Year 2015*," at p.17, accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Apr/FY%202015%20IPR%20Stats%20Presentation.pdf. *See also* National Intellectual Property Rights Coordination Center, "*Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad,*" (November 2011) at p.20, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/view.

[74] The number of personal care items seized by the U.S. Department of Homeland Security in FY 2015 was 1,836, a 16 percent increase from 1,578 items seized in FY 2014. *See* United States Department of Homeland Security, "*Intellectual Property Rights Seizure Statistics: Fiscal Year 2015*," at p.17, accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Apr/FY%202015%20IPR%20Stats%20Presentation.pdf. *See also* National Intellectual Property Rights Coordination Center, "*Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad,*" (November 2011) at p.20, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/view.

[75] *See* United States Department of Justice, "*Prosecuting Intellectual Property Crimes*" (United States Attorneys' Bulletin Vol. 64, No. 1: January 2016) at p.36, accessed from https://www.justice.gov/usao/file/813026/download.

[76] United States Department of Homeland Security, U.S. Customs and Border Protection, *"Joint Operation Seizes Critical Counterfeit Beauty Personal Care Products,"* (June 17, 2015), accessed from https://www.cbp.gov/newsroom/national-media-release/2015-06-17-000000/joint-operation-seizes-critical-counterfeit-beauty.

[77] 21 U.S.C. Sec. 301 *et. seq*.

[78] *See* United States Department of Justice, "*Prosecuting Intellectual Property Crimes*" (United States Attorneys' Bulletin Vol. 64, No. 1: January 2016) at p.36, accessed from https://www.justice.gov/usao/file/813026/download.

[79] United States Department of Homeland Security, Customs and Border Protection, *"Joint Operation Seizes Critical Counterfeit Beauty Personal Care Products"* (June 17, 2015), accessed from https://www.cbp.gov/newsroom/national-media-release/2015-06-17-000000/joint-operation-seizes-critical-counterfeit-beauty. *See also* United States Department of Justice, Federal Bureau of Investigation, "*Counterfeit Cosmetics, Fragrances: Hazardous to Your Health*" (Jan. 2, 2014), accessed from https://www.fbi.gov/news/stories/counterfeit-cosmetics-fragrances; City of London Police, Police Intellectual Property Crime Unit (PIPCU), "*PIPCU urges the public to 'Wake up – don't fake up!'*," (May 22, 2015), accessed from https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/wakeupdontfakeup/Pages/wakeupdontfakeup.aspx.

[80] *See, e.g.*, Zulueta, Adrienna, *Massive fake health and beauty supplies ring busted,"* (CNN.com: March 9, 2014) (reporting that the seizures of "counterfeits included everyday health and beauty items such as ChapStick, Johnson's Baby Oil, Vaseline and Always sanitary pads"), accessed from http://www.cnn.com/2014/03/08/justice/new-york-counterfeit-beauty-supplies/index.html.

[81] *See* United States Department of Homeland Security, "*Intellectual Property Rights Seizure Statistics: Fiscal Year 2015*," accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Apr/FY%202015%20IPR%20Stats%20Presentation.pdf.

[82] *See, e.g.*, Arnold, Ben, *"Insights and Opinions from Analysts and Experts in more than 20 Industries,"* (NPG Group Blog: August 24, 2015) (in the U.S., from July 2014 to July 2015, sales of headphones totaled $2.9 billion, with Beats by Dre and Bose commanding 81% of the premium headphone market) accessed from https://www.npd.com/wps/portal/npd/us/blog/2015/summers-end-no-match-for-stereo-headphone-sales. *See also* Nylander, Johan, "*Chinese Fakes Cash in on Dr. Dre's Beats Headphones Bonanza,"* (CNN.com: October 13, 2013) (finding that a counterfeiting operation in China was willing to deliver 100 units of Beats products in a day, and 1,000 units in a week), accessed from http://www.cnn.com/2013/10/13/business/china-fake-headphones-dr-dre-beats.

[83] *See* Underwriters Laboratories, "*Counterfeit iPhone Adapters: A UL Technical Investigation Shows a 99 Percent Failure Rate*," (2016) (hereinafter "UL Report"), accessed from library.ul.com/wp-content/uploads/sites/40/2016/09/10314-Counterfeiti-Phone-WP-HighRes_FINAL.pdf.

[84] UL Report at 2.

[85] UL Report at 5.

[86] *See* World Customs Organization, "*WCO Members join together to fight imports of substandard and counterfeit electrical products*," (October 24, 2011), accessed from http://www.wcoomd.org/en/media/newsroom/2011/october/wco-members-join-together-to-fight-imports-of-substandard-and-counterfeit-electrical-products.aspx. *See also* United States Consumer Product Safety Commission, "*May is National Electrical Safety Month: CPSC Warns of Dangerous Counterfeit Electrical Products*" (May 9, 2007), accessed from http://www.cpsc.gov/en/newsroom/news-releases/2007/may-is-national-electrical-safety-monthcpsc-warns-of-dangerous-counterfeit-electrical-products/; Consumer Reports, "*Counterfeit Goods: How to Tell the Real From the Rip-off*" (May 28, 2015), accessed from http://www.consumerreports.org/cro/magazine/2015/05/counterfeit-goods-how-to-tell-real-from-ripoff/index.htm.

[87] *See* United Nations Office on Drugs and Crime, "*Focus On: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime*," accessed from https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf.

[88] *See, e.g.*, United States Department of Homeland Security, Customs and Border Protection, "*CBP Office of Trade—IPR Division: Hoverboard Enforcement Update, June 2016*," accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Jul/2016_06_Hoverboard%20Enforcement%20Update.pdf.

[89] *See, e.g.*, United States Department of Homeland Security, Customs and Border Protection, "*Intellectual Property Rights Seizure Statistics - Fiscal Year 2013*," accessed from https://www.cbp.gov/sites/default/files/documents/ipr_annual_report_2013_072414%20Final.pdf.

[90] The Economist, *"Fake Pharmaceuticals - Bad Medicine: The World's Drug Supply Is Global. Governments Have Failed To Keep Up"* (October 13, 2012), accessed from http://www.economist.com/node/21564546.

[91] *See* National Intellectual Property Rights Coordination Center, "*Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad*," (November 2011) at p.30, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/view.

[92] United States Food and Drug Administration, *"Testimony of Howard Sklamberg before the Committee on Energy and Commerce Subcommittee on Oversight and Investigations,"* (February 27, 2014), accessed from http://www.fda.gov/NewsEvents/Testimony/ucm387449.htm.

[93] Reichelt, Kevin M., International Intellectual Property Institute, "*Avoiding Counterfeit Goods: A How-To Guide for Consumers,"* accessed from http://iipi.org/wp-content/uploads/2010/07/Identifying_Counterfeit_Goods_-_A_Guide_for_Consumers.pdf. Boric acid is a monobasic Lewis acid of boron often used as a pesticide. It can cause gastrointestinal problems and renal failure.

[94] *See* INTERPOL, "*Pharmaceutical Crime Operations: "Operation Pangea,*" accessed from http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations

[95] Reichelt, Kevin M., International Intellectual Property Institute, "*Avoiding Counterfeit Goods: A How-To Guide for Consumers,"* accessed from http://iipi.org/wp-content/uploads/2010/07/Identifying_Counterfeit_Goods_-_A_Guide_for_Consumers.pdf; Somra, Gene, *"Patients fooled by fake drugs made with poison and brick dust,"* (CNN.com: August 30, 2015), accessed from http://www.cnn.com/2015/08/30/asia/pakistan-fake-drugs/.

[96] 2008 OECD Report at p.68.

[97] *See* World Health Organization, *"Fact Sheet: Substandard, spurious, falsely labelled, falsified and counterfeit (SSFFC) medical products,"* (Updated January 2016), accessed from http://www.who.int/mediacentre/factsheets/fs275/en/.

[98] *See* World Health Organization, *"Fact Sheet: Substandard, spurious, falsely labelled, falsified and counterfeit (SSFFC) medical products"* (Updated January 2016), accessed from http://www.who.int/mediacentre/factsheets/fs275/en/.

[99] *See* INTERPOL, "*Operations—Pangea VIII*" (June 2015), accessed from http://www. interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea. The U.S. National Intellectual Property Rights Center coordinated with INTERPOL to support Operation Pangea, an effort that brought together 115 countries and 236 agencies to combat the sale of illegal medicines online.

[100] Office of the United States Trade Representative, "*2016 Special 301 Report*," (April 2016) at p.17, accessed from https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.

[101] *See* INTERPOL, "*Operations—Pangea VIII*" (June 2015), accessed from http://www. interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea. *See also* United States Food and Drug Administration, "*BeSafeRX: Know Your Online Pharmacy*," accessed from http://www.fda.gov/drugs/resourcesforyou/consumers/buyingusingmedicinesafely/buyingmedicinesovertheinternet/besaferxknowyouronlinepharmacy/default.htm; The Center for Safe Internet Pharmacies, *"The Internet Pharmacy Market in 2016"* (January 2016), accessed from https://safemedsonline.org/wp-content/uploads/2016/01/The-Internet-Pharmacy-Market-in-2016.pdf.

[102] *See* United States Food and Drug Administration, "*FDA Unit Pursues Illegal Web Pharmacies*" (January 15, 2014), accessed from http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm381534.htm. *See also* The Center for Safe Internet Pharmacies, *"The Internet Pharmacy Market in 2016"* (January 2016), accessed from http://www.safemedsonline.org/wp-content/uploads/2016/01/The-Internet-Pharmacy-Market-in-2016.pdf.

[103] *See* National Association of Boards of Pharmacy, "*Internet Drug Outlet Identification Program*" (July 2013), accessed from https://awarerx.s3.amazonaws.com/system/redactor_assets/documents/237/NABP_Internet_Drug_Outlet_Report_July2013.pdf.

[104] *See* United States Department of Homeland Security, "*Intellectual Property Rights Center warns of counterfeit auto parts*," (October 2, 2014), accessed from https://www.ice.gov/news/releases/intellectual-property-rights-center-warns-counterfeit-auto-parts.

[105] *See* United States Department of Transportation, National Highway Traffic Safety Administration (NHTSA), "*Safety Advisory: NHTSA Alerting Consumers to Dangers of Counterfeit Air Bags*" (NHTSA 42-12: October 10, 2012), accessed from http://www.nhtsa.gov/About+NHTSA/Press+Releases/2012/Safety+Advisory:+NHTSA+Alerting+Consumers+to+Dangers+of+Counterfeit+Air+Bags. *See also* NHTSA, "*Counterfeit Air Bags Information*," accessed from http://www.safercar.gov/Vehicle+Shoppers/Air+Bags/Counterfeit+Air+Bags+General+Information.

[106] *See* United States Department of Homeland Security, "*Intellectual Property Rights Center warns of counterfeit auto parts*," (October 2, 2014), accessed from https://www.ice.gov/news/releases/intellectual-property-rights-center-warns-counterfeit-auto-parts.

[107] *See* United States Department of Homeland Security, "*Intellectual Property Rights Center warns of counterfeit auto parts*," (October 2, 2014), accessed from https://www.ice.gov/news/releases/intellectual-property-rights-center-warns-counterfeit-auto-parts.

[108] *See* United States Department of Homeland Security, "*Intellectual Property Rights Center warns of counterfeit auto parts*," (October 2, 2014) (noting that the "use of illegal

counterfeit automotive parts is increasing in the United States," and that the trend line is "growing at an alarming rate"), accessed from https://www.ice.gov/news/releases/intellectual-property-rights-center-warns-counterfeit-auto-parts.

[109] United States Department of Homeland Security, Customs and Border Protection, *"CBP Seizes Thousands of Counterfeit Auto Parts at Port Everglades,"* (May 15, 2015), accessed from https://www.cbp.gov/newsroom/local-media-release/2015-05-15-000000/cbp-seizes-thousands-counterfeit-auto-parts-port.

[110] *See* United Nations Office on Drugs and Crime, "*Counterfeit Products*," (2010) at p.174., accessed from https://www.unodc.org/documents/data-and-analysis/tocta/8.Counterfeit_products.pdf.

[111] *See* European Commission, DG Health and Food Safety, "*Ad-hoc Study on the Trade of Illegal and Counterfeit Pesticides in the EU*" (March 2015) (estimating counterfeit pesticides constitute up to 10% of Europe's crop protection market), accessed from https://croplife.org/wp-content/uploads/pdf_files/DG-Health-Food-Safety-study-on-the-trade-of-illegal-and-counterfeit-pesticides-in-the-EU-March-2015.pdf; Organization for Security and Co-operation in Europe (OSCE), "*Counteraction to Counterfeit and Contraband Pesticides*" (2015) (reporting that "[c]ounterfeit pesticides are estimated to be as high as 25% of the global pesticide market" with profitability in counterfeit pesticide trade making "it one of the top ten most lucrative organized crime businesses"), accessed from http://www.osce.org/secretariat/192516?download=true. *See also* Federation of Indian Chambers of Commerce and Industry (FICCI), "*Study On Substandard, Spurious/Counterfeit Pesticides in India*" (2015) (estimating trade in counterfeit pesticides in India at approximately USD 525 million per year, resulting in more than 10 million tons of food production loss each year), accessed from https://croplife.org/wp-content/uploads/2015/10/Study-on-sub-standard-spurious-counterfeit-pesticides-in-India.pdf.

[112] *See* Organization for Economic Co-operation and Development, "*The Economic Impact of Counterfeiting and Piracy: Executive Summary*," (2007) at p.17, accessed from https://www.oecd.org/sti/38707619.pdf.

[113] *See* Europol and the Office for Harmonization in the Internal Market, "*2015 Situation Report on Counterfeiting in the European Union*" (2015) at p.26, accessed from https://www.europol.europa.eu/sites/default/files/publications/2015situationreportoncounterfeiting.pdf. *See also* Europol, "*Huge Seizures of 190 Tonnes of Counterfeit Pesticides*" (December 18, 2015), accessed from https://www.europol.europa.eu/content/huge-seizures-190-tonnes-counterfeit-pesticides.

[114] *See* Europol, "*Europol Warns of Growing Trade in Counterfeit Pesticides Worth Billions of Euros a Year*," accessed from https://www.europol.europa.eu/content/europol-warns-growing-trade-counterfeit-pesticides-worth-billions-euros-year.

[115] *See* INTERPOL, "*Environmental Crime and its Convergence with other Serious Crimes*" (October 30, 2015), accessed from http://www.interpol.int/Media/Files/Crime-areas/Environmental-crime/INTERPOL-Strategic-Report-Environmental-Crime-and-its-Convergence-with-other-Serious-Crimes/. *See also* United Nations Office of Drugs and Crime, "*Transnational Organized Crime in East Asia and the Pacific: A Threat Assessment*," (April 2013) at pp.ix,117, accessed from https://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_EAP_web.pdf.

[116] *See* INTERPOL, "*Against Organized Crime: INTERPOL Trafficking And Counterfeiting Casebook 2014*," accessed from http://www.interpol.int/Media/Files/Crime-areas/Trafficking-in-Illicit-Goods/Against-Organized-Crime-INTERPOL-Trafficking-and-Counterfeiting-Casebook.

[117] *See* United States Immigration and Customs Enforcement, "*Michigan Computer Company, Owner Sentences for International Environmental and Counterfeiting Crimes*," (March 2013), accessed from https://www.ice.gov/news/releases/michigan-computer-company-owner-sentenced-international-environmental-and#wcm-survey-target-id.

[118] *See* Soetgen, Judith, "*Disposing of Counterfeit Goods: Unseen Challenges*," (WIPO Magazine: November 2012), accessed from http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html.

[119] *See* INTERPOL, "*Environmental Crime and its Convergence with other Serious Crimes*" (October 30, 2015), accessed from http://www.interpol.int/Media/Files/Crime-areas/Environmental-crime/INTERPOL-Strategic-Report-Environmental-Crime-and-its-Convergence-with-other-Serious-Crimes/.

[120] *See, e.g.*, United Nations Office on Drugs and Crime, *"The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime,"* accessed from https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf; Anti-Slavery International, "*Trafficking for Forced Criminal Activities and Begging in Europe"* (September 2014) at p.26 (noting that reports in the U.K. where foreign nationals were alleged to have been locked in warehouses, or children being forced to produce and sell pirated DVDs), accessed from http://www.antislavery.org/includes/documents/cm_docs/2014/t/2_trafficking_for_forced_criminal_activities_and_begging_in_europe.pdf.

[121] *See, e.g.*, United Nations Office on Drugs and Crime, *"The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime,"* accessed from https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf.

[122] *See, e.g.*, Europol, *"OCTA 2011: EU Organised Crime Threat Assessment,"* (2011) at p.36, accessed from https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf. *See also* International Labour Office Geneva, *"Labour Market Discrimination Against Migrant Workers in Italy,"* (September 2004), accessed from http://ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---migrant/documents/publication/wcms_201593.pdf.

[123] *See* Europol, *"OCTA 2011: EU Organised Crime Threat Assessment,"* (2011) at p.36, accessed from https://www.europol.europa.eu/sites/default/files/publications/octa2011.pdf. *See also* Organization for Economic Co-operation and Development, *"The Economic Impact of Counterfeiting,"* (1998) (noting that organized and petty criminals profit largely from counterfeiting), accessed from https://www.oecd.org/sti/ind/2090589.pdf.

[124] *See, e.g.*, United States Office of the Intellectual Property Enforcement Coordinator, *"Intellectual Property Spotlight"* (December 2010), at p.2, accessed from https://www.justice.gov/sites/default/files/dag/legacy/2011/01/05/ipec-ip-spotlight-dec2010.pdf. *See also* United States Department of Justice, *"Three Sentenced to Federal Prison for Forcing Labor and Distributing Pirated/Counterfeit CDs and DVDs,"* (October 14, 2011), accessed from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/lopezSent.pdf.

[125] United States Department of Justice, *"Three Sentenced to Federal Prison for Forcing Labor and Distributing Pirated/ Counterfeit CDs and DVDs,"* (October 14, 2011), accessed from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/lopezSent.pdf.

[126] *See* Statement of Gordon M. Snow, Assistant Director, United States Federal Bureau of Investigation, Cyber Division, Before the Senate Judiciary Committee, " (June 22, 2011), accessed from https://www.fbi.gov/news/testimony/intellectual-property-law-enforcement-efforts.

[127] United States Government Accountability Office, *"GAO-16-236: Counterfeit Parts—DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk,"* (February 2016) at p. 1, accessed from http://www.gao.gov/assets/680/675227.pdf; Report of the United States Committee on Armed Services, *"Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain,"* **(**May 21, 2012), accessed from http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf; *see also* Goldman David, *"Fake tech gear has infiltrated the U.S. government,"* (CNN.com: November 8, 2012) (reporting that a "record number of tech products used by the U.S. military and dozens of other Federal agencies are fake. That opens up a myriad of national security risks, from dud missiles to short-circuiting airplane parts to cyberespionage"), accessed from http://money.cnn.com/2012/11/08/technology/security/counterfeit-tech/index.html.

[128] *See, e.g.*, United States Government Accountability Office, *"GAO-16-236: Counterfeit Parts—DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk,"* (February 2016) at p. 1, accessed from http://www.gao.gov/assets/680/675227.pdf.

[129] United States Government Accountability Office, *"GAO-16-236: Counterfeit Parts—DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk,"* (February 2016) at p. 1, accessed from http://www.gao.gov/assets/680/675227.pdf.

[130] United States Government Accountability Office, *"GAO-16-236: Counterfeit Parts—DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk,"* (February 2016) at p. 10, accessed from http://www.gao.gov/assets/680/675227.pdf.

[131] *See, e.g.*, United States Department of Homeland Security, *"Critical Infrastructure Sectors,"* accessed from https://www.dhs.gov/critical-infrastructure-sectors.

[132] *See* The White House, "*Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*," (July 2011), accessed from https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

[133] *See* INTERPOL, "*Trafficking in Illicit Goods and Counterfeiting,*" accessed from http://www.interpol.int/Crime-areas/Trafficking-in-illicit-goods-and-counterfeiting/Trafficking-in-illicit-goods-and-counterfeiting.

[134] Statement of The Honorable Ronald K. Noble, Secretary General, INTERPOL, Before The Committee on International Relations, House of Representatives, "*The Links Between Intellectual Property Crime And Terrorist Financing,*" (July 16, 2003) at pp.29-30, accessed from http://commdocs.house.gov/committees/intlrel/hfa88392.000/hfa88392_0f.htm. The National Intellectual Property Rights Coordination Center has also noted that: "Terrorist supporters have used intellectual property crime as one method to raise funds. Central to this judgment is the distinction between terrorist supporters who merely provide funding and resources to a terrorist organization versus terrorist organization members who engage in the actual terrorist activities of violence." (National Intellectual Property Rights Coordination Center, "*Intellectual Property Rights Violations: A Report on Threats to United State Interests at Home and Abroad,*" (November 2011) at p.40, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/.

[135] *See, e.g.*, The White House, *"Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security"* (2011) at pp.3, 14, accessed from https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

[136] The White House, "*Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*" (2011) at p.7, accessed from https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

[137] *See, e.g.*, United Nations Office of Drugs and Crime, *"The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime,"* accessed from https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf; United Nations Interregional Crime and Justice Research Institute (UNICRI), *"Counterfeit Medicines and Organized Crime"* (2012) at p.90, accessed from http://www.unicri.it/topics/counterfeiting/medicines/report/Ctf_medicines_and_oc_advance_unedited2013.pdf; United Nations Interregional Crime and Justice Research Institute (UNICRI), "*Counterfeiting: a global spread, a global threat"* (2007), at pp.103-120, accessed from http://www.unicri.it/news/article/0712-3_counterfeiting_crt_foundation; United States Department of Justice, *"Overview of The Law Enforcement Strategy to Combat International Organized Crime,"* (April 2008), pp. 4-5, 9 (discussing an Asian criminal organization that was smuggling counterfeit cigarettes and pharmaceuticals; a raid against the Italian organized crime group, the Camorra, in connection with the sale of counterfeit goods; and the 'Ndrangheta crime syndicate's involvement with counterfeit trade), accessed from https://www.justice.gov/sites/default/files/criminal-icitap/legacy/2015/04/23/04-23-08combat-intl-crime-overview.pdf. *See also* United States Department of Justice, U.S. Attorney's Office for the Eastern District of New York, "*Three Members Of International Organization Of Money Launderers For The Largest Drug Cartels Arrested*" (September 10, 2015) (noting that "international organization of money launderers and drug trafficking organizations conspired to carryout trade-based money laundering activities … on behalf of drug trafficking organizations in Mexico and Colombia to fund purchases of counterfeit goods in China, which were then shipped to Colombia and elsewhere for resale.") (Note: *The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty),* accessed from https://www.justice.gov/usao-edny/pr/three-members-international-organization-money-launderers-largest-drug-cartels-arrested; National Intellectual Property Rights Coordination Center, "*Intellectual Property Rights Violations: A Report on Threats to United State Interests at Home and Abroad,*" (November 2011) at pp.39-40, accessed from https://www.iprcenter.gov/reports/ipr-center-reports/IPR%20Center%20Threat%20Report%20and%20Survey.pdf/; Booth, William, *"Drug Cartels Muscle In To Piracy Business"* (The Washington Post: May 29, 2011) (reporting that the Mexican Attorney General found that one large Mexican drug cartel may "generate as much as $2 million a day through video piracy"), accessed from https://www.washingtonpost.com/world/americas/drug-cartels-muscle-in-to-piracy-business/2011/05/28/AG93GLEH_story.html.

[138] United States Department of State, Bureau of Diplomatic Security, *"Mexico 2014 Crime and Safety Report: Mexico City,"* accessed from https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=15151.

[139] *See, e.g.*, Statement of The Honorable Ronald K. Noble, Secretary General, INTERPOL, Before The Committee on International Relations, House of Representatives, "*The Links Between Intellectual Property Crime And Terrorist Financing*," Hearing (July 16, 2003) at pp.31-35, accessed from http://commdocs.house.gov/committees/intlrel/hfa88392.000/hfa88392_0f.htm; *see also*, INTERPOL, *"INTERPOL Warns of Link Between Counterfeiting and Terrorism,"* (July 16, 2003), accessed from http://www.interpol.int/News-and-media/News/2003/PR019; INTERPOL, "*Growing evidence of links between counterfeit goods and terrorist financing,*" (April 6, 2004) (reporting seizure of several containers filled with counterfeit brake pads and shock absorbers destined for supporters of Hezbollah), accessed from http://www.interpol.int/en/News-and-media/News/2004/PR012/; United States Department of Justice, United States Attorney's Office, Eastern District of Michigan, "*Press Release: Nineteen Charged With Racketeering to Support Terrorist Organization*" (March 29, 2006) (a Joint Terrorist Task Force indicted a 19 person multi-national criminal syndicate, alleging that group was selling counterfeit medicines and other products to raise money for Lebanese terrorist organization Hezbollah) (Note: *The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty*), accessed from http://www.prnewswire.com/news-releases/nineteen-charged-with-racketeering-to-support-terrorist-organization-70737752.html; INTERPOL, "*INTERPOL Targets Organized Crime With Global Initiative Against Trafficking In Illicit Goods,"* (June 22, 2012) (INTERPOL President Khoo Boon Hui noting "clear links between transnational organized crime trafficking in illicit goods and the manufacture and distribution of counterfeit goods, combined with growing evidence of terrorism also being financed through illicit trade"), accessed from http://www.interpol.int/en/News-and-media/News/2012/PR050; Associated Press, *"Counterfeit Goods Linked to Al Qaeda"* (Los Angeles Times: July 17, 2003) ("From knockoffs of designer Kate Spade handbags to pirated DVDs, Al Qaeda and other terrorist groups increasingly are turning to counterfeit goods to fund their operations, lawmakers were told Wednesday"), accessed from http://articles.latimes.com/2003/jul/17/nation/na-counterfeit17; Cusack, Jim,*"Al-Qaeda rocket sparks fresh IRA smuggling feud"* (The Independent: December, 22, 2013) (reporting the "seizure of €4.3m worth of illegal cigarettes after an Al-Qaeda rocket blew the lid off an IRA smuggling racket"), accessed from http://www.independent.ie/irish-news/alqaeda-rocket-sparks-fresh-ira-smuggling-feud-29859081.html; *see also* Spencer, Richard, *"Suez Canal targeted as war in Sinai spreads"* (The Telegraph: November 17, 2013) ("The anonymous briefing however, the first by a senior official, gave a fuller picture. One of the two missiles did indeed bounce off a strut holding the containers… exposing, it turned out, a large load of counterfeit cigarettes, subsequently tracked and seized when they were unloaded in Ireland"), accessed from http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/10454020/Suez-Canal-targeted-as-war-in-Sinai-spreads.html.

[140] *See, e.g.*, The Union des Fabricants (UNIFAB), *"Counterfeiting and Terrorism – Edition 2016,"* at pp.12-18, accessed from http://www.unifab.com/wp-content/uploads/2016/06/Rapport-A-Terrorisme-2015_GB_22.pdf; Statement of John S. Pistole, Assistant Director, Counterterrorism Division, United States Federal Bureau of Investigation, Before the House Committee on Financial Service Subcommittee on Oversight and Investigations, (September 24, 2003) ("The FBI is also investigating smaller Hamas financing efforts being conducted by criminal enterprises in the U.S., which have shown either associations with known Hamas members or sympathies toward its ideology. These investigations have uncovered a myriad of criminal activities used to generate funds, a portion of which is then forwarded to NGOs associated with Hamas…[which] include, but are not limited to, drug trafficking, credit card fraud, [and sale of] counterfeit products"), accessed from https://archives.fbi.gov/archives/news/testimony/the-terrorist-financing-operations-section; United States Department of State, Office of the Coordinator For Counterterrorism, *"Patterns of Global Terrorism,"* (April 30, 2003) (reporting that during the arrest of "suspected Sunni extremist Ali Nizar Dahroug, nephew of former Triborder shopkeeper and suspected al-Qaida associate Muhammad Dahroug," that "[p]olice seized counterfeit goods and receipts documenting wire transfers of large sums of money to persons in the United States and the Middle East"), accessed from http://www.state.gov/j/ct/rls/crt/2002/html/19987.htm; United States Federal Bureau of Investigation, Philadelphia Division, "*Alleged Supporter of Terrorist Group Extradited from Paraguay*" (February 25, 2011) (defendant charged in a conspiracy to provide material support to Hizballah, associated with "counterfeit goods—namely, counterfeit Nike® shoes and Mitchell & Ness® sports jerseys") (Note: *The charges contained in the Indictment are merely accusations and the defendant is presumed innocent unless and until proven guilty*), accessed from https://archives.fbi.gov/archives/philadelphia/press-releases/2011/ph022511a.html; United States Bureau of Alcohol, Tobacco, Firearms and Explosives, "*Congressional Budget Submission – Fiscal Year 2012*," (2012) ("Organized criminal groups, including those with ties to terrorist organizations, have increasingly engaged in the illegal trafficking in tobacco products, particularly counterfeit and lawfully manufactured cigarettes"), accessed from: https://www.atf.gov/file/10741/download; Levitt, Matthew, *"Hamas: Politics, Charity, and Terrorism in the Service of Jihad"* (Yale Univ. Press: 2006); Doward, Jamie, *"How cigarette smuggling fuels Africa's Islamist violence"* (The Guardian: January 26, 2013) (reporting that counterfeit and illicit cigarettes have become an increasingly important source of financing for the groups, second only to the heroin trade, according to Pakistani intelligence officials), accessed from https://www.theguardian.com/world/2013/jan/27/cigarette-smuggling-mokhtar-belmokhtar-terrorism; Wilson, Kate, International Consortium of Investigative Journalists, *"Terrorism and Tobacco"* (June 29, 2009) (reporting that the smuggling of cigarettes—either untaxed or counterfeit—has proved a particularly lucrative, low-risk way to fund operations on behalf of entities such as Hezbollah, the Taliban, Al-Qaeda, the Real IRA, the Kurdistan Workers' Party (PKK), the FARC, and the Tutsi-backed rebel group called The Congress National Pour la Defense du Peuple (CNDP)), accessed from https://www.icij.org/project/tobacco-underground/terrorism-and-tobacco.

While the distribution of counterfeit cigarettes by transnational organized criminal networks or terrorist-affiliated entities is sufficient reason to worry, the illicit activity also raises grave health concerns. It has been reported, for example, that counterfeit cigarettes have tested positive for containing significantly higher levels of the heavy metal cadmium, as well as elevated levels of lead and other chemicals, than the genuine product. *See, e.g.*, He Y, *et. al.*, *"Investigation of Lead and Cadmium in Counterfeit Cigarettes Seized in the United States,"* (Food Chem Toxicol.: July 2015), accessible from http://www.ncbi.nlm.nih.gov/pubmed/25862957. The toxin cadmium—often used in batteries and metal plating—can lead to cancer, kidney failure and lung damage.

[141] It has also been reported that a group selling counterfeit t-shirts and other goods, generating millions of dollars in illicit profits, was run by followers of Sheik Omar Abdel Rahman, the blind cleric who was convicted for his role in the 1993 World Trade Center bombing and sentenced to 240 years in prison;

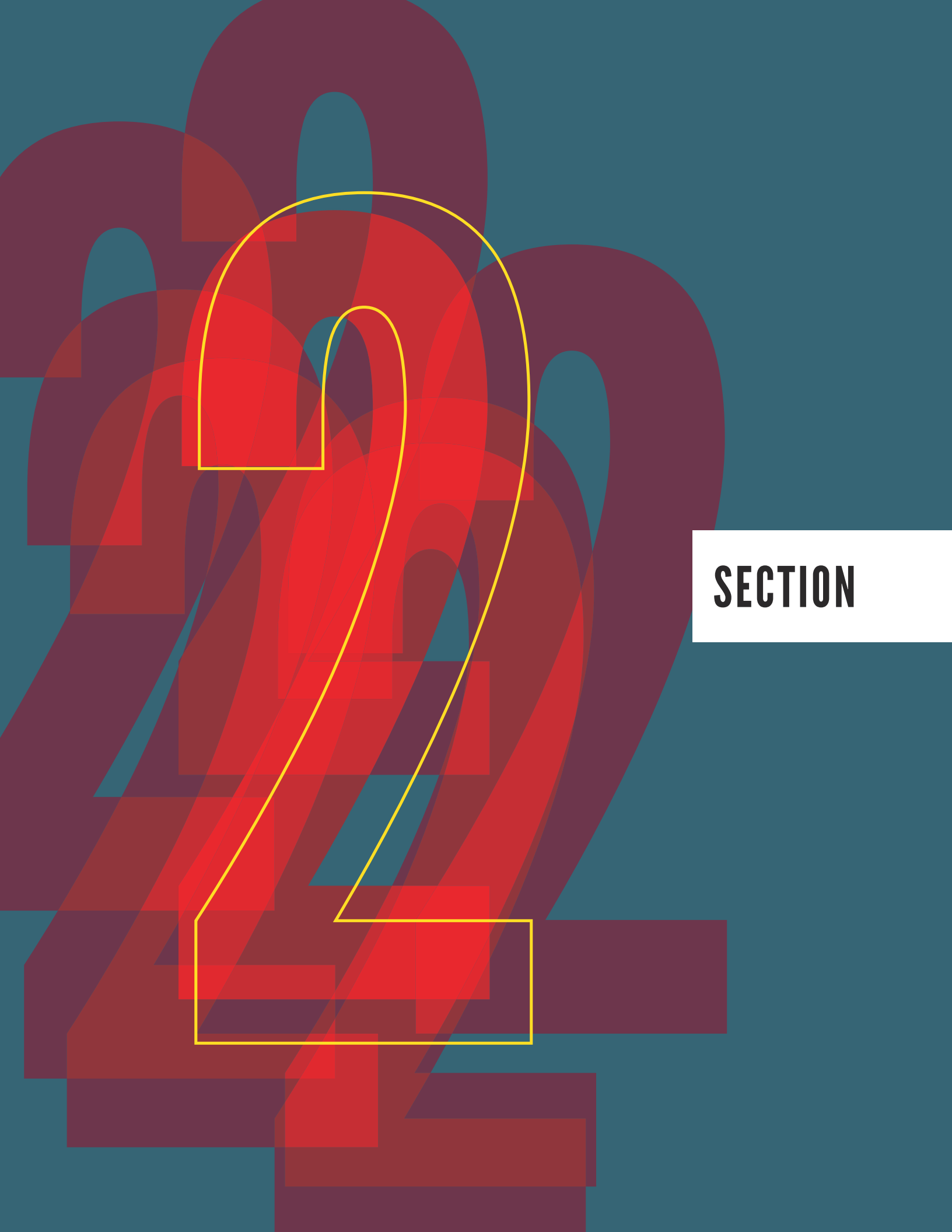
that the perpetrators of the 2004 Madrid train bombings, which killed 191 people, raised illicit proceeds from the sale of pirated CDs and DVDs; and more recently, that those behind the Paris (Charlie Hebdo) terrorist attacks in January 2015, which killed 17 people, raised illicit proceeds from the sale of counterfeit footwear and apparel. *See, e.g.*, John Mintz and Douglas Farah, *"Small Scams Probed for Terror Ties,"* (The Washington Post: Aug. 12, 2002), accessed from https://www.washingtonpost.com/archive/politics/2002/08/12/small-scams-probed-for-terror-ties/acfb904e-002e-49c2-a531-8c7c2e46573b/; Kaplan, Eben, *"Tracking Down Terrorist Financing,"* (April 4, 2006), accessed from http://www.cfr.org/terrorist-financing/tracking-down-terrorist-financing/p10356; International Herald Tribune, *"Counterfeit goods are linked to terror groups,"* (February 12, 2007), accessed from http://www.nytimes.com/2007/02/12/business/worldbusiness/12iht-fake.4569452.html; Yan, Holly, *"Suspected ringleader of Belgian terror cell sought,"* (CNN.com: January 19, 2015) ("Sales of counterfeit goods by Charlie Hebdo attacker Cherif Kouachi helped fund the purchase of weapons, a source familiar with the ongoing investigation in France told CNN"), accessed from http://www.cnn.com/2015/01/19/europe/europe-terror-threat/; Union des Fabricants (UNIFAB), *"Counterfeiting and Terrorism – Edition 2016,"* at p.14, accessed from http://www.unifab.com/wp-content/uploads/2016/06/Rapport-A-Terrorisme-2015_GB_22.pdf.

[142] *See, e.g.*, Jay Solomon and Gordon Fairclough, *"North Korea's Counterfeit Goods Targeted"* (The Wall Street Journal: June 1, 2005) (reporting that since Sept. 11, 2001, North Korea's sales of counterfeit products, namely counterfeit cigarettes and pharmaceuticals, have grown exponentially from $100 million to $500 million annually), accessed from http://www.wsj.com/articles/SB111756528456047297; Ryall, Julian, *"North Korea branches out into ivory, fake cigarette and pharmaceutical trade"* (The Telegraph: April 12, 2014), accessed from http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10766587/North-Korea-branches-out-into-ivory-fake-cigarette-and-pharmaceutical-trade.html; Yi Whan-woo, *"N. Korea Selling Counterfeit Money To Terrorists"* (The Korean Times: June 27, 2016) (reporting that the "cash-strapped regime may try to expand trafficking networks in drugs, weapons, cigarettes, and counterfeit luxury goods as alternative means to generate hard currency following a series of sanctions against it."), accessed from http://www.koreatimes.co.kr/www/news/nation/2016/06/485_207990.html; The White House, Office of the Press Secretary, *"Statement by the Press Secretary on the Executive Order Entitled 'Imposing Additional Sanctions with Respect to North Korea',"* (January 2, 2015) (naming the Government of North Korea as the actor of the "destructive and coercive cyberattack on Sony Pictures Entertainment"), accessed from https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s.

[143] *See* Statement of Gordon M. Snow, Assistant Director, United States Federal Bureau of Investigation Cyber Division, Before the Senate Judiciary Committee (June 21, 2011), accessed from https://www.fbi.gov/news/testimony/intellectual-property-law-enforcement-efforts.

[144] *See* The White House, "*Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security,*" (July 2011), accessed from https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

THIS PAGE IS INTENTIONALLY LEFT BLANK


SECTION

2

HELPING TO PROMOTE A SAFE AND SECURE INTERNET: MINIMIZE COUNTERFEITING AND IP-INFRINGING ACTIVITY ONLINE



SECTION 2 CONTENTS

HELPING TO PROMOTE A SAFE AND SECURE INTERNET: MINIMIZE COUNTERFEITING AND INTELLECTUAL PROPERTY-INFRINGING ACTIVITY ONLINE

A. Targeting Financial Support Flowing to Criminals: A "Follow-the-Money" Approach to Combating Online Commercial Piracy and Counterfeiting 61

1. Strengthen Payment Processor Networks' Efforts to Curb Illicit Proceeds 62
2. Strengthen Online Advertising Networks' Efforts to Curb Flow of Illicit Revenue 63
3. Strengthen Foreign Banking Practices to Curb the Financing of Illicit Trade 66

B. In Furtherance of a Healthy Domain Name System 68

1. Assessing the Enforcement Challenge of Domain Name Hopping 68

C. Reducing Online Piracy and Counterfeiting by Increasing the Ability of Consumers to Locate Content and Products Through Lawful Means 69

1. Support Consumers' Identification of Websites Offering Legal Goods or Services 69
2. Support Practices and Policies to Improve DMCA Notice-and-Takedown Processes 70
3. Support Practices and Policies Within Social Media Channels to Curb Intellectual Property Based Illicit Activity 71
4. Support Practices and Polices to Reduce Intellectual Property Infringement Facilitated by Mobile Apps 73
5. Putting the Consumer First: Combatting Operators of Notorious Websites by Way of Consumer Education 74
6. Encourage Efforts that Support Content Platforms Offering Content Legally and Minimize Deceptive Sites That Operate with a Commercial "Look and Feel" 76
7. Opportunities to Curb Sales of Counterfeit and Pirated Goods on E-Commerce Platforms 77

D. Support Responsible 3D Printing Communities and Business Models 79

E. Address Cyber-Enabled Trade Secret Theft 80



INTRODUCTION

From the operation of stand-alone websites dedicated to illicit IPR-based activity, to the exploitation of legitimate platforms and services by illicit actors, opportunities exist to support and develop enhanced mechanisms to curb counterfeiting and infringing activity online. This includes an examination of a "follow-the-money" approach to disrupt illicit financing models (via payment processors, ad networks and the like), to practices and policies aimed at curbing abusive practices within e-commerce platforms, social media channels, the domain name ecosystem, and the search environment, among others.

A. TARGETING FINANCIAL SUPPORT FLOWING TO CRIMINALS: A 'FOLLOW-THE-MONEY' APPROACH TO COMBATING ONLINE COMMERCIAL PIRACY AND COUNTERFEITING.

The online infringement of IPR is a lucrative activity. Commercial-scale counterfeiters and pirates enjoy the fruits of another's labor, profiting from famous brands, hit songs, television shows, movies and the like without having to make major investments and absorb the risks facing legitimate businesses and entrepreneurs.

On the content side, it is time consuming and expensive for authors and legitimate entities to create and produce original content ("first copy"), but it costs next to nothing to make an unauthorized copy. As a result, the digital commercial pirate can enjoy staggering unearned and unlawful profits, reportedly ranging from 80 percent to close to 100 percent, in connection with digital piracy and the sale of pirated digital video discs (DVDs) and compact discs (CDs).[1]

Turning to brands, counterfeit medicines, for example, require no research and development and are manufactured under minimal cost, and thus enjoy profit margins reportedly as high as 3,000 percent; a $1,000 investment in counterfeit prescription drugs may result in a $30,000 return, which is 10 times the reported profit rate of trafficking heroin.[2] Similarly, a 40-foot container of counterfeit cigarettes may cost as little as $70,000 to produce, but carry a street value of approximately $3,000,000 – $4,000,000, a profit margin of more than 5,000 percent.[3]

An effective enforcement strategy against commercial-scale piracy and counterfeiting therefore, must target and dry up the illicit revenue flow of the actors engaged in commercial piracy online.[4] That requires an examination of the revenue sources for commercial-scale pirates. The operators of direct illict download and streaming sites enjoy revenue through membership subscriptions serviced by way of credit card and similar payment-based transactions, as is the case with the sale and purchase of counterfeit goods, while the operators of torrent sites may rely more heavily on advertising revenue as the primary source of income. As a result, an effective "follow-the-money" approach must include, at a minimum, the continued voluntary engagement of third parties, including payment processor networks, the online advertising ecosystem, and the banking sector to minimize the flow of money to website operators engaged in illicit activity.

1. Strengthen Payment Processor Networks' Efforts to Curb Illicit Proceeds.

Illicit actors that engage in the commercial sale of counterfeit goods, or provide online subscription services for mass piracy websites, depend on payment services provided by credit card companies and money transfer entities (collectively, "payment processors"). With the continued growth of global e-commerce and streaming services, illicit actors may be able to reap billions of dollars in illicit proceeds every year from transactions made through payment processors.[5]

All legitimate payment processors prohibit the use of their services and platforms for unlawful conduct, including IP-infringing activities. They do so by way of policy and contract through terms of use and other agreements applicable to their users (herein referred to as "Terms of Service").[6] Yet, notwithstanding these prohibitions, payment processor platforms continue to be exploited by illicit merchants of counterfeit products and infringing content. Examples of the ways in which illicit actors exploit legitimate payment processors include, "(i) opening multiple accounts at the same bank, (ii) opening multiple accounts at different banks, and (iii) aggregation."[7] Furthermore, sophisticated actors have come to understand that investigative transactions (*i.e.* trace messages) are conducted by law enforcement and rights holders to glean merchant-identifying information for targeting purposes, and these actors have in turn implemented detection systems to thwart these "test" transactions conducted for investigatory purposes.[8]

In addition, some credit card companies are "open-loop" payment networks, meaning that they do not have direct contractual relationships with merchants; instead, they rely on a third-party acquiring or issuing bank to take action against a merchant should the bank suspect wrongful activity by the merchant.[9] Since termination of payment processing services happens at the level of the individual consumer or merchant account and without regard to the underlying business (such as the offending website), the website may continue to transact business after some of its payment processing rights have been terminated.

Both legitimate payment processors and IP rights holders have expressed concerns over these increasingly sophisticated exploitative techniques, and they have a shared desire to minimize the rate of illicit financial transactions. Cutting the source of revenue to illicit actors greatly reduces the commercial viability of websites dedicated to counterfeit sales, piracy, and related illegal activity.[10]

Implementing an effective follow-the-money approach requires a number of key members of the online ecosystem—including rights holders, payment processors, merchant banks, and others—to work in concert to stem the money flow to illicit enterprises.[11] Several years ago, with IPEC's leadership and support, a number of leading payment processors adopted a set of best practices to investigate complaints and withdraw payment services from websites dedicated by their operators to distributing counterfeit goods and engaging in commercial piracy.[12] Building on this, third party organizations have launched efforts that have helped grow and implement the payment processors' voluntary best practices.[13] These voluntary and private-sector-driven mechanisms demonstrate a growing recognition among a wide spectrum of actors in the Internet ecosystem that they have an opportunity to secure a legitimate and safe online environment and deter illegal activity online, including counterfeiting and infringement.[14]

Opportunities exist for expanded collaboration between all stakeholders to augment these voluntary initiatives and stay ahead of the rapidly changing tactics illicit actors employ to unlawfully exploit

legitimate payment processing services and engage in counterfeiting and infringement in the rapidly evolving online environment. Expanded collaboration, for example by geographic scope, and enhanced transparency (including sharing with the public generalized, anonymized data on the nature and profile of merchant accounts terminated by payment processors for violating the Terms of Service for counterfeiting and infringement), will improve benchmarking of these voluntary initiatives and enable stakeholders to identify further opportunities to deny criminals financial support.

ACTION NO. 2.1: Support efforts to enhance payment processor voluntary initiatives. IPEC—as well as members of the U.S. Interagency Strategic Planning Committees on IP Enforcement—will consider opportunities to further engage with the voluntary payment processor initiatives currently in place, including with regard to the number of active participants in, and geographic scope of, the initiatives and best practices. Consideration will be given to multistakeholder engagement with the private sector, public interest organizations, academia, and bi-lateral engagements with other governments to understand the expansion of these voluntary initiatives' application in other countries, and other tools to support and expand these voluntary agreements designed to cut-off worldwide funding to illicit merchants.

ACTION NO. 2.2: Encourage enhanced transparency in the operation and effectiveness of the private-sector-led voluntary initiatives to combat revenue flow to online commercial pirates and commercial-scale traders of counterfeit goods. Payment processors are encouraged to make appropriately generalized and anonymized data publicly available as part of their best practices and initiatives to permit study and analysis of illicit activity intercepted on their networks. Such data will allow study by public and private actors alike to identify patterns of behavior or tactics associated with illicit merchants. IPEC, along with members of the U.S. Interagency Strategic Planning Committees on IP Enforcement, will identify means to enhance data-driven research opportunities in the area of illicit online financing trends, tactics, and characteristics.

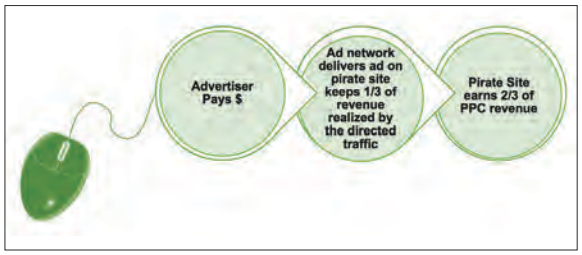
ACTION NO. 2.3: Encourage benchmarking studies to gauge and strengthen voluntary best practice initiatives. IPEC and USPTO, with private sector input, will facilitate benchmarking studies of current voluntary initiatives designed to combat revenue flow to rogue sites to determine whether existing voluntary initiatives are functioning effectively, and thereby promote a robust, data-driven voluntary initiative environment.

2. Strengthen Online Advertising Networks' Efforts to Curb Flow of Illicit Revenue.

The unlawful exploitation of copyrighted material is substantially financed by advertising dollars. As one report stated: "Ad revenue is the oxygen that allows content theft to breathe."[15] Ad-supported piracy is extensive. According to one report, online advertising supports up to 86 percent of IP infringing websites that allow web users to download or stream infringing content for free to the end-user.[16]

Whereas the rogue website operator pays nothing for a downloaded or streamed movie or song, for example, the ads that appear beside the misappropriated content generate revenue for the website operator—generally in the form of pure profit. The artist, label, and studio do not see a penny. The ad network that delivered ads to the website dedicated to offering infringing content also generates revenue (FIG. 33), while again, the artist, label and studio receive no compensation for their work. Everyone profits, except the creator and/or authorized distributor of the original content.

FIG. 33: Example of "Pay Per Click" (PPC) Ad Flow in a Piracy Model.



As digital advertising is dependent in part on the number of users who are exposed to the website ads, websites promoting counterfeit or unauthorized content can receive substantial digital advertising revenue when placed on pages featuring popular content, such as music, films, television shows, games, software, and eBooks. According to one recent study, operators of websites dedicated to unlawfully exploiting third-party content may have made nearly $250 million, with "the 30 largest sites that profit exclusively from advertising dollars by pushing stolen movies, music, and television programs" generating an average of more than $4 million dollars a year in illicit proceeds.[17]

Excerpt of Testimony Before the House Committee on the Judiciary

"As a global leader in online advertising, Google is committed to rooting out and ejecting rogue sites from our advertising services. Google continues its efforts, both proactive and reactive, to detect and act against advertisers and web publishers who violate our policies against copyright infringement. Since 2012, we have ejected more than 73,000 sites from our AdSense program, the vast majority of those caught by our own proactive screens."

Testimony of Google's Senior Copyright Policy Counsel before the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet Hearing (March 13, 2014).

As with payment processor models discussed above, all legitimate ad networks similarly prohibit—by way of contractual "terms of use" or "terms of service"—the use of their services and platforms for unlawful conduct, including IP-infringing activities.[18] Reporting suggests that the enforcement of these terms of service (*see sidebar*) has helped root out a large volume of advertisers and web publishers who engaged in copyright infringement. Notwithstanding these contractual prohibitions, and efforts to implement industry best practices including the use of proactive screening, ad network platforms continue to be exploited by sophisticated entities engaged in widespread infringement of third-party content.

Moreover, concerns about ad-supported websites dedicated to counterfeit or infringing activity go beyond the revenue loss to the content creator. Those entities engaged in the operation of such websites reportedly display malware-based ads in significant numbers that pose risks to consumers and generate income by defrauding legitimate advertisers and other businesses. According to recent reports, high-risk ads comprised of malware and fraudulent ad-revenue generation techniques (such as click generator fraud, pop-under ads, pixel stuffing, etc.) represent from 51 to 60 percent of all ads displayed on websites dedicated to offering counterfeit products and infringing content.[19]

American advertising industry groups have in recent years launched several initiatives that seek to protect the integrity of the digital advertising system and of third-party content and brands from criminal exploitation by working to keep the flow of legitimate advertising dollars to the operators of legitimate websites and away from those engaged in illicit activity, including content infringement and counterfeiting.[20] Building on pledges from the advertising community, a new voluntary initiative has been launched to further dry up advertising revenue generated by traffic to websites offering infringing content.[21] Through this and other industry-led initiatives, many of the world's largest brand advertisers and agencies have committed to take aggressive steps to keep their digital ads off these sites.[22] There remains significant work ahead, since legitimate companies continue to find their advertisements (and thus their ad dollars) inadvertently placed on sites dedicated to widespread, commercial-scale IP infringement (FIG. 34). According to one report, nearly 30 percent of sampled websites in a survey of ad-supported pirate websites carried ads for "blue-chip" premium brands with recognizable household names.[23]

Opportunities exist to support and expand collaboration between all stakeholders to augment these voluntary initiatives and stay ahead of the rapidly changing tactics rogue actors employ. Expanded collaboration, including by geographic scope, and enhanced sharing with the public of generalized, anonymized data on terminated accounts (such as, for example, by age of account, revenue flow to the site, geographic location of the site),

FIG. 34: Example of Legitimate Advertisements Appearing on "Notorious Market" (Kat.cr).[24]



can improve benchmarking of these initiatives and enable stakeholders to study and identify further opportunities to deny financial support to rogue websites.

ACTION NO. 2.4: Encourage efforts to minimize ad revenue support of websites dedicated to counterfeiting and infringement. IPEC and the IPR Center (with its constituent law enforcement partners), along with other relevant Federal agencies, will convene the advertising industry to hear further about their voluntary efforts. The U.S. Interagency Strategic Planning Committees on IP Enforcement will assess opportunities to support efforts to combat the flow of ad revenue to criminals.

ACTION NO. 2.5: Call for enhanced transparency. As part of best practices and initiatives, advertising networks are encouraged to make appropriately generalized and anonymized data publicly available to permit study and analysis of illicit activity intercepted on their platforms and networks. Such data will allow study by public and private actors alike to identify patterns of behavior or tactics associated with illicit actors who seek to profit from ad revenue from content theft websites. IPEC, along with members of the U.S. Interagency Strategic Planning Committees on IP Enforcement, will identify means to enhance data-driven research opportunities in the area of illicit online ad-based financing trends, tactics, and characteristics.

ACTION NO. 2.6: Encourage benchmarking studies to gauge and strengthen voluntary best practice initiatives. IPEC and USPTO, with private sector input, will facilitate benchmarking studies of current voluntary initiatives designed to combat revenue flow to rogue sites to determine whether existing voluntary initiatives are functioning effectively, and thereby promote a robust, data-driven voluntary initiative environment.

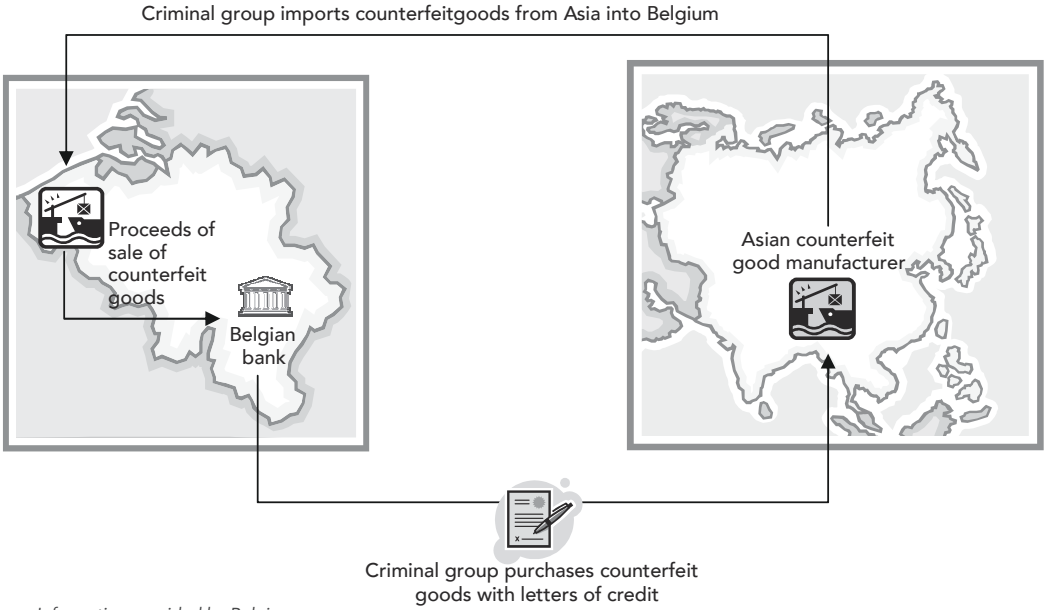
3. Strengthen Foreign Banking Practices to Curb the Financing of Illicit Trade.

The most effective "follow the money" approach to combat illicit proceeds from online commercial piracy and counterfeiting hinges on participation from all key stakeholders found along the money trail, including in particular, voluntary participation from banks and third-party financial technology processors.

Two primary money-laundering methods through which illicit actors capture and move illicit proceeds for purposes of disguising their origins are: (1) manipulation of the financial system, and (2) the physical movement of illicit goods in commerce.[26] Rogue actors abuse banking and financial technology services to receive, transfer, or withdraw illicit deposits made around the world, as well as to process credit card and other payments through the use of one or more merchant or acquiring banks.[27] With respect to the physical movement of illicit goods in commerce, trade based money laundering schemes are used to disguise the proceeds through transactions and tactics that include over-and-under-invoicing of goods or the false description of goods, such as counterfeit goods (FIG. 35).[28]

FIG. 35: Example of Trade-Based Money Laundering Scheme.[25]

- A criminal group imports counterfeit goods from Asia into Belgium using a letter of credit and sells them for cash.
- The group deposits the money into a Belgian bank account and arranges a subsequent letter of credit.
- The group purchases additional counterfeit goods from Asia using the new letter of credit.
- These additional counterfeit goods are sold and the receipts deposited in the bank and used to arrange additional letters of credit.



Source: Information provided by Belgium.

Commentary – In this case, the criminal group was able to use the cash deposited in the bank to arrange letters of credit. Subsequently, it was able to make use of these letters of credit to purchase a series of shipments of counterfeit goods. The criminal group thought that the use of letters of credit related to trade transactions, rather than wire transfers, would increase the appearance of legitimacy of these transactions and reduce their risk of detection.

Source: Financial Action Task Force (Groupe d'action financiere)

Several sources suggest that a small handful of non-U.S. banks may be disproportionately used as safe havens for proceeds stemming from illicit activities, including international trade in counterfeit goods.[29] In particular, it has been reported that more than 90 percent of accounts used to process online credit card payments for hundreds of thousands of websites dedicated to the sale of counterfeit goods are concentrated in three banks based in China: the Bank of China, the Bank of Communications, and Agricultural Bank of China.[30] The results of an academic investigation published in 2016 by the MIT Technology Review similarly revealed that these same banks in China processed the majority of seized fake goods purchased during an 18-month period—that is, 291 of 300 transactions.[31]

The U.S. Department of State reports that the "development of China's financial sector has required increased enforcement efforts to keep pace with the sophistication and reach of criminal networks," and the "primary sources of criminal proceeds" involve "intellectual property theft" and the sale of "counterfeit goods."[32] While further study is needed, there are significant indications suggesting that both Chinese and non-Chinese actors are exploiting the Chinese banking system to launder money made through counterfeit trade (FIG. 36).

The scope of abuse of the banking and international trading systems must be better understood. Where further substantiated, actions to combat these apparent abuses must be a central part of the Nation's IP enforcement strategy. Safeguarding the financial system from illicit use is critical to safeguarding the rule of law and global economic well-being. It is also critical to promoting a safe online environment that supports effective IP enforcement. Opportunities exist to curb the exploitation of banking networks and illicit IPR-based activity alike, by working through established mechanisms dedicated to safeguarding the financial system from illicit use, including through existing bi-lateral and multi-lateral engagement.

ACTION NO. 2.7: Increase awareness and understanding of syndicates' exploitation of the global financial system to harbor and launder proceeds of commercial-scale ip theft. The IPEC will designate a working group comprised of relevant members of the U.S. Interagency Strategic Planning Committees on IP Enforcement to explore opportunities to initiate a study on the scope of the problem of transnational money laundering involving counterfeit goods. Additionally, the Departments of the Treasury, Homeland Security, State, and Justice, and other relevant Federal agencies will consider ways to ensure that anti-money laundering efforts and strategies take into account IP-based illicit activity.

FIG. 36: Global Networks: Unsealed Indictment Alleging Link Between Chinese Banks, Transnational Organized Crime, Money Laundering & Counterfeit Trade.[33]

Department of Justice | Unsealed Indictment | E.D.N.Y. Docket No. 15-Cr-81

According to an unsealed indictment by the U.S. Department of Justice in September 2015, three Colombian nationals based in Guangzhou, China, are alleged to have carried-out more than $5 billion in trade-based money laundering activities in China on behalf of drug cartels based in **Mexico** and **Colombia**. The defendants are alleged to have laundered money through bank accounts in **Hong Kong** and **mainland China** to fund the purchase counterfeit goods in China, which were then sold around the world.



ACTION NO. 2.8: Integrate awareness of IP crime and its illicit proceeds into broader efforts to combat money laundering and the financing of transnational organized crime networks. IPEC, in coordination with relevant members of the U.S. Interagency Strategy Planning Committees on IP Enforcement, will engage international partners to examine opportunities to integrate awareness of IP crime into broader efforts to combat money laundering and financing of criminal networks.

B. IN FUTHERANCE OF A HEALTHY DOMAIN NAME SYSTEM.

1. Assessing the Enforcement Challenge of Domain Name Hopping.

For purposes of this section, the Administration has directed its focus to detailing some of the reported tactics used by criminal actors in the online environment and the corresponding enforcement challenges. In observance of the established global multistakeholder approaches used to address domain name issues and the National Telecommunications and Information Administration's (NTIA) role as the convener of the U.S. government's DNS interagency working group which establishes U.S. policy positions on domain name issues broadly and with respect to the Internet Corporation for Assigned Names and Numbers (ICANN), including the Governmental Advisory Committee (GAC) and its working groups, the U.S. Interagency Strategic Planning Committees on IP Enforcement reaffirms the principle that the "U.S. Government remains dedicated to working within the multistakeholder construct at ICANN and all relevant venues to vigorously defend and advance U.S. interests."[34]

It has been reported that entities engaged in online counterfeit sales, the unlawful exploitation of copyrighted materials, and other large-scale infringing activity may engage in a combination of "domain name hopping" and "venue shopping" for perceived domain name safe havens.[35] These tactics have been reported within both the gTLD and ccTLD domain name environments.

Top Level Domains (TLDs) are those strings of characters that follow the last 'dot' in a domain name – for example ".gov" in www.whitehouse.gov. TLDs are typically divided into two categories: generic Top Level Domains (gTLDs) and country code Top-Level Domains (ccTLDs). gTLDs are those TLDs of three or more characters, the operators of which typically have contractual agreements with ICANN. ccTLDs are those TLDs representing two-letter abbreviations for countries and territories, such as .us for the United States or .io for the British Indian Ocean Territory, delegated under policies developed by the Internet Engineering Task Force's Request For Comment (RFC) 1591.[36] The relationship between any given ccTLD administrator and its government will differ from case to case and may depend on complex and sensitive arrangements particular to the local political climate. Different ccTLD policies will reflect different approaches with respect to process for the suspension, transfer, or cancellation of a domain name registration. Some ccTLDs use the same dispute resolution mechanism as gTLDs do – the Uniform Domain Name Dispute Resolution Policy – while others tailor their own variations of this policy.

While the TLD environment provides Internet users with a diversity of choice, operators of websites engaged in illicit IP-based activities exploit this openness. To evade law enforcement, bad actors will register the same or different domain name with different registrars. They then attempt to evade law enforcement by moving from one registrar to another, thus prolonging the so-called "whack-a-mole" pursuit. The result of this behavior is to drive up costs of time and resources spent on protecting intellectual property rights.[37]

By way of illustration (FIG. 37), an operator of a large file-sharing site found guilty of facilitating criminal peer-to-peer file sharing of movies, music and games continued to circumnavigate the globe and exploit the domain name environment by moving from ccTLD to ccTLD to evade law enforcement.

In the "Notorious Markets" Out-of-Cycle Review, the Office of the U.S. Trade Representative lists illustrative markets facilitating counterfeiting and piracy. In the lists from 2013-2015, a total of 26 of 54 named sites, or almost half of named online sites, operate within the ccTLD environment.[38] Based on the most recent Notorious Markets lists available prior to issuance of this plan, ccTLDs comprise roughly half of all named "notorious" top-level domains.[39] Considering that ccTLDs are outnumbered by gTLDs in the domain name base by more than a 2-to-1 ratio, the frequency of bad

FIG. 37: Domain Name Hopping: Bad Faith Exploitation of ccTLD Environment.

A Journey Around the World: From Sweden to Grenada, with a Dozen Stops in Between.[41]

1. Sweden (.se)
2. Greenland (.gl)
3. Iceland (.is)
4. Saint-Martin (.sx)
5. Ascension Island (.ac)
6. Peru (.pe)
7. Guyana (.gy)
8. Montserrat (.ms)
9. South Georgia (.gs)
10. Laos (.la)
11. British Virgin Islands (.vg)
12. Armenia (.am)
13. Mongolia (.mn)
14. Grenada (.gd)



faith ccTLD sites appear to be disproportionate in nature and worthy of further research and analysis.[40]

ACTION NO. 2.9: Continue to assess the nature of abusive domain name registration tactics and identify opportunities to minimize criminal activity. As part of a multistakeholder process aimed at crime prevention and the protection of public health, safety, and consumer welfare, the U.S DNS Interagency working group will work with the Interagency Strategic Planning Committees on IP Enforcement, to assess the scope of abusive domain name registration tactics and trends, and consider appropriate opportunities to work with stakeholders to curb criminal activity.

C. REDUCING ONLINE PIRACY AND COUNTERFEITING BY INCREASING THE ABILITY OF CONSUMERS TO LOCATE CONTENT AND PRODUCTS THROUGH LAWFUL MEANS.

Ensuring the existence of, and access to, secure online services and platforms that offer legal content and products is an important part of an effective approach to reducing infringing online activity. Online platforms, however, are subject to a number of challenges and limitations. For example, these providers are subject to abusive tactics themselves when their platforms are used by criminal actors engaged in illicit activity, and are forced to compete with illegitimate providers offering infringing content or platforms through which substandard and counterfeit goods are offered. Efforts to support and enhance the lawful activity in the online ecosystem—from search providers to social media, mobile apps to e-commerce, and others in between—will enable businesses to expand lawful uses of copyrighted content, services, support consumer welfare, and erode rates of counterfeiting and infringing activity online.

1. Support Consumers' Identification of Websites Offering Legal Goods or Services.

A large percentage of Internet transactions begin with a search query. One of the leading search providers, for example, is reported to transact over 100 billion searches per month, which equates to over one trillion searches per year.[42] Search has remained the number one content discovery tool for mobile users.[43] In view of the volume of search engine queries, and the growing number of Digital Millennium Copyright Act (DMCA) take down requests received by search providers each year, search engines have played an increasing role in curbing access to websites used to promote illicit activity.

Search companies have recently reported a number of innovations in this space, including: (i) implementing updates to search algorithms in order to "downrank"

sites that have received a large number of valid DMCA take down notices, and otherwise refining search results to visibly affect the rankings of some of the sites with the most notorious illegal uses; (ii) removing additional terms from autocomplete predictions that would pull-up DMCA demoted sites; and (iii) testing new advertising formats to help point consumers to legitimate sources of content.[44]

These search innovations represent promising actions towards reducing traffic to websites whose operators' or users' primary purpose is the dissemination of infringing music, film, and other creative content.[45] For example, one leading search provider reported in 2015 that its initial search modifications "have been promising, demonstrating that sites that received significant volumes of copyright infringement notices were impacted" in terms of traffic and visibility.[46] Another search entity's improvements to its search functions reportedly cut search-directed traffic to sites used to promote and distribute unlicensed content by as much as 50 percent.[47]

The prioritization of search results to lawful content and products is not a complete solution to combat commercial infringement, especially since sophisticated commercial pirates will continually evolve their tactics, and also because non-search functions are also used to locate and access new sites used to promote illegal content and products. Nevertheless, current public reporting indicates that prioritizing search results to legal content can play a central role in promoting a safe and secure Internet experience.

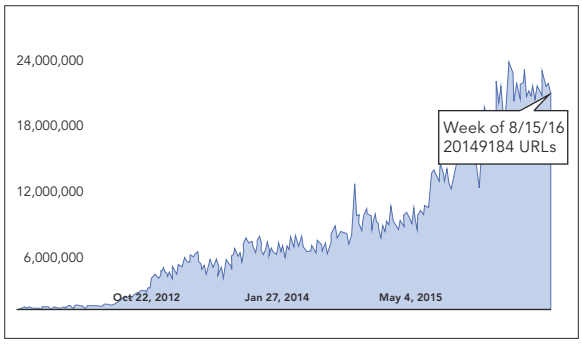
ACTION NO. 2.10: Support development of best practices, through a multistakeholder process, for Internet search providers to address search result rankings of significant commercial-scale piracy and counterfeiting sites. IPEC and the U.S. Interagency Strategic Planning Committees on IP Enforcement have identified the need for research and further development of best practices, through a multistakeholder process, on autocomplete, down-ranking/demotion, and other targeted treatment of websites used to promote illegal content in Internet search as a means of diverting traffic away from infringing content or counterfeit products. Such research and best practices could also address the potential development of adaptive methodologies to anticipate and thwart the operators of these websites' methods of circumventing internationally-recognized IPR norms. Further, best practices should protect principles of free expression and fair use, and avoid mechanisms that are overly-restrictive, attempt to filter legitimate search results, or impose unnecessary burdens on search service providers.

2. Support Practices and Policies to Improve DMCA Notice-and-Takedown Processes.

The DMCA established a notice-and-takedown regime to facilitate the removal of IP-infringing content, while limiting the liability of online service providers, including, *inter alia* when they act as "mere conduits" or host content at the request of third parties.[48] When implemented appropriately, the regime allows internet service providers (ISPs) to benefit from a "safe harbor" that limits their monetary liability. Importantly, ISPs are not required to proactively monitor the use of their services for users' infringing activity.

The digital economy of the 21st century has produced unanticipated types of infringing activity that are testing the limits of the DMCA safe harbor provision, creating technological and legal challenges for IP rights holders and Internet intermediaries alike. While the DMCA provides a mechanism to combat some forms of copyright infringement, rights holders have commented that the takedown system is too resource-intensive and time consuming, especially when it requires constant re-notification of the same content.[49] Moreover, "many individual creators and small and medium-sized enterprises (SMEs) do not have the resources to engage in the ongoing monitoring and notification process required by the DMCA."[50] Meanwhile, ISPs face a significant

FIG. 38: Uniform Resource Locators (URLs) requested to be removed from Search per week (over 20 million URL removal requests the week of August 15, 2016).[52]



administrative burden in having to address a large volume of notices of alleged infringement. For example, one leading search engine reports that it received more than 75 million copyright takedown requests in just one month.[51]

For some platforms, the sheer number of takedown requests received, many of which are automated, have required a shift toward automated review and adjudication, resulting in some notices and takedowns of questionable validity.[53] The misidentification of non-infringing content as infringing risks affecting the integrity of the notice-and-takedown regime for rights holders, Internet intermediaries, and users.

Left unaddressed, these range of problems risk undermining the benefits of the notice and takedown system. The continued development of private sector best practices, led through a multistakeholder process, may ease the burdens involved with the DMCA process for rights holders, Internet intermediaries, and users while decreasing infringing activity. These best practices may focus on enhanced methods for identifying actionable infringement, preventing abuse of the system, establishing efficient takedown procedures, preventing the reappearance of previously removed infringing content, and providing opportunity for creators to assert their fair use rights. These efforts would provide valuable assistance to existing enforcement tools as they confront large volumes of infringing activity occurring online.

In 2014, the Department of Commerce's Internet Policy Task Force convened a multistakeholder forum to find ways to improve the operation of the DMCA notice and takedown system. In April 2015, the Task Force released an agreement by the multistakeholder forum entitled "DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices," outlining practices to both pursue and avoid in order to improve the efficiency of DMCA notices by both senders and recipients.[54] The IPTF convened a multistakeholder forum on the issue that included a diverse set of stakeholders including rights holders, intermediaries, and users. Continued multistakeholder collaboration may achieve goals common to all members of the content creation and distribution ecosystem, and aim to protect creative works while continuing to maintain the benefits of an open and robust Internet.

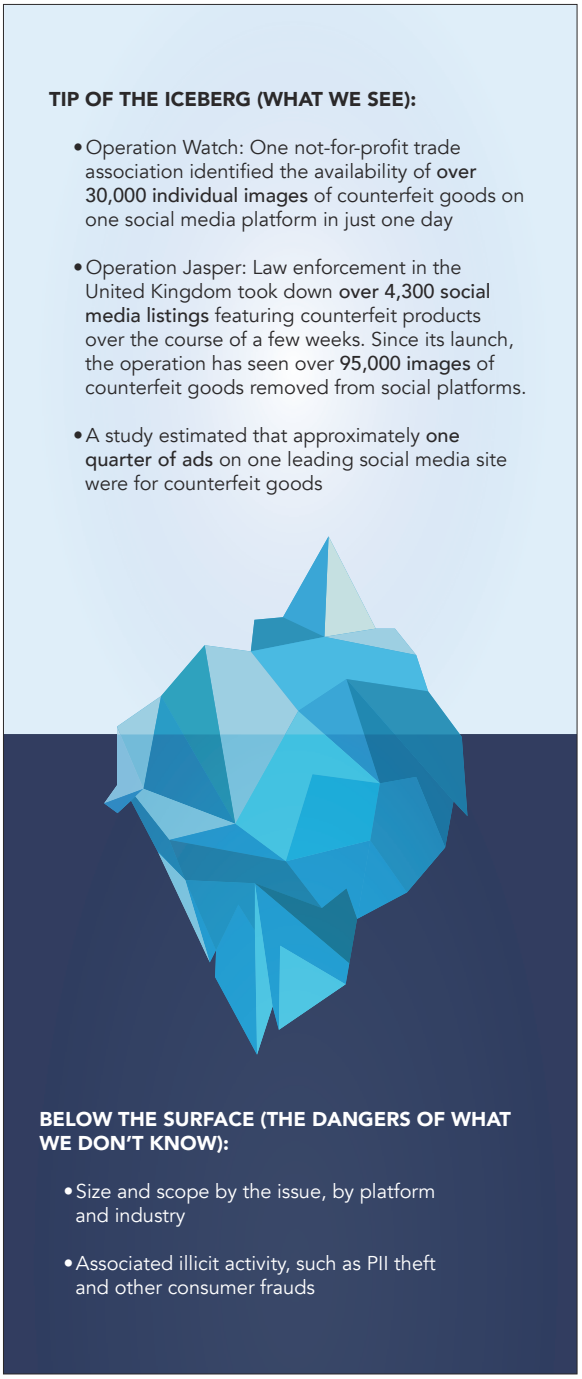
ACTION NO. 2.11: Support and promote the continued implementation of best practices in furtherance of evolving DMCA needs. The Department of Commerce's Internet Policy Task Force will monitor the progress made in the application of best practices and related topics. If and when it would be useful, the Task Force will reconvene the multistakeholder forum to further develop best practices and other measures to increase efficiency and effectiveness of the DMCA takedown process for all interested parties.

ACTION NO. 2.12: Support Copyright Office evaluation of Section 512. The United States Copyright Office is undertaking a public study to evaluate the impact and effectiveness of the safe harbor provisions contained in Section 512 of Title 17, United States Code. Among other issues, the Copyright Office study will consider the costs and burdens of the notice-and-takedown process set forth in section 512 on large- and small-scale copyright owners, online service providers, and the general public.[55] The Copyright Office will also review how successfully section 512 addresses online infringement and protects against improper takedown notices, and whether potential legislative improvements are advisable. As a member of the interagency Intellectual Property Enforcement Advisory Committee under the PRO-IP Act, the Copyright Office will provide a briefing to the Committee on its recommendations and findings. IPEC will work closely with the Copyright Office, and with other agencies, including those in the Internet Policy Task Force, to determine appropriate areas in which the Executive Branch may support balanced approaches to the Copyright Office's goals of improving the overall functioning of the safe harbor system.

3. Support Practices and Policies Within Social Media Channels to Curb Intellectual Property-Based Illicit Activity.

The rapidly evolving social media environment has given rise to new challenges for both copyright and trademark owners. Entities engaged in illicit activity targeting IP have adapted their tactics to exploit social media as new means to sell counterfeit goods as well as provide access to unauthorized streaming, downloading, stream-ripping, syncing and other means of illegally distributing protected content.

FIG. 39: Enforcement Activity Suggests the Scope of Problem Is Large.[57]



According to one United Kingdom law enforcement report, social media has recently overtaken online auction sites as criminals' "channel-of-choice" for counterfeit and piracy activity.[56]

Rogue actors operating in social media channels seek to deceive consumers in a number of relevant ways. These methods include: using social media tools to generate web traffic and divert consumers to websites selling their infringing products; using in-site "buy buttons" facilitating purchases directly from page posts and ads; relying on pseudonymous product reviews, blog entries and fabricated social media profiles to provide an aura of legitimacy; and using links and paid-for advertising space on social media platforms to generate illicit profits through the unlawful exploitation of third-party content.[58]

On the content-side, it has been reported that in the first quarter of 2015 alone, 725 of the 1,000 most watched videos on a leading U.S.-based social media site were unauthorized re-uploads from other media-hosting websites, generating a total of 17 billion misappropriated views in this short period.[59] These unauthorized re-uploads threaten the livelihood of original content creators and the artistic community as it deprives them of payment for their works, while simultaneously creating the possibility that unwarranted profits will be generated by social media channels through paid-for advertising featured alongside such unauthorized copyrighted content.[60]

Going forward, industry and policymakers must work together to address copyright infringement facilitated through the use of social media channels. In light of the volume of traffic and the complexity of the issues (including free speech and privacy rights of social media users), coupled with the threats to public health and safety (such as with the sale of fake medicines) and infringement of copyrights, the social media industry has an important role to play to establish meaningful standards and best practices to curb illicit activities on their respective platforms, while protecting the rights and ability of users to use those platforms for non-infringing and other lawful activities.

ACTION NO. 2.13: Encourage the development of industry standards and best practices, through a multistakeholder process, to curb abuses of social media channels for illicit purposes, while protecting the rights of users to use those channels for non-infringing and other lawful activities. Social media platforms generally have terms of services prohibiting unlawful practices, and opportunities exist to enhance express prohibitions with respect to copyright infringement and the promotion and sale of counterfeit merchandise,

as well the development of "repeat infringer" policies to address notorious or serial, bad faith offenders. Platforms should explore and adopt mechanisms that may facilitate the effective reporting of clear IP-related abuses of their services, while protecting the rights of users to use those platforms for non-infringing and other lawful activities. One underutilized resource may be the users themselves, who may be in a position to report suspicious product offerings or other illicit activity, if provided a streamlined opportunity to do so, as some social media companies are beginning to explore.

ACTION NO. 2.14: Encourage the development of "know your seller" programs for social media channels engaged in e-commerce. In order to minimize the exploitation of a site's services and platforms by entities engaged in the sale of counterfeit goods, social media platforms could consider requiring new sellers using the social media platform to submit to a multi-factor verification system or other mechanism to support a "trusted" seller and advertiser program.

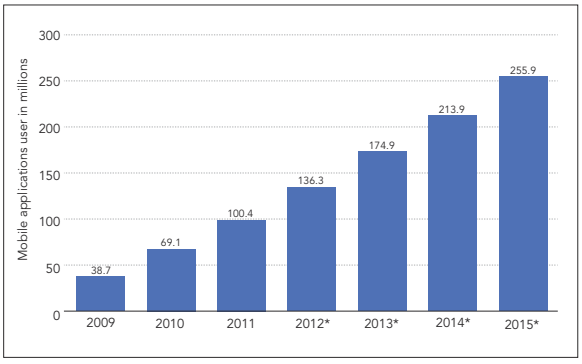
4. Support Practices and Policies to Reduce Intellectual Property Infringement Facilitated by Mobile Apps.

Mobile applications (apps) have changed the way people communicate and access, share, and interact with information. More than 3 billion people, or 44 percent of the world's population, will access the Internet in 2016—and two billion of them will use only mobile devices to do so.[61] As more people access creative content, e-commerce, financial services, and lifestyle services from their smartphones and tablets, mobile app downloads and engagement is expected to continue to increase exponentially. Indeed, a recent study reported that overall app usage grew by 58 percent in 2015.[62]

Millions of apps currently exist in today's mobile app market, and with 1,000 new apps added daily, the mobile apps market continues to thrive.[65] The same low entry barriers that catalyze innovation also make mobile apps an attractive outlet for illicit IP-related activity, including: counterfeit apps, such as fake antivirus, browsers, and games;[66] apps filled with content stripped from another app or site without authorization;[67] and apps that illegally stream copyrighted content such as hit TV shows or movies.[68] A fake version of the popular "Angry Birds" game, for example, was reported to contain harmful malware in the form of a "Trojan horse" virus.[69]

The growth of illicit apps must be viewed in the larger context of opportunistic, cyber-based illicit activity. Whereas developers make money from apps by pushing advertisements to users, online criminals may install mobile ad software development kits in their fake copies so they receive the revenue instead of the original developers, and they may insert malicious code that can result in harm to the user.[70]

FIG. 40: Mobile App Usage on the Rise.[63]



Source: Statista[64]

FIG. 41: Example of Fake App That Extracts Account Data.[71]



Source: Symantec

Despite efforts to screen for potential infringing apps,[72] consumers continue to have access to illicit apps. This is in part because when an illicit app is taken down, a new one often takes its place, app developers find new avenues to distribute the app, or existing downloads are not necessarily disabled.[73]

Without action, the number of infringers may continue to grow and may begin to crowd out legitimate creators. Looking ahead, industry and policymakers must ensure that mobile app platforms function as gateways to innovative and lawful new ways for users to engage with content. Needed improvements to the mobile app ecosystem could be achieved in a variety of ways, including coordinated, voluntary best practice initiatives, created through a multistakeholder process.

ACTION NO. 2.15: Encourage research and development of industry standards and best practices created through a multistakeholder process involving a diverse set of interested parties to curb IP-infringing apps and abuses on app platforms while protecting the rights of users to use apps for non-infringing and other protected activities. Content owners and app developments, together with app stores and other relevant stakeholders, are encouraged to create or enhance existing tools that identify IP-infringing apps before they become available for purchase. IPEC and other relevant members of the U.S. Interagency Strategic Planning Committees on IP Enforcement will explore opportunities to support the development of balanced and measured best practices for app and app distribution platforms.

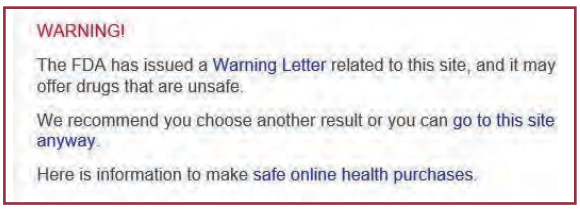
5. Putting the Consumer First: Combatting Operators of Notorious Websites by Way of Consumer Education.

The digital economy is a significant driver of U.S. economic growth,[74] but it cannot fully succeed if consumers do not trust their security and privacy online. The public and private sectors jointly share a responsibility to promote a safe and secure Internet that minimizes opportunities for deception and fraud and reduces the vulnerability of web users. Cooperation between the public and private sectors can bolster the security and integrity of the Internet environment while ensuring the free flow of information vital to the structure of the digital economy.

By way of example, Internet and tech companies came together in the early-2000s to support an initiative to protect consumers from malware—computer viruses, spyware, and the programs that steal data, send spam, or otherwise infect a user's computer—in a manner that consumers can understand, and learn from in the process.[75] This and other initiatives have resulted in something to which web users are now all well accustomed, *i.e.*, educational banner pop-ups informing a user that the target site is suspected of propagating malware (FIG. 42, alternate page).

In this spirit, a leading search provider partnered with the U.S. Food and Drug Administration (FDA) in late 2015 to help give users more information about the dangers of visiting unsafe online pharmacies so they can make informed decisions.[76] The educational pop-up shown in Figure No. 43 appears when a participating search user clicks on a pharmaceutical site that has been cited by the FDA as a fake online pharmacy engaged in illegal activity, such as the sale of counterfeit drugs to U.S. consumers.

FIG. 43: "Fake Online Pharmacy" Educational Pop-Up.



This educational pop-up does not prevent users from visiting the site, but rather cautions them about the possible risks of proceeding to the site, and in turn provides links to resources where they can learn more about selecting a safe online pharmacy. If the owner of an affected site believes that the pop-up notice is in error, there is a process in place for that company to address the issue.

These and other evolving online practices are educating the public and providing enhanced trust and security in areas that pose significant risk of harm to the public. There is an opportunity to develop new, and to refine existing, targeted educational campaigns for purposes of consumer protection. As exemplified in the FDA-Search example, public-private partnerships aimed at reducing the consumer knowledge gap through the development of appropriate education initiatives enable consumers to make better informed and safer online transactions.

FIG. 42: Examples of Educational Pop-Ups Issued by Search, Browsers, Operating Systems, and Anti-Virus Software.



Excerpt from *The Economist*

"The most troubling recent trend is that online counterfeiters have discovered a new source of revenue. Some of their sites have no goods to sell, real or fake. They are simply out to steal unwitting shoppers' card details, a business that can enjoy higher margins than [counterfeiting]."

(August 1, 2015)

Source: http://www.economist.com/news/business/21660111-makers-expensive-bags-clothes-and-watches-are-fighting-fakery-courts-battle.

One area that may be appropriate for private sector consideration as an educational pilot program is to identify the sub-set of websites dedicated to engaging in the sale of counterfeit goods, where payment processing services have been expressly withdrawn by one or more credit card networks (a verifiable factor), but where the withdrawn service provider's logo remains visible on the "checkout page." In this case, the consumer is lured to enter his or her credit card information (and other PII) in a situation where the site operator, brand owner, payment processor and others are fully aware that the transaction will not go through, but where the PII may nonetheless be compromised. A similar pop-up warning message—at search level, at the browser level, by the operating system, or by way of an anti-virus software provider—may be appropriate in this limited circumstance, subject to adequate controls.

The private sector is encouraged to examine opportunities for targeted consumer education on known sites that pose verifiable risks.

ACTION NO. 2.16: Convene an interagency group to identify options to analyze online consumer behavior and identify means to promote consumer protection. IPEC will convene an interagency group, including Federal independent agencies such as the Consumer Product Safety Commission and the Federal Trade Commission, and other relevant stakeholders, to discuss and assess online consumer behavior to better understand threats and vulnerabilities; evaluate existing Federal, state, and private sector consumer education efforts; and identify opportunities for effective programs to protect consumers.

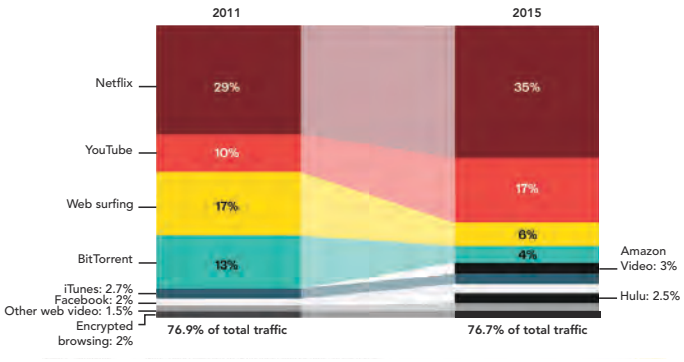
6. Encourage Efforts that Support Content Platforms Offering Content Legally and Minimize Deceptive Sites That Operate with a Commercial "Look and Feel."

Under the right conditions in the global marketplace, content providers will continue to expand the reach of their services and platforms, helping to erode rates of piracy as consumers are presented with enhanced options to obtain and enjoy content lawfully. Put simply, when people around the world are given real choices between legal and illegal options for accessing content, the vast majority will want to choose the legal option when it is made readily available.[77]

In this vein, a growing number of legitimate providers of streaming movies, television shows, music and other content have been investing significant financial and other resources to expand offerings, including for example, one provider that recently expanded its platform to directly serve over 190 countries, making licensed content available nearly worldwide.[78] The wide accessibility of online content platforms promoting legal access to content may be reducing certain types of web traffic traditionally associated with piracy, such as with peer-to-peer networks via BitTorrent (FIG. 44).

Investments by online platforms legally offering content (to expand their geographic service, the availability of licensed content, or the production of original content) are subject to a number of challenges

FIG. 44: Web Traffic Streams (2011-2015).



Source: Sandvine
Note: Data collected in September and October of each year

and limitations. These content providers face a panoply of differing national laws and enforcement regimes around the world, and sites face the difficulty of having to compete with those offering infringing content at a lower cost (often for free) or otherwise free of certain other potential limitations or restrictions. This challenge is only exacerbated when the unlawful option is designed to attract and mislead consumers by operating in a manner much like popular, legitimate sites. Such sites are notable for their commercial "look and feel," including featuring prominent branding, third-party advertisements and credit card logos—that lend an air of legitimacy (FIG. 45).

Although the operator of a website dedicated to infringement may switch between gTLDs, ccTLDs, registrars, or hosting companies when challenged for IP infringement, for example, the illict activity could be significantly curtailed if the operator is unable to take his name or brand along the way from website to website, (Sec. II, B).

The growth of legal alternatives will likely help to reduce piracy rates in parts of the world by making lawful content more readily accessible. However, these efforts must go hand-in-hand with continued enforcement efforts against unlawful actors to ensure that IP-infringing activity is not permitted to outpace the expansion of sites legally providing access to content.

FIG. 45: Commercial Look-and-Feel: Example of "Notorious Market" Piracy Site.[79]



ACTION NO. 2.17: Promote best practices that bring broader awareness of online sources of legal available content. The U.S. Interagency Strategic Planning Committees on IP Enforcement, and other relevant Federal agencies, as appropriate, will assess opportunities to support public-private collaborative efforts aimed at increasing awareness of legal sources of copyrighted material online and educating users about the harmful impacts of digital piracy.

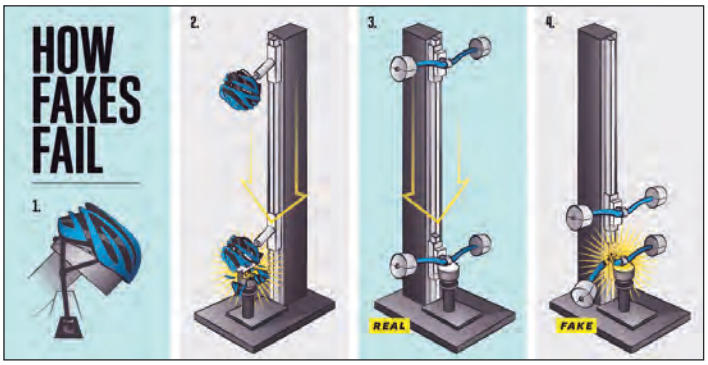
ACTION NO. 2.18: Support and improve the coordination of U.S. and foreign enforcement efforts aimed to protect IP abroad, including targeting unlawful actors that infringe U.S. IPR and inhibit the growth of online sites offering legal access to content. The IPR Center will continue to support efforts to curb infringing activity overseas, including by identifying appropriate opportunities for law enforcement joint operations.

7. Opportunities to Curb Sales of Counterfeit and Pirated Goods on E-Commerce Platforms.

E-commerce platforms provide a thriving online marketplace in which goods can be bought and sold from anywhere in the world, by way of various models such as Business-to-Consumer (B2C), Business-to-Business (B2B), and Consumer-to-Consumer (C2C). With e-commerce sales steadily growing over the past decade and projected to reach $1.915 trillion in 2016,[80] counterfeiters (including domestic and international criminal organizations) have turned their attention to online marketplaces.[81]

In the online environment, consumers are often unable to distinguish meaningfully between authentic and counterfeit products. Counterfeiters, for example, will use pictures of the authentic product and will set the sales price close to the price of the genuine article, so as to hide any clear indications that their product is actually counterfeit. In light of these and other tactics, consumers are frequently unaware that the products they are buying online could be fake. One study found that nearly one out of every four online shoppers had reported unknowingly

FIG. 46: Dangerous Goods Abound - Example of Counterfeit Bicycle Helmet Sold Online.



Source: http://www.bicycling.com/bikes-gear/components/catch-counterfeiter-sketchy-world-fake-bike-gear

SAFETY TESTING RESULTS:

Dynamic Retention Test: Counterfeit helmet is strapped and adjusted to a level head form. A 4kg weight is secured to the chinstrap and dropped .6m. The straps can't stretch more than 30mm. The fake exceeded 30mm.
= FAIL

Impact Test: Counterfeit helmet is strapped to a 5kg head form and dropped from various heights onto flat, hemispherical and metal anvils. Peak instantaneous acceleration on impact may not exceed 300 Gs. The fake's peak acceleration reached 1,052 Gs.
= FAIL

purchasing products online that later turned out to be counterfeit.[82] In addition to defrauding customers, these counterfeit products can cause serious injury and even death (FIG. 46).

It is difficult to identify and effectively terminate online sellers of counterfeit goods. The scale and volume of the transactions presents unique challenges. Alibaba Group Holding, for example, reported over $14 billion in e-commerce transactions in 2015 during its "Singles' Day" (November 11th), which is a peak day for e-commerce activity in China.[83]

Opportunities exist for governments, rights holders, and the owners and operators of e-commerce sites to engage in sustained and meaningful efforts to combat counterfeiting within these e-commerce platforms. Enhanced coordination between rights holders and marketplaces, for example, is required to identify effectively and timely remove infringing listings, while coordination and cooperation is necessary among all stakeholders to curb persistent serial offenders.

Some leading e-commerce businesses have developed internal best practices and policies with respect to infringing products. These and other efforts must be encouraged and directed toward the continued evolution of these practices, to expanding the adoption of best practices around the globe, and to enhancing benchmarking, transparency, and public reporting of counterfeit incidents in order to support data-driven policies.

The use of technology by e-commerce platforms (such as algorithms to spot fraud) has provided enhanced detection measures over the years that, coupled with other actions, have reportedly helped to combat the proliferation of counterfeit goods being sold online. Technological solutions must not remain static, and in light of new trends and counterfeit practices, there remains an opportunity for continued investments in technological improvements and innovative business practices to protect consumers and IP rights holders.

The U.S. Government, by way of its law enforcement agencies, is in a unique position to share appropriate information on emerging trends, the behavior of criminal syndicates, and other relevant data; and to assist e-commerce sites in refining their proprietary analytical tools and techniques to identify and disrupt fraud in the form of counterfeit and pirated goods carried on their platforms.

ACTION NO. 2.19: Support enhanced coordination between rights holders and e-commerce platforms. To help facilitate enhanced coordination between rights holders and leading e-commerce platforms, IPEC—in partnership with the FBI, the IPR Center, USPTO, USTR, and other relevant members of the U.S. Interagency Strategic Planning Committees on IP Enforcement—will coordinate an annual meeting to assess the state of e-commerce initiatives to curb counterfeit trade, and opportunities for

continued enhancement and development of "best practices." E-Commerce sites are encouraged to maintain and publish clear take-down procedures and statistics to aid rights holders, deter repeat offenders, and support meaningful and effective enforcement policies.

ACTION NO. 2.20: Support advanced, technology-driven measures to curb illicit accounts. E-Commerce platforms are encouraged to adopt advanced technology measures to prevent known offenders (including terminated sellers) from opening new accounts, or jumping from platform to platform. The wide-spread adoption of a ratings system allowing the public to assess whether a seller has any history of counterfeit violations (or no transaction history at all) may prove useful in improving consumer awareness and making it more difficult for illicit actors to establish a long-term business model or client-base.

ACTION NO. 2.21: Support enhanced transparency and public reporting of counterfeit incidents on e-commerce platforms. In light of the potentially criminal nature of counterfeit trade, consumers should have access to the tools needed to assess the nature and frequency of counterfeit incidents on an e-commerce platform. Specifically:

- Enhanced transparency and public reporting of generalized and anonymized data regarding counterfeit incidents on e-commerce platforms provides an opportunity to educate consumers and assist law enforcement, consumer protection entities, policy-makers, and others to understand better the scope of the issue, while producing additional incentives to ensure continued evolution of best practices.
- E-Commerce platforms are encouraged to share complete selling history records to law enforcement upon the identification of a seller suspected of being engaged in significant counterfeiting operations.
- IPEC—in partnership with the FBI, the IPR Center, USPTO, USTR, and other relevant Federal agencies—will assess opportunities to support e-commerce transparency efforts.

ACTION NO. 2.22: Encourage development of enhanced "know your seller" programs in e-commerce channels. In order to minimize the exploitation of e-commerce platforms by entities engaged in the sale of counterfeit goods, e-commerce platforms are encouraged to assess the applicability of an appropriately tailored "know your seller" program, where, for example, sellers provide some measure of identity verification before being able to sell products via the site. Adoption of a voluntary multi-factor verification system or other mechanism to support a "trusted" seller program may curb illicit exploitation of e-commerce channels, while providing consumers additional tools in order to assess the risks associated with any particular merchant.

ACTION NO. 2.23: Promote and expand U.S. law enforcement partnerships with e-commerce platforms to disrupt incidents of fraud. The Department of Homeland Security—in partnership with the FBI and law enforcement agencies in the United States and abroad, as appropriate—will continue to invest in and further develop and promote its private sector outreach programs to facilitate the sharing of information with e-commerce sites on emerging trends, criminal syndicates, and other relevant matters to improve identification and disruption of illicit trade and consumer fraud.

D. SUPPORT RESPONSIBLE 3D PRINTING COMMUNITIES AND BUSINESS MODELS.

Additive technology, also known as 3D printing, is emerging as one of the most important transformative changes in manufacturing processes and global supply chains today. This evolving technology is offering the promise of a manufacturing environment driven by digital data. As one commentator noted, the move to 3D printing may be understood as a transformation from a traditional supply chain that is hardware-based to one that is "software-defined."[84]

Unlike conventional or "subtractive" manufacturing processes—such as drilling or milling that creates a part by cutting away and removing material—additive manufacturing builds a part by fusing materials together, layer-by-layer, with heat, chemicals, adhesives, or other methods. Additive manufacturing has been employed in design and prototyping for

some time, but the application is now shifting rapidly to the direct production of parts that are ready for distribution and sale.[85]

Reports indicate that manufacturing leaders may not be fully prepared for a projected rapid migration toward additive technology.[86] As a GAO report has summarized, 3D printing poses far-reaching implications for businesses, consumers, and policymakers on a wide array of issues, including on grounds of national security, product liability, IP, and environmental, health, and safety concerns.[87] With respect to IP, one of the primary concerns is that as scanning and 3D printing technology improves and proliferates, the digital design files that support 3D printing will be widely shared on the Internet. Sharing design files may help researchers and legitimate uses such as open licenses, however there is some concern that it would make it easier for entities to bypass and infringe upon valid utility and design patents, copyrights, and trademarks.[88]

The challenge for all stakeholders is to ensure that 3D printing's potential is realized in a manner that contributes positively to innovation and that protects non-infringing uses without providing new and troubling avenues for counterfeiters and bad actors to further evolve their illicit trade practices. Public-private partnerships can play a critical role in ensuring that appropriate IP protections do not lag behind 3D printing technological advances. Exploring how to apply IP laws, including patents, copyrights, and trademarks, or utilizing technological solutions to curb the abuse of 3D printing within software sharing communities and platforms, would help to ensure that this new emerging technology will be integrated into the economy while protecting against its exploitation by illicit actors.[89]

ACTION NO. 2.24: Support responsible integration of 3D printing into manufacturing and business practices. The U.S. Interagency Strategic Planning Committees on IP Enforcement will continue to monitor the integration of 3D printing into responsible manufacturing and business practices, including assessing the sufficiency of current laws, implementation of those laws in practice, and the state of, and challenges associated with, the prosecution of IP-based crimes involving 3D printing, while protecting non-infringing uses of the technology.

E. ADDRESS CYBER-ENABLED TRADE SECRET THEFT.

Cybersecurity is one of the most important challenges we face as a Nation. Malicious actors, whether they are criminals, terrorists, or nation state actors, can ignore traditional national borders and conduct their malicious cyber activities from afar. As more data that is sensitive is stored online, the potential consequences of such attacks are only growing more significant. U.S. businesses and academic institutions are increasingly targeted for economic espionage and theft of trade secrets by foreign entities. With the increasing connectivity of our businesses and academic institutions, there is a greater change that these malicious actors will use cyber-enabled means to steal trade secrets or other confidential business information. Gone are the days when a spy needed physical access to a document to steal it, copy it, or photograph it; modern technology now enables global access and transmission instantaneously.

Due to the profound implications of cybersecurity and cyber-enabled trade secret theft to the Nation, the Federal Government has been aggressive in meeting these threats head-on. The United States must lead international efforts to build consensus on conceptions of responsible state behavior in order to enhance international cyber stability by reducing the risk of escalation posed by national security threats – including threats to economic security – emanating from cyberspace. The identification and promotion of voluntary, peacetime norms of responsible state behavior in cyberspace is one pillar of the United States' framework for stability, which also includes the affirmation of the applicability of international law to cyberspace, and the development and implementation of practical confidence building measures. One norm the United States has identified is that states should not conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.

In the context of Chinese President Xi Jinping's September 2015 visit to Washington, the United States and China made a series of cyber commitments, including that neither state would engage in the cyber-enabled theft of intellectual property for commercial gain. Building on the commitment, the United States successfully

obtained an affirmation of this norm by the leaders of the G-20 at the 2015 Antalya Summit, and is working with likeminded countries to encourage broader international adoption of this and other norms of responsible state behavior, including that states should cooperate with requests for assistance in mitigating malicious cyber activity emanating from their territory.

Since the U.S. – China commitment on cyber-enabled IP theft for commercial gain, we have seen a number of other countries seek and reach agreement with China on similar commitments of their own, including Germany, and the United Kingdom. Adherence to our bilateral cyber commitments is an important part of the overall U.S. – China relationship, and it is reviewed throughout the year, including during the semi-annual meetings of the U.S. – China High-Level Joint Dialogue on Cybercrime and Related Issues.

In addition to these initiatives, the United States will continue to leverage the full array of tools to take appropriate action against those who engage in cyber-enabled theft of intellectual property for commercial gain. These tools include law enforcement action as well as economic actions, which could include designating entities under Executive Order 13694 issued on April 1, 2015, declaring that certain malicious cyber-enabled activities constitute a serious threat to U.S. national security and economic competitiveness, including specifically the misappropriation of trade secrets for commercial or competitive advantage or private financial gain.[90]

The United States will also continue to implement relevant strategies and Acts, including the U.S. "Strategy on Mitigating the Theft of U.S. Trade Secrets" issued in 2013,[91] and the Defend Trade Secrets Act of 2016. In February 2016, President Obama directed the implementation of the Cybersecurity National Action Plan (CNAP) that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.[92] Trade secret theft is more broadly addressed in Section IV of this plan. Through ongoing implementation of these strategies and Acts, the U.S. Government will continue to monitor, assess, and respond to cyber-enabled trade secret theft, as appropriate.

ENDNOTES

[1] *See, e.g.*, Organization for Economic Cooperation and Development, "*The Economic Impact of Counterfeiting and Piracy*," at p. 273 (2008), accessed from http://www.keepeek.com/Digital-Asset-Management/oecd/trade/the-economic-impact-of-counterfeiting-and-piracy_9789264045521-en#.V_0WF_lrjq4#page1. *See also* Digital Citizens Alliance, "*Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business*," at p. 8 (February 2014), accessed from http://media.digitalcitizensactionalliance.org/ 314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf.

[2] *See, e.g.*, Blackstone, Erwin *et al.*, "*The Health and Economic Effects of Counterfeit Drugs*," American Health & Drug Benefits, 7(4): 216, at p. 220 & n.37 (June 2014), accessed from http://www.ncbi.nlm.nih.gov/pmc/articles/ PMC4105729/#R37, citing to Ehrenberg, Rachel, "*Counterfeit Crackdown*," Science News, 179: 22-25 (June 18, 2011), available at [subscription required] https://www.sciencenews.org/article/counterfeit-crackdown.

[3] *See, e.g.*, Kan, Paul Rexton *et al.*, "*Criminal Sovereignty: Understanding North Korea's Illicit International Activities*," at p. 15 (U.S. Army War College, Strategic Studies Institute; March 2010), accessed from http://www.strategicstudiesinstitute.army.mil/pdffiles/pub975.pdf.

[4] A diverse set of stakeholders has long advocated for the development and implementation of a "follow the money" approach as a solution to curb commercial online piracy and counterfeiting. This approach is embodied in the voluntary private sector initiatives that have been developed and implemented, which are discussed elsewhere in this Strategic Plan and in the 2013 Joint Strategic Plan on Intellectual Property Enforcement. This approach was also discussed, for example, at the 2011 hearing (before the House Judiciary Committee's Subcommittee on Intellectual Property, Competition, and the Internet) on "*Promoting Investment And Protecting Commerce Online: Legitimate Sites v. Parasites*" (March 14 and April 6, 2011), House Doc. 112-153, accessed from https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg65186/html/CHRG-112hhrg65186.htm. *See also* Abrams, Rachel, "*Eric Schmidt, Harvey Weinstein Talk Piracy*," Variety (July 11, 2013), accessed from http://variety.com/2013/digital/news/sun-valley-eric-schmidt-harvey-weinstein-talk-piracy-1200561819/ (quoting Eric Schmidt from Google as saying that: "Our position is that somebody's making money on this pirated content and it should be possible to identify those people and bring them to justice.").

[5] *See* International Chamber of Commerce (ICC)/Business Action to Stop Counterfeiting and Piracy (BASCAP), "*Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain*," at p.89 (March 2015), accessed from http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/International-engagement-and-Advocacy/Roles-and-Responsibilities-of-Intermediaries/. *See also* Federal Bureau of Investigation, "*Countering the Growing Intellectual Property Theft Threat: Enhancing Ties Between Law Enforcement and Business*" (January 22, 2016), accessed from https://www.fbi.gov/news/stories/countering-the-growing-intellectual-property-theft-threat ("Technological advances continue at an even faster pace, dramatically increasing the threat posed by criminals who steal trade secrets, produce and/or traffic in counterfeit products, and infringe on copyrights. One important factor in this increase is the global expansion of online marketplaces, which aids international and domestic criminal organizations in trafficking in counterfeit goods.").

[6] Below are examples of Terms of Service:

Visa Terms of Service:	"Visa is committed to preventing the use of its payment brand and system for illegal transactions…" and "upon receiving…credible evidence…that the merchant ("Merchant") is engaged in transactions involving the sale of infringing goods on the Internet using Visa-branded payment cards, Visa [may direct] the Merchant to cease selling infringing goods identified by the IP Owner or terminating the Merchant account." *See* https://usa.visa.com/legal/intellectual-property-rights.html
MasterCard Terms of Services:	"MasterCard has…adopted a policy that provides for the immediate removal of any content or the suspension of any user that is found to have infringed on the rights of MasterCard or of a third party, or that has otherwise violated any intellectual property laws or regulations…" *See* https://www.mastercard.us/en-us/about-mastercard/what-we-do/terms-of-use.html#propertyrights
American Express Terms of Services:	Establishing that American Express cards may not be used "…for sales of products over the Internet that would constitute a violation of copyright or trademark laws[.]" *See* https://www.americanexpress.com/us/content/legal-disclosures/website-rules-and-regulations.html?inav=footer_Terms_of_Use

[7] International Anti-Counterfeiting Coalition, "*IACC Payment Processor Portal Program: First Year Statistical Review*," at pp. 13-14 (Oct. 2012), accessed from http://docplayer.net/2433238-International-anticounterfeiting-coalition-iacc-payment-processor-portal-program-first-year-statistical-review.html.

[8] "A 'trace message' is an attempt to make an online purchase using a valid, yet set-to-decline credit card. It is similar to a test purchase, but because the payment is declined, no goods are delivered. The purpose of a trace message is to assist the Card Network in identifying the merchant account associated with the website." International Anti-Counterfeiting Coalition, "*IACC Payment Processor Portal Program: First Year Statistical Review*," at p. 6 n.5 (October 2012), accessed from http://docplayer.net/2433238-International-anticounterfeiting-coalition-iacc-payment-processor-portal-program-first-year-statistical-review.html. Regarding the detection systems that thwart "test" transactions, *see id.*, at pp. 15-16 & n. 18.

[9] By contrast, in the closed-loop payments model (e.g., American Express), the payment services are provided directly to merchants by the owner of the network without involving third-party financial institution intermediaries. *See, e.g.*, International Anti-Counterfeiting Coalition, "*IACC Payment Processor Portal Program: First Year Statistical Review*," at p. 7 (October 2012), accessed from http://docplayer.net/2433238-International-anticounterfeiting-coalition-iacc-payment-processor-portal-program-first-year-statistical-review.html.

[10] *See, e.g.*, Mike Weatherley, MP (Intellectual Property Adviser to the Prime Minister), on "*Follow The Money: Financial Options To Assist In The Battle Against Online IP Piracy: A Discussion Paper by Mike Weatherley, MP* " (2014), accessed from http://www.olswang.com/media/48204227/follow_the_money_financial_options_to_assist_in_the_battle_against_

online_ip_piracy.pdf. *See also* United Nations Interregional Crime and Justice Research Institute (UNICRI) and International Chamber of Commerce (ICC)/Business Action to Stop Counterfeiting and Piracy (BASCAP), "*Confiscation of the Proceeds of Crime: A Modern Tool for Deterring Counterfeiting and Piracy*" (April 2013), accessed from http://www.unicri.it/services/library_documentation/publications/unicri_series/A_modern_tool_for_deterring_counterfeiting_and_piracy.pdf; European Commission, "*Commission presents actions to better protect and enforce intellectual property rights*" (July 1, 2014) ("The adoption of this Action Plan shows how we want to re-orientate our policy towards better compliance with intellectual property rights by the private sector", said EU Commissioner for Internal Market and Services Michel Barnier. "Rather than penalising the individual for infringing intellectual property rights, often unknowingly, the actions set out here pave the way towards a 'follow the money' approach, with the aim of depriving commercial-scale infringers of their revenue flows."), accessed from http://europa.eu/rapid/press-release_IP-14-760_en.htm.

[11] International Chamber of Commerce (ICC)/Business Action to Stop Counterfeiting and Piracy (BASCAP), "*Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain,*" at p. 91 (March 2015), accessed from http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/International-engagement-and-Advocacy/Roles-and-Responsibilities-of-Intermediaries/.

[12] *See* Victoria Espinel, United States Intellectual Property Enforcement Coordinator, "*Progress on the Intellectual Property Enforcement Strategy*" (February 7, 2011), accessed from https://www.whitehouse.gov/blog/2011/02/07/progress-intellectual-property-enforcement-strategy; United States Government, "2013 Joint Strategic Plan on Intellectual Property Enforcement," at pp. 1-2, 36 (June 2013), accessed from https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

[13] *See, e.g.*, International Anti-Counterfeiting Coalition (IACC), "RogueBlock®," accessed from http://www.iacc.org/online-initiatives/rogueblock (discussing the "collaborative effort of the IACC and the payment industry to create a streamlined, simplified procedure for members to report online sellers of counterfeit or pirated goods directly to credit card and financial services companies"; "To date, the program has terminated over 5,000 individual counterfeiters' merchant accounts, which has impacted over 200,000 websites.")

[14] *See, e.g.*, International Intellectual Property Alliance, Comment Letter to U.S. Intellectual Property Enforcement Coordinator, at pp. 5-6 (October 16, 2015) (providing comments in response to IPEC's Federal Register notice of September 1, 2015), accessed from https://www.regulations.gov/?s#!documentDetail;D=OMB-2015-0003-0043.

[15] Digital Citizens Alliance, *"Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business,"* at p. 1 (May 2015), accessed from https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/298a8ec6-ceb0-4543-bb0a-edc80b63f511.pdf.

[16] *See, e.g.*, Office for Harmonization in the Internal Market (OHIM), *"Digital Advertising on Suspected Infringing Websites,"* at p. 1 & n. 4 (January 2016) (explaining that "86% of peer-to-peer infringing websites exist due to advertising revenue"), accessed from https://euipo.europa.eu/ohimportal/documents/ 11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites, *citing to* PRS for Music and Google, "*The Six Business Models of Copyright Infringement: A data-driven study of websites considered to be infringing copyright,*" at p. 11 (June 27, 2012), accessed from https://www.prsformusic.com/aboutus/policyandresearch/researchandeconomics/Documents/TheSixBusinessModelsofCopyrightInfringement.pdf.

[17] *See, e.g.*, Digital Citizens Alliance, "*Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business*" (February 2014) at p. 8, accessed from: http://media.digitalcitizensactionalliance.org/ 314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf.

[18] *See, e.g.*, Google, "*AdSense Program Policies*" ("**Copyrighted material.** AdSense publishers may not display Google ads on webpages with content protected by copyright law unless they have the necessary legal rights to display that content. This includes sites that display copyrighted material, sites hosting copyrighted files, or sites that provide links driving traffic to sites that contain copyrighted material. . . . **Counterfeit goods.** AdSense publishers may not display Google ads on webpages that offer for sale or promote the sale of counterfeit goods. . . ."), accessed from https://support.google.com/adsense/answer/48182?hl=en&ref_topic=1261918&rd=1; Google, "*Content Policies*" ("Copyrighted material. What's the policy? Google ads may not be displayed on websites with content protected by copyright law unless they have the necessary legal rights to display or direct traffic to that content. Some examples of copyrighted content might include MP3 and video files, television shows, software, comics, and literary works. . . ."), accessed from https://support.google.com/adsense/answer/1348688#Copyrighted_material.

[19] Office for Harmonization in the Internal Market (OHIM), *"Digital Advertising on Suspected Infringing Websites,"* at pp. 23-24 (January 2016) ("click generators and malware found in 51% of the ads"), accessed from https://euipo.europa.eu/ohimportal/documents/ 11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites. *See* Digital Citizens Alliance, *"Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business,"* at p. 9 (February 2014) ("The actual downloads often contain malware. These ads were extremely common, appearing on 60% of the large sites."), accessed from http://media.digitalcitizensactionalliance.org/314A5A5A9ABBBB C5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf.

[20] *See, e.g.*, United States Government, "*2013 Joint Strategic Plan on Intellectual Property Enforcement,*" at pp. 2, 36 (June 2013), accessed from https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf. For additional background on the advertising industry activities, see the following discussion in Trustworthy Accountability Group (TAG), "*Core Criteria for Effective Digital Advertising Assurance, version 1.0,*" at page 2 (footnotes omitted) (February 2015), accessed from https://tagtoday.net/wp-content/uploads/2015/02/Core-criteria_final.pdf:

> "The major advertising trade associations have recognized this issue and have taken a leadership role in addressing it. In 2012, the Association of National Advertisers (ANA) and the American Association of Advertising Agencies (4A's), supported by the Interactive Advertising Bureau (IAB), adopted a Statement of Best Practices to Address Online Piracy and Counterfeiting, providing language for marketers to use in their media placement contracts and insertion orders to prevent advertisements from appearing on sites

dedicated to intellectual property infringement. In July 2013, leading ad networks also announced a set of Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting. Also in 2013, the IAB updated its Network and Exchange Quality Assurance Guidelines to include a ban on selling ad inventory on "copyright infringement" and "warez" sites. In June 2014, the IAB also announced its Trustworthy Digital Supply Chain Initiative, identifying fighting Internet piracy as one of its five objectives, along with eliminating fraudulent traffic, combatting malware, and promoting brand safety through increased transparency, and creating accountability."

[21] The initiative is spearheaded by the Trustworthy Accountability Group (TAG), which was created by the Association of National Advertisers (ANA), the American Association of Advertising Agencies (4A's), and the Interactive Advertising Bureau (IAB). According to its website, TAG is a "cross-industry accountability program to create transparency in the business relationships and transactions that undergird the digital ad industry, while continuing to enable innovation. A joint marketing-media industry program, TAG was created with a focus on four core areas: eliminating fraudulent digital advertising traffic, combating malware, fighting ad-supported Internet piracy to promote brand integrity, and promoting brand safety through greater transparency." TAG, "*About Us*," accessed from http://www.tagtoday.net/aboutus/.

[22] *See* Trustworthy Accountability Group (TAG), *"Largest Brands And Agencies Take TAG Pledge To Fight Ad-Supported Piracy For All Digital Ads*" (December 8, 2015), accessed from https://tagtoday.net/largest-brands-and-agencies-take-tag-pledge-to-fight-ad-supported-piracy-for-all-digital-ads/ (noting that "many of the world's largest brand advertisers and agencies have pledged to require their ad partners to take aggressive steps to help fight the $2.4 billion lost to pirate sites each year.")

[23] *See, e.g.*, Digital Citizens Alliance, "*Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business,*" at pp. 3, 9 (February 2014), accessed from http://media.digitalcitizensactionalliance.org/ 314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/4af7db7f-03e7-49cb-aeb8-ad0671a4e1c7.pdf.

[24] Kat.cr is subject to a number of court-ordered injunctions due to copying infringement, and is described in USTR's 2015 review of "notorious markets" as "the biggest torrent site in terms of visitors and popularity." Office of the United States Trade Representative, "*2015 Out-of-Cycle Review of Notorious Markets,*" at p. 14 (December 2015), accessed from https://ustr.gov/sites/default/files/USTR-2015-Out-of-Cycle-Review-Notorious-Markets-Final.pdf. Screen shots from <Kat.cr> were captured on May 2, 2016, featuring third-party advertisements on behalf of the likes of GoDaddy, GAP, West Elm, Edible Arrangements, Jaguar, Sephora, National Geographic, Giant (and Tide), Starwood (and American Express), Verizon, Pottery Barn, Gilt, and the Ad Council (on behalf of the U.S. Forest Service).

[25] *See, e.g.*, United States Department of State, Bureau for International Narcotics and Law Enforcement Affairs, "*International Narcotics Control Strategy Report, Volume II: Money Laundering and Financial Crimes*," at p. 95 (March 2016) (discussing the laundering of criminal proceeds in China), accessed from http://www.state.gov/documents/organization/253983.pdf. *See also* Financial Action Task Force (FATF), Organization for Economic Cooperation and Development, "*Trade Based Money Laundering*," at p. 1 (June 23, 2006) (discussing three types of money laundering: the use of the financial system, the physical movement of money, and the physical movement of goods), accessed from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/Trade-based-ML_062006.pdf.

[26] *See* Section II.

[27] *See* Financial Action Task Force (FATF), Organization for Economic Cooperation and Development, "*Trade Based Money Laundering,*" at pp. 3-7 (June 23, 2006), accessed from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/Trade-based-ML_062006.pdf.

[28] This Figure is found in Financial Action Task Force (FATF), Organization for Economic Cooperation and Development, "*Trade Based Money Laundering*," at p. 18 ("Case Study 10") (June 23, 2006), accessed from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/Trade-based-ML_062006.pdf.

[29] *See, e.g.*, Kinetz, Erica, *"Chinese banks serve as safe haven for booming counterfeit goods trade,"* The Associated Press (May 7, 2015), accessed from http://www.usnews.com/news/business/articles/2015/05/07/ap-exclusive-chinese-banks-a-haven-for-web-counterfeits; Hong, Nicole *et al.*, "*China's Banks Test U.S. Legal System: Bank of China says turning over account records would violate Chinese law,*" The Wall Street Journal (November 18, 2015), accessed from http://www.wsj.com/articles/chinas-banks-test-u-s-legal-system-1447822800; "*Bank of China fraud: Italy seeks trial for 300 people,*" BBC News (June 21, 2015), accessed from: http://www.bbc.com/news/world-europe-33214450 (prosecutors in Italy allege that more than US $5 billion in proceeds from counterfeiting, prostitution, labor exploitation, and tax evasion was transferred from Italy to China, and that nearly half went through the Bank of China's branch in Milan).

[30] *See* Kinetz, Erica, *"Chinese banks serve as safe haven for booming counterfeit goods trade"* The Associated Press (May 7, 2015) (quoting the President of the International Anti-Counterfeiting Coalition), accessed from http://www.usnews.com/news/business/articles/2015/05/07/ap-exclusive-chinese-banks-a-haven-for-web-counterfeits.

[31] The academic investigation is reported in Simonite, Tom, "*Spam Trail Leads to China's Three Largest Banks,*" MIT Technology Review (January 29, 2016), accessed from https://www.technologyreview.com/s/546311/spam-trail-leads-to-chinas-three-largest-banks/?utm_source=The+Sinocism+China+Newsletter&utm_campaign=3357bb065c-Sinocism02_01_162_1_2016&utm_medium=email&utm_term=0_171f237867-3357bb065c-29652241&mc_cid=3357bb065c&mc_eid=f4df4b6d0d, and in Shahani, Aarti, "*How Major Chinese Banks Help Sell Knock-Offs,*" National Public Radio's *All Things Considered* (February 16, 2016), accessed from http://www.npr.org/sections/alltechconsidered/2016/02/16/466340567/how-major-chinese-banks-help-sell-knock-offs. *See also* Kinetz, Erika *et al.*, "*AP Investigation: How con man used China to launder millions,*" The Associated Press (March 28, 2016), accessed from http://bigstory.ap.org/article/7500da6eb1d94e1dbb7e5650d1c20bd6/ap-investigation-how-con-man-used-china-make-millions (reporting that China is "emerging as an international hub for money laundering," including as part of the counterfeit trade network).

[32] *See, e.g.*, United States Department of State, Bureau for International Narcotics and Law Enforcement Affairs, "*International Narcotics Control Strategy Report, Volume II: Money Laundering and Financial Crimes*," at p. 95 (March 2016), accessed from http://www.state.gov/documents/organization/253983.pdf.

[33] The indictment is discussed in United States Department of Justice, U.S. Attorney's Office for the Eastern District of New York, "*Three Members Of International Organization Of Money Launderers For The Largest Drug Cartels Arrested: Defendants Used Chinese Banking System and Trade-Based Money Laundering Scheme to Launder Over $5 Billion*" (September 10, 2015), accessed from https://www.justice.gov/usao-edny/pr/three-members-international-organization-money-launderers-largest-drug-cartels-arrested.

[34] NTIA, *"Testimony of Assistant Secretary Strickling on Protecting Internet Freedom: Implications of Ending U.S. Oversight of the Internet"* (September 14, 2016), accessed from: https://www.ntia.doc.gov/speechtestimony/2016/testimony-assistant-secretary-strickling-protecting-internet-freedom.

[35] *See, e.g.*, Office of the United States Trade Representative, "*2015 Out-of-Cycle Review of Notorious Markets,*" at p. 14 (December 2015), accessed from https://ustr.gov/sites/default/files/USTR-2015-Out-of-Cycle-Review-Notorious-Markets-Final.pdf (reporting that "domain hopping tactics deployed by KAT. CR allow the site to reappear at the top of search results and evade court-ordered injunctions"); Representatives Goodlatte and Schiff, "*International Creativity and Theft-Prevention Caucus Applauds USTR Report*" (December 28, 2015) ("the challenges of sustained enforcement for online piracy are evident including domain name hopping and the cloning of closed sites"), accessed from http://www.judiciary.house.gov/index.cfm/press-releases?ID=EBEFCCFA-41DB-4862-9194-F157FDFC000B.

[36] RFC 1591, titled "Domain Name System Structure and Delegation," emphasizes the principle of subsidiarity in policy development; the ccTLD manager should, in the first instance, consider the needs and interests of the local community it serves, as a "trustee for the delegated domain" for the Nation.

[37] The "whack-a-mole" challenge is exacerbated at times when individuals or entities engaged in illicit online activities actively obscure their true identity by registering domain names under false information. *See, e.g.*, Europol, "*The Internet Organised Crime Threat Assessment,*" Chapter 4 – Facilitators and Relevant Factors (2014), accessed from https://www.europol.europa.eu/iocta/2014/chap-4-3-view1.html ("Criminals can misuse/abuse WHOIS data in a number of ways" including "[g]iving false WHOIS credentials to Registrars to avoid identification, in order to conduct illegal or harmful Internet activities"); National Physical Laboratory, "*A Study of Whois Privacy and Proxy Service Abuse: Final Report,*" at p. 8 (March 7, 2014) (reporting that a "significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services to obscure the perpetrator's identity"), accessed from https://whois.icann.org/en/file/pp-abuse-study-final-07mar14-en.

[38] "Despite the criminal conviction of its founders, Sweden-based The Pirate Bay (TPB) continued to navigate the globe and the country code top level domain (ccTLD) system to facilitate user downloading of unauthorized copyright-protected content." Office of the United States Trade Representative, "*2013 Out-of-Cycle Review of Notorious Markets,*" at p. 10 (February 12, 2014), accessed from https://ustr.gov/sites/default/files/02122014-2013-OCR-Notorious-Markets.pdf. According to reports, TPB has used over a dozen ccTLDs as part of an attempt to stay beyond the reach of law enforcement, including the ccTLDs for Sweden (.se), Greenland (.gl), Iceland (.is), Saint Martin (.sx), Ascension Island (.ac), Peru (.pe), Guyana (.gy), South Georgia (.gs), Laos (.la), the British Virgin Islands (.vg), Armenia (.am), Mongolia (.mn), Grenada (.gd), and Montserrat (.ms). See USTR's "*2013 Out-of-Cycle Review of Notorious Markets," id.*; Ernesto, "*The Pirate Bay Moves to .AC After Domain Name Seizure*," Torrent Freak (December 10, 2013), accessed from https://torrentfreak.com/the-pirate-bay-moves-to-ac-after-domain-name-seizure-131210/; Ernesto, "*Pirate Bay Moves to Guyana After Domain Suspension, 70 Domains to Go*," Torrent Freak (December 18, 2013), accessed from https://torrentfreak.com/pirate-bay-moves-to-guyana-131218/; Ernesto, "*Pirate Bay Moves to GS, LA, VG, AM, MN, and GD Domains*," Torrent Freak (May 19, 2015), accessed from https://torrentfreak.com/pirate-bay-moves-to-gs-la-vg-am-mn-and-gd-domains-150519/; Ernesto, "*Registry Suspends Pirate Bay's 'New' .MS Domain Name*," Torrent Freak (January 14, 2016), accessed from https://torrentfreak.com/registry-suspends-pirate-bays-new-ms-domain-name-160114/.

[39] *See* Office of the United States Trade Representative, "*2013 Out-of-Cycle Review of Notorious Markets*" (February 12, 2014), accessed from https://ustr.gov/sites/default/files/02122014-2013-OCR-Notorious-Markets.pdf; "*2014 Out-of-Cycle Review of Notorious Markets*" (March 5, 2015), accessed from https://ustr.gov/sites/default/files/2014%20Notorious%20Markets%20List%20-%20Published_0.pdf; "*2015 Out-of-Cycle Review of Notorious Markets*" (December 2015), accessed from https://ustr.gov/sites/default/files/USTR-2015-Out-of-Cycle-Review-Notorious-Markets-Final.pdf.

[40] Office of the United States Trade Representative, "*2015 Out-of-Cycle Review of Notorious Markets*" (December 2015), accessed from https://ustr.gov/sites/default/files/USTR-2015-Out-of-Cycle-Review-Notorious-Markets-Final.pdf.

[41] *See, e.g.*, Verisign, "*The Domain Name Industry Brief*" (Volume 13 – Issue 3: September 2016) (reporting that an estimated 334.6 million domain names are registered across all TLDs, with ccTLDs comprising an estimated 149.9 million domain names), accessed from https://www.verisign.com/assets/domain-name-report-sept2016.pdf.

[42] *See, e.g.*, Sullivan, Danny, "*Google Still Doing At Least 1 Trillion Search Per Year: Company is sticking with figure it gave in 2012 but stresses it's 'over' that amount. How much over, Google's not saying.,*" Search Engine Land, (January 16, 2015), accessed from http://searchengineland.com/google-1-trillion-searches-per-year-212940.

[43] Sterling, Greg, "*Search Is Number One Content Discovery Tool For Mobile Users: Study shows mobile web is widely used despite 'time spent' gap with apps,*" Search Engine Land (January 15, 2015), accessed from http://searchengineland.com/search-leading-content-discovery-tool-mobile-users-212855.

[44] *See, e.g.*, Google Public Policy Blog, "*Continued Progress on Fighting Piracy*" (October 17, 2014), accessed from http://googlepublicpolicy.blogspot.com/2014/10/continued-progress-on-fighting-piracy.html; Microsoft Corporate Blogs, "*An Update on Microsoft's efforts to reduce online piracy and improve search results*" (June 22, 2015), accessed from http://blogs.microsoft.com/on-the-issues/2015/06/22/an-update-on-microsofts-efforts-to-reduce-online-piracy-and-improve-search-results/.

[45] *See, e.g.*, Ernesto, *"Google's Piracy Filter Cuts 'Pirate Bay' Searches in Half, But . . .,"* Torrent Freak (April 20, 2012), accessed from https://torrentfreak.com/googles-piracy-filter-cuts-pirate-bay-searches-in-half-but-120420/.

[46] Microsoft Corporate Blogs, "*An Update on Microsoft's efforts to reduce online piracy and improve search results*" (June 22, 2015), accessed from http://blogs.microsoft.com/on-the-

issues/2015/06/22/an-update-on-microsofts-efforts-to-reduce-online-piracy-and-improve-search-results/.

[47] *See* Ernesto, "*Google's Anti-Piracy Filter Is Quite Effective,*" Torrent Freak (July 12, 2011), accessed from https://torrentfreak.com/googles-anti-piracy-filter-110712/; Ernesto, "*Google's Piracy Filter Cuts 'Pirate Bay' Searches in Half, But . . .,*" Torrent Freak (April 20, 2012), accessed from https://torrentfreak.com/googles-piracy-filter-cuts-pirate-bay-searches-in-half-but-120420/.

[48] The "safe harbor" provisions of the Digital Millennium Copyright Act (DMCA), originally enacted in 1998 in Pub. L. No. 105-304 (and since amended), are codified at 17 U.S.C. § 512.

[49] United States Department of Commerce, Internet Policy Task Force, "*Copyright Policy, Creativity, and Innovation in the Digital Economy,*" (July 2013) at p.56, accessed from http://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf.

[50] United States Department of Commerce, Internet Policy Task Force, "*Copyright Policy, Creativity, and Innovation in the Digital Economy,*" (July 2013) at p.56, accessed from http://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf, *citing* Stewart, Christopher S., Wall Street Journal (March 4, 2013) (reporting that owner of small independent film distributor "found more than 903,000 links to unauthorized versions of her films" with estimated losses of "over $3 million in revenue" and a cost to send takedown notices of "over $30,000 a year.").

[51] *See* Welch, Chris, "*Google received over 75 million copyright takedown requests in February: The company is processing over 100,000 links each and every hour,*" (The Verge: March 7, 2016), accessed from http://www.theverge.com/2016/3/7/11172516/google-takedown-requests-75-million. *See also* "*Requests to remove content due to copyright,*" Google Transparency Report, accessed from https://www.google.com/transparencyreport/removals/copyright/.

[52] Accessed via Google, *Transparency Report*, accessed from https://www.google.com/transparencyreport/removals/copyright/.

[53] *See, e.g.*, Urban, Jennifer M. *et al.*, "*Notice and Takedown in Everyday Practice*" UC Berkeley Public Law Research Paper No. 2755628 (March 29, 2016) at pp.116-117, accessed from http://ssrn.com/abstract=2755628.

[54] United States Department of Commerce, DMCA Multistakeholder Forum, "*DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices*" (April 7, 2015), accessed from https://www.uspto.gov/sites/default/files/documents/DMCA_Good_Bad_and_Situational_Practices_Document-FINAL.pdf.

[55] *See* United States Copyright Office, "*Section 512 Study: Notice and Request for Public Comment,*" 80 FR 81862 (December 31, 2015), accessed from https://www.gpo.gov/fdsys/pkg/FR-2015-12-31/pdf/2015-32973.pdf.

[56] Forster, Stephen, "*Crackdown on counterfeiting & piracy online,*" U.K. National Trading Standards, eCrime Team (June 24, 2015) ("according to the latest IP Crime Report 2013/14, social media has overtaken auction sites as criminals' 'channel-of-choice' for counterfeit and piracy activity"), accessed from http://www.tradingstandardsecrime.org.uk/crack-down-on-counterfeiting-and-piracy-on-social-media/.

[57] *See* U.K. Intellectual Property Office, "*IP Crime Report 2015/16,*" (September 28, 2016), at pp.7, 15, 29, accessed from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557539/ip-crime-report-2015-16.pdf; National Trading Standards, "*Social Media Counterfeting Operation,*" (July 5, 2016), accessed from http://www.tradingstandardsecrime.org.uk/social-media-counterfeiting-operation-expands-across-borders/; Chu, Kathy, "*For Counterfeit Fighters on Social Media, Fake Profiles are a Real Ally,*" (The Wall Street Journal: April 25, 2016), accessed from http://www.wsj.com/articles/for-counterfeit-fighters-on-social-media-fake-profiles-are-a-real-ally-1461578495.

[58] Regarding the general increase in the use of "buy buttons" for legitimate commerce, *see, e.g.*, Boorstin, Julia, "*Twitter launches 'buy now' buttons for retailers,*" CNBC (September 30, 2015), accessed from http://www.cnbc.com/2015/09/30/twitter-launches-buy-now-buttons-for-retailers.html; Honig, Zach, "*Facebook's Buy button lets you purchase products directly from Page posts and ads,*" EnGadget.com (July 18, 2014), accessed from http://www.engadget.com/2014/07/18/facebook-testing-buy-button/; Griffith, Erin, "*Pinterest expands 'buy button' program to boost shopping on platform,*" Fortune (October 5, 2015), accessed from http://fortune.com/2015/10/05/pinterest-buy-button-expansion/.

[59] D'Onfro, Jillian, BusinessInsider.com, "*Here's a look at just how big a problem 'freebooting' is for Facebook*" (August 3, 2015), accessed from http://www.businessinsider.com/freebooting-video-on-facebook-2015-8; O'Rieilly, Lara, "*A YouTube video that claims Facebook is 'stealing billions of views' is going viral,*" BusinessInsider.com (November 12, 2015), accessed from http://www.businessinsider.com/how-facebook-is-stealing-billions-of-views-youtube-video-goes-viral-2015-11; Luckerson, Victor, "*This is Facebook's Biggest Problem With Video Right Now,*" Time (August 25, 2015), accessed from http://time.com/4009015/facebook-youtube-freebooting/.

[60] *See, e.g.*, Griffith, Erin, "*Facebook's video monetization plan is here,*" Fortune (July 1, 2015) (describing social media platforms' collection of ad revenue from uploaded content alongside discussion of identical content viewed 23 million times from an unauthorized source and only 2 million times from the content creator), accessed from http://fortune.com/2015/07/01/facebook-video-monetization/.

[61] International Data Corporation (IDC), "*Mobile Internet Users to Top 2 Billion Worldwide in 2016, According to IDC*" (Dec. 17, 2015), accessed from http://www.idc.com/getdoc.jsp?containerId=prUS40855515.

[62] Khalaf, Simon, "*Media, Productivity & Emojis Give Mobile Another Stunning Growth Year,*" Flurry Analytics Blog (Jan. 5, 2016), accessed from http://flurrymobile.tumblr.com/post/136677391508/stateofmobile2015?soc_src=mail&soc_trk=ma.

[63] This Figure found in "*Global mobile applications user base from 2010 to 2015 (in millions),*" Statista, accessed from http://www.statista.com/statistics/219959/global-mobile-applications-user-base-forecast/.

[64] Figure sourced from Statista, https://www.statista.com/statistics/219959/global-mobile-applications-user-base-forecast/.

[65] Mathew, Jerin, "*Apple App Store Growing by Over 1,000 Apps Per Day,*" International Business Times (June 6, 2015)

("Developers are currently submitting more than 1,000 apps to Apple's App Store per day, according to data compiled by Pocketgamer.biz."), accessed from http://www.ibtimes.co.uk/apple-app-store-growing-by-over-1000-apps-per-day-1504801.

[66] Norton, "*How to Spot a Fake Android App*" (August 18, 2014), accessed from http://community.norton.com/en/blogs/norton-protection-blog/how-spot-fake-android-appjp.

[67] *See, e.g.*, Casey, Dan, "*Column: Web Entrepreneur cries foul over purloined content,*" The Roanoke Times, (November 30, 2015), accessed from http://www.roanoke.com/news/columns_and_blogs/columns/dan_casey/column-web-entrepreneur-cries-foul-over-purloined-content/article_f0d7b0a7-0438-5fd2-81b1-3383c7c5d514.html.

[68] *See, e.g.*, Statt, Nick, "*Microsoft's Windows app stores still 'cesspool' of copyright infringement*," CNET, (May 22, 2015), accessed from http://www.cnet.com/news/microsoft-windows-app-stores-copyright-infringement/#.

[69] *See, e.g.*, Gross, Doug, "*Virus found in fake Android version of 'Angry Birds: Space'*," CNN (April 12, 2012), accessed from http://www.cnn.com/2012/04/12/tech/gaming-gadgets/angry-birds-virus-android/; Arthur, Charles, "*Android users targeted in Angry Birds malware scam,*" The Guardian (May 25, 2012), accessed from https://www.theguardian.com/technology/2012/may/25/android-users-angry-birds-malware (reporting that "[n]early 1,400 UK Android smartphone users have been hit by premium-rate phone scams . . . when they opened fake versions of game apps including Angry Birds, Assassin's Creed and Cut the Rope").

[70] Luo, Symphony *et al.*, "*Fake Apps: Feigning Legitimacy,*" Trend Micro Research Paper, (2014), accessed from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fake-apps.pdf. The quote regarding SDK modification is on page 7.

[71] This Figure is found in Asrar, Irfan, "*Will Your Next TV Manual Ask You to Run a Scan Instead of Adjusting the Antenna?,*" Symantec Official Blog (October 12, 2011), accessed from https://www.symantec.com/connect/blogs/will-your-next-tv-manual-ask-you-run-scan-instead-adjusting-antenna, and is also cited in Mills, Elinor, "*Phony Netflix Android app steals account data: Malicious app looks like real Netflix app but grabs log-in data, says Symantec,*" CNET (October 12, 2011), accessed from http://www.cnet.com/news/phony-netflix-android-app-steals-account-data/, and in Kovacs, Nadia, "*How to Spot a Fake Android App,*" Norton (August 18, 2014), accessed from http://community.norton.com/en/blogs/norton-protection-blog/how-spot-fake-android-appjp.

[72] *See, e.g.*, "*App Store Review Guidelines,*" Apple, accessed from https://developer.apple.com/app-store/review/guidelines. Section 5 of the Guidelines establishes the framework around which Apple will review submitted apps for compliance with applicable law.

[73] For example, in December 2014, Google removed from its Play Store several infringing applications associated with the notorious Pirate Bay website. However, the apps remained available elsewhere, and the apps downloaded prior to the takedown continued to function (but without updates). *See* de Looper, Christian, "*Google Pulls Pirate Bay Apps Citing Piracy Concerns,*" Tech Times (December 8, 2014), accessed from http://www.techtimes.com/articles/21765/20141208/google-pulls-pirate-bay-apps-citing-piracy-concerns.htm.

[74] Announcing the launch of the Digital Attache Program, United States Secretary of Commerce, Penny Pritzker, stated that, "America's economic growth and competitiveness depend on our capacity to embrace digitization in the economy." "*U.S. Secretary of Commerce Penny Pritzker Launches Digital Attache Program to Address Trade Barriers*" (March 11, 2016), accessed from https://www.commerce.gov/news/press-releases/2016/03/us-secretary-commerce-penny-pritzker-launches-digital-attache-program.

[75] *See, e.g.*, Talbot, David, "*Google, Sun Backing New Anti-Malware Efforts: Harvard, Oxford researchers aim to create Internet defensive strategies geared to consumers,*" MIT Technology Review (January 25, 2006), accessed from https://www.technologyreview.com/s/405213/google-sun-backing-new-anti-malware-effort/.

[76] "*Bing to warn customers about the threats of fake online pharmacies,*" Bing blogs (August 6, 2015), accessed from https://blogs.bing.com/search/2015/08/06/bing-to-warn-customers-about-the-threats-of-fake-online-pharmacies/.

[77] *See, e.g.*, "*2013 Joint Strategic Plan on Intellectual Property Enforcment,*" at p. 7, accessed from https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

[78] *See, e.g.*, Minaya, Ezequiel *et al.*,"*Netflix Expands to 190 Countries,*" The Wall Street Journal (January 6, 2016), accessed from http://www.wsj.com/articles/netflix-expands-to-190-countries-1452106429.

[79] The Figure is of the Popcorn Time app, which courts have held to infringe copyright and have no legitimate purpose. *See Twentieth Century Fox Film Corp. et al. v. Sky UK Ltd. Et al.*, [2015] EWHC 1082 (Ch), accessed from *http://www.bailii.org/ew/cases/EWHC/Ch/2015/1082.html* (holding in paragraph 66 that "[t]he point of Popcorn Time is to infringe copyright. The Popcorn Time application has no legitimate purpose"; injunction ordered). Similar court ruling have been reported in Canada and New Zealand. *See* Ungerleider, Neal, "*MPAA Shuts Down Torrent Site Popcorn Time: Court rulings in Canada and New Zealand bring down Popcorn Time and fellow pirate site YTS.*," FastCompany (November 4, 2015), http://www.fastcompany.com/3053227/fast-feed/mpaa-shuts-down-torrent-site-popcorn-time.

[80] *See, e.g.*, U.S. Department of Commerce, Census Bureau, *"Quarterly Retail E-Commerce Sales, 2nd Quarter 2016"* (August 16, 2016), accessed from http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf. *See also* eMarketer, *"Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year"* (August 22, 2016), accessed from https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369 (citing proprietary eMarketer estimates that "Double-digit growth [in e-commerce] will continue through 2020, when sales will top $4 trillion").

[81] *See, e.g.*, Federal Bureau of Investigation, "*Countering the Growing Intellectual Property Theft Threat: Enhancing Ties Between Law Enforcement and Business*" (January 22, 2016), accessed from https://www.fbi.gov/news/stories/2016/january/countering-the-growing-intellectual-property-theft-threat/countering-the-growing-intellectual-property-theft-threat.

[82] MarkMonitor, "*MarkMonitor Online Barometer and Global Consumer Shopping Habits Survey 2015*" (November 2015), at p. 4, accessed from https://www.markmonitor.com/download/report/MarkMonitor_Online_Barometer-2015.pdf.

[83] *See, e.g.*, Carsten, Paul, "*Alibaba's Singles' Day sales surge 60 percent to $14.3 billion,*" Reuters (November 11, 2015), accessed from http://www.reuters.com/article/us-alibaba-

singles-day-idUSKCN0SZ34J20151112.

[84] *See, e.g.,* IBM Global Business Services, "*The New Software-Defined Supply Chain: Preparing for the Disruptive Transformation of Electronics Design and Manufacturing*" (2013), p. 1, accessed from: http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03571usen/GBE03571USEN.PDF.

[85] *See, e.g.,* U.S. Government Accountability Office (GAO), "GAO-15-505SP: *3D Printing: Opportunities, Challenges, and Policy Implications of Additive Manufacturing,"* (June 2015), accessed from http://www.gao.gov/assets/680/670960.pdf.

[86] *See, e.g.,* IBM Global Business Services, "*The New Software-Defined Supply Chain: Preparing for the Disruptive Transformation of Electronics Design and Manufacturing*" (2013), accessed from: http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03571usen/GBE03571USEN.PDF.

[87] *See, e.g.,* U.S. Government Accountability Office (GAO), Report to the Chairman, Committee on Science, Space, and Technology, House of Representatives, *"3D Printing: Opportunities, Challenges, and Policy Implications of Additive Manufacturing"* (June 2015) (GAO-15-505SP), pp. 39-41, accessed from: http://www.gao.gov/assets/680/670960.pdf.

[88] *See, e.g.,* U.S. Government Accountability Office (GAO), Report to the Chairman, Committee on Science, Space, and Technology, House of Representatives, *"3D Printing: Opportunities, Challenges, and Policy Implications of Additive Manufacturing"* (June 2015) (GAO-15-505SP), pp. 40-41, accessed from: http://www.gao.gov/assets/680/670960.pdf.

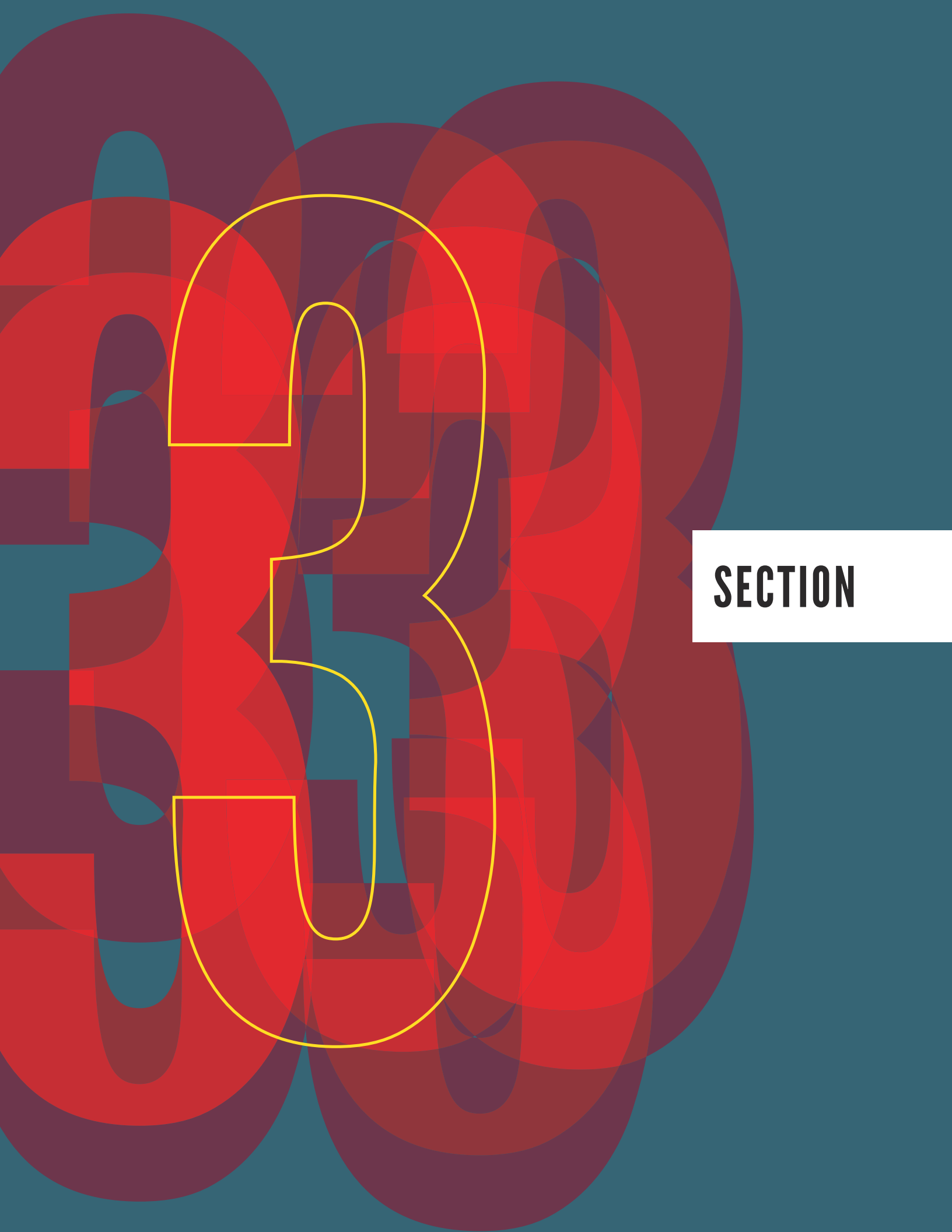
[89] On June 28, 2016, the U.S Patent and Trademark Office hosted a public conference to examine the legal and policy considerations of intellectual property (IP) in 3D printing. See USPTO, "USPTO IP and 3D Printing Conference" (June 28, 2016), accessed from: https://www.uspto.gov/learning-and-resources/ip-policy/uspto-ip-and-3d-printing-conference.

[90] Executive Order 13694 (April 01, 2015).

[91] Executive Office of the President, "*Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*," (February 2013) at pp.1-2.

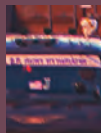
[92] *See* The White House, "*Fact Sheet: Cybersecurity National Action Plan*" (February 6, 2016), accessed from https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

THIS PAGE IS INTENTIONALLY LEFT BLANK


SECTION

SECURE AND FACILITATE LEGITIMATE CROSS-BORDER TRADE





SECTION 3 CONTENTS

SECURE AND FACILITATE LEGITIMATE CROSS-BORDER TRADE

A. Safeguarding our Borders: Enhancing Identification and Interdiction of Counterfeit and Pirated Goods Bound for the U.S. Market 93

1. Employ an "All-Threats" Approach to Cargo Screening 94
2. Combat the Domestic Assembly and Finishing of Counterfeit Goods 94
3. Address the Surge of Small Parcels in the Express Consignment and International Mail Environments 96
4. Implement Advance Targeting Capabilities in the International Mail Environment to Address Rising Threats in the Global Marketplace 99
5. Assess Scope of, and Respond to, Importer Identity Theft in the Trade Environment 100
6. Enhance Customs Recordation Systems and Public-Private Collaboration on Information Collection 101
7. Invest in Anti-Counterfeiting Technology 102
8. Enhance Interdiction Through Specialized Task Forces 104
9. Enhance Fines, Penalties, and Forfeiture Processes and Practices 104
10. Improve Administration of ITC Exclusion Orders 105
11. Expand and Enhance the Use of Post-Entry Audits 106

B. Working Globally: Efforts to Curb the Movement and Trade of Counterfeit and Pirated Goods Around the World 106

1. Promote Necessary Seizure Authority and Best Practices Around the World 107
2. Curb Illegal Operations Within Free Trade Zones 109
3. Support Modern Recordation Systems in Developing Countries 110
4. Tackle the Growing Costs Associated with the Storage and Destruction of Counterfeit Goods 111
5. Dispose of Infringing Goods in an Environmentally-Friendly Manner 112



INTRODUCTION

U.S. and international authorities face a significant challenge in facilitating legitimate trade and travel, while at the same time identifying and preventing infringing and unsafe merchandise from entering into the stream of commerce. As discussed in Section 1, the sophisticated networks that move counterfeit and pirated products through international channels undermine the rule of law, and their actions bring about substantial health, security, and economic ramifications that extend well beyond any single shipment. As a result, counterfeit and pirated products must not be regarded as simply a secondary enforcement concern. Each country should assess and reaffirm its commitment to the fight against illicit trade as a primary concern, while seeking to develop, update, and implement robust national policies that reflect this priority.

This Section focuses on domestic efforts to enhance the Nation's ability to identify and interdict illicit trade in the form of counterfeit and pirated products bound for the U.S. market (see subsection "A"). It also details international opportunities to improve global capacity and frameworks to curb illicit activities where they occur and address some of the effects of illicit trade (see subsection "B"). Collaborative efforts among domestic and international stakeholders are necessary to maintain pace with the deceptive tactics used to exploit shipping channels and methods. Law enforcement and industry stakeholders must work in partnership to develop and advance innovative strategies to stem the flow of money to criminal networks profiting from infringing IP activities.

A. SAFEGUARDING OUR BORDERS: ENHANCING IDENTIFICATION AND INTERDICTION OF COUNTERFEIT AND PIRATED GOODS BOUND FOR THE U.S. MARKET.

Each year, more than 11 million containers arrive at U.S. seaports, another 13 million shipments arrive by truck and rail at our Nation's land borders, and an additional quarter billion cargo, postal, and express consignment packages arrive by plane.[1] CBP officers have to make admissibility determinations on this staggering volume of incoming goods, and enforce nearly 500 U.S. trade laws and regulations on behalf of 47 Federal agencies at America's 328 ports of entry (POEs).[2]

Effectively policing a continuous high-volume of shipments requires a well-developed, layered risk management approach that includes enhanced identification efforts prior to arrival and augmented authentication and interdiction techniques at the POE, followed by tailored investigative procedures designed to protect rights holders' IP, the health and safety of consumers, and other important national interests. Enhanced coordination between agencies at various levels of government, both foreign and domestic, as well as public-private collaboration and data-sharing, are also essential elements of an effective enforcement agenda, and are discussed in Section IV of the Strategic Plan.

1.Employ an "All-Threats" Approach to Cargo Screening.

Intellectual Property enforcement is often regarded as a trade matter and not as a national security threat for cargo screening purposes. While trade concerns are indeed materially present in the importation of counterfeit goods, the failure to regard such goods as also posing a security threat undermines enforcement efforts in a number of ways.

Security initiatives such as the Container Security Initiative (CSI) and the Importer Security Filing (ISF) and Additional Carrier Requirements, often referred to as "10+2," employ a "single-threat" approach to cargo screening. This means that a single threat is the focus of the search, and any other actual or potential threats discovered in the course of the search for that threat may go unreported when discovered.

CSI, for example, is an initiative where CBP officers abroad work with host customs administrations to identify maritime containers used to deliver weapons illicitly. CSI results in prescreening of over 80 percent of all maritime containerized cargo bound for U.S. ports. The ISF initiative, on the other hand, requires carriers of cargo to transmit electronically data about shipments prior to lading, allowing CBP to target containers that pose an elevated risk of transporting illicit weapons. In both cases, CBP officers are bound by established arrangements and regulations, and may be unable to act upon any additional illicit IPR intelligence that is identified in the process of screening the cargo. As a result, dangerous counterfeits that pose serious risks to U.S. health, safety, and national security may be identified by CBP officers but, because they are subject to the arrangements governing CSI and ISF, the contents may not be acted upon without being subject to additional screening or confiscation by CBP personnel.

An "all-threats" approach to cargo screening would reflect the reality, discussed in detail in Section I of this Plan, that trade in counterfeit and pirated goods increasingly presents a clear threat to national security by undermining legitimate markets, financing transnational criminal organizations, endangering the health and safety of consumers, exploiting labor, and harming the environment. Shifting from the current "single-threat" approach to an "all-threats" approach to cargo screening would present opportunities to increase the efficiency and effectiveness of CBP screening operations. It would reduce screening redundancies. This would also empower CBP officers to act upon any relevant intelligence gathered in the course of a permissible cargo screening to further screen, exclude, or seize cargo, as appropriate, under the full spectrum of U.S. law.

ACTION NO. 3.1: Consider opportunities to utilize an "all-threats" approach in cargo screening programs. CBP will assess opportunities for existing cargo screening programs, including CSI and ISF, to evaluate a shipment concurrently for threats to national security, IPR violations, and other issues as appropriate.

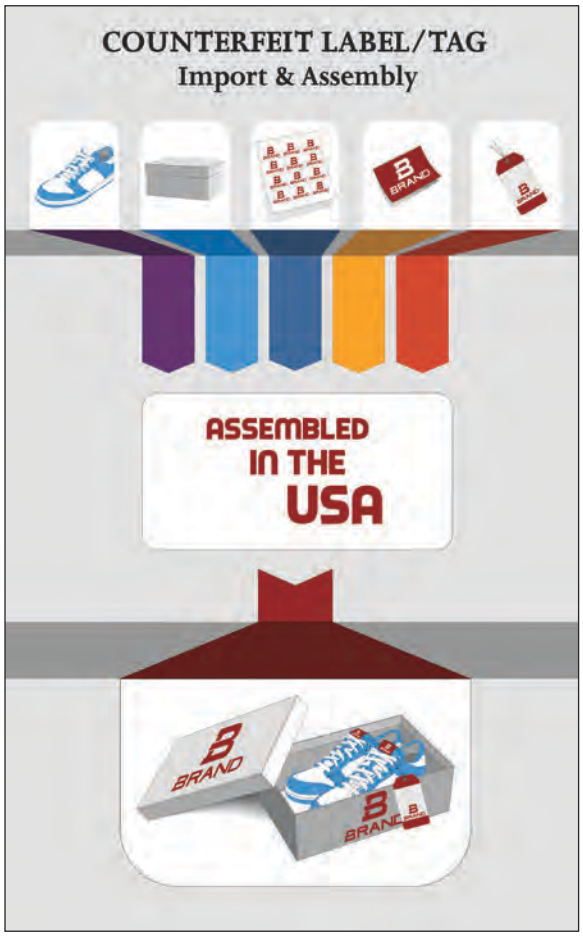
2. Combat the Domestic Assembly and Finishing of Counterfeit Goods.

When law enforcement entities take action against certain illicit methods and tactics, criminals tend to migrate to and exploit other methods. In part, this reflects that more aggressive policy actions and enforcement measures increase the risk of detection and seizure, raising the counterfeiter's costs. Put differently, the illicit trader is continually conducting both a risk and cost-benefit analysis to determine the best course of action to evade detection and maximize profits.

As a result of rising seizures at U.S. POE and other factors, law enforcement is reporting an increase in "domestic production and assembly" of counterfeit products, that is, the practice of shipping unbranded

items into the United States, to which domestic workers then affix branded labels, hangtags, logos, stamps, hardware, embroidery, or other identifying details (collectively referred to as "labels and tags") to the finished counterfeit product.

FIG. 47: Illustration of Domestic Assembly and Finishing Operation: Individual Components Come in, Counterfeit Products Goes Out.



Source: U.S. Customs and Border Protection

Domestic assembly is a common tactic to try to circumvent Customs interdiction.[3] As illustrated above (FIG 47), a common practice is to reduce a product to its smallest form—blank or unbranded products in one or more packages, with identifying labels, hang tags, and packaging in other packages—with the parts imported independently in the hope that, separately, each of the individual components may clear Customs. If Customs seizes one shipment, it may likely be the one of least monetary value: the un-affixed labels featuring the famous brand. Should that occur, the illicit trader will merely send a second parcel (filled with labels) to replace the first, and the game of cat-and-mouse continues.

Between FY 2012 and FY 2015, DHS seized over 2,500 shipments containing millions of individual labels and tags intended for domestic finishing, with an affixed value of more than $115 million, had the finished goods been genuine. The dollar value of seized labels and tags increased by 46.9 percent in FY 2015 over FY 2014, and 37 percent in FY 2013 over FY 2012.[4] Domestic assembly is reportedly a widespread practice across different parts of the world.[5]

These tactics merit further attention and a comprehensive assessment, as little information is publicly available. Moving forward, it is important to evaluate the impact of seizures on the illicit domestic production industry, including resulting disruptions to criminal networks and an overall assessment of the effectiveness of law enforcement programs. Relatedly, the Federal Government can optimize its response to illicit domestic finishing through an evaluation of the scope and nature of domestic criminal production and finishing operations.

ACTION NO. 3.2: Identify and evaluate trends in domestic production and finishing operations for counterfeit goods. Within 18 months of the issuance of this Plan, ICE will identify and evaluate trends in domestic production and finishing operations.

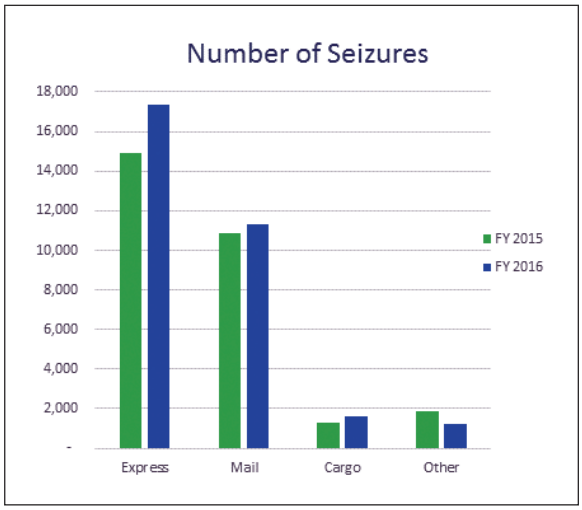
ACTION NO. 3.3: Enhance interdiction efforts and the identification, investigation, and prosecution of illicit domestic finishing operations. Based on its identification and evaluation of trends in domestic production and finishing operations, ICE will work, as appropriate, with CBP and other Federal, State, and local law enforcement partners to enhance interdiction efforts and other activities for combating such operations. This may include identifying opportunities for increased collaboration with and among Federal, State and local law enforcement entities–to further the identification, investigation, and prosecution of illicit domestic finishing operations.

3. Address the Surge of Small Parcels in the Express Consignment and International Mail Environments.

Economic globalization, especially with the fast growing e-commerce sector, is creating increases in supply and demand while simultaneously accelerating the flow of capital and goods around the world. These same forces put a strain on international mail and express shipments, collectively referred to as "small parcels," as they are becoming increasingly exploited to commit fraud and illicit activity. In fact, as of 2015, the express environment now accounts for over half of all U.S. IPR-related seizures.[6]

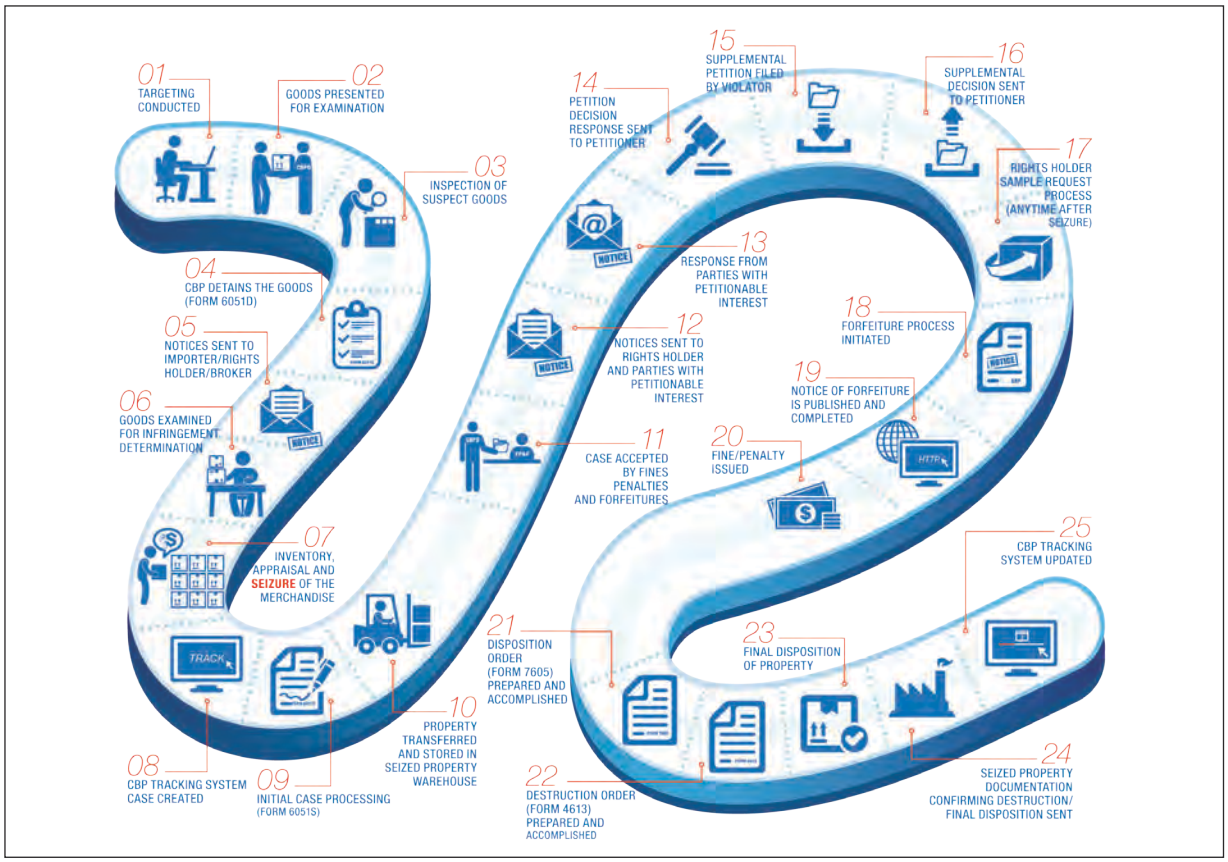
The large and growing number of small parcels moving daily through international mail and express facilities present challenges to law enforcement in the fight against counterfeiting and piracy. These high-volume, often low-value, shipments place a tremendous burden on CBP resources, potentially impacting the agency's ability to intercept additional or higher-value shipments. Although express consignment shipments generally contain a smaller piece count with a lower value than containerized cargo, they nonetheless are subject at this time to the same seizure and forfeiture procedures as larger cargo shipments.

FIG. 48: IPR-Violative Shipments Seized by Mode of Transportation.[7]



Source: Department of Homeland Security, CBP

FIG. 49: CBP's Existing 25-Point IPR Seizure Process.[8]



With each small parcel seizure costing the U.S. Government hundreds of dollars, improved or alternative methods of interdiction are critical to efficient customs processes.[9]

A number of different methods may identify improvements to interdiction practices. However, it may be helpful to consider process optimization in the small parcel environments as involving the interplay of at least the following three areas of focus: (i) a strategy to identify opportunities to improve day-to-day operational efficiencies; (ii) an institutional commitment to pursuing operational innovation; and (iii) the adoption of advanced technological solutions and the application of computer science techniques to leverage insights and trends from "big data." The importance of advanced technological solutions compels that we treat it as a stand-alone third prong so that it may be fully developed in a strategic manner. However, it is acknowledged that these technology-based solutions must be fully integrated in both operational models.

General improvements in "operational efficiency"—also referred to as "operational excellence"—should not be confused with "operational innovation."

Operational innovation facilitates entirely new ways of carrying out activities that an entity performs. Operational efficiency, on the other hand, utilizes existing modes of operation to achieve higher performance but without fundamentally changing how that work gets accomplished.

See Michael Hammer, Michael, "Deep Change: How Operational Innovation Can Transform Your Company," Harvard Business Review, (April 2004).

Operational Efficiency.

There exist opportunities to pursue enhanced operational efficiencies to significantly streamline Custom's lengthy and time-consuming seizure process (FIG 49). To reflect the shift in international shipping from ocean shipping containers to small parcels, many of the authorities currently in place must be reviewed to determine how they may be dynamically applied to current and anticipated shipping practices.

Interdiction and seizure procedures should be continually assessed in order to identify and eliminate inefficiencies on a timely basis. The express consignment and international mail environments are not static and, as a result, processes should be reviewed periodically to avoid outdated procedures that could result in productivity gaps. Accordingly, an opportunity exists for CBP to engage in an agency-wide strategy setting exercise to examine routine processes and procedures, and identify opportunities to simplify each segment within the interdiction and seizure framework, including with assistance of advanced technological solutions to minimize "frontline" parcel touch-points and "back office" administrative processing. To the extent that solutions may not be fully implemented due to perceived limitations and obstacles—including, for example, the need for legislative or regulatory reform—those constraints may be shared with the IPEC for further consideration.

Additionally, CBP, in consultation with the Office of Management and Budget (OMB), IPEC, and other interested Federal agencies, must also consider whether CBP staffing levels and user fees for customs inspection services are sufficient to meet the demands of current and anticipated shipping trends and risk analysis. Staffing and user fee funding appropriately aligned with current shipping trends and risk determinations would help prevent illicit goods from entering the marketplace and enable stakeholders to optimally align deterrence efforts.

Operational Innovation.

As a result of the dynamic shift to small parcels as a favored method to move illicit merchandise, customs authorities (domestically and internationally) must rethink critical dimensions of the work performed, and assess all opportunities to implement innovative new ways of carrying out their respective mandates.

As one example of operational innovation, in FY 2015, CBP began exploring an alternative to the traditional, full seizure process in an effort to prevent more small parcels with counterfeit and piratical merchandise from entering the United States. Specifically, CBP collaborated with its express consignment industry partners to develop a simplified IPR enforcement process in the express consignment environment through which CBP would offer the importer and the U.S. consignee an option to voluntarily abandon a shipment suspected of containing counterfeit or pirated goods.[10]

As successful as CBP's pilot program proved to be at preventing illicit goods from entering the stream of commerce, it must be seen as only one avenue for addressing this large and growing challenge. Further refinements are necessary.[11] Specifically, additional mechanisms are needed to enable private stakeholders (whose rights are implicated by the abandoned parcels) to be in a position to conduct their own investigations and initiate civil actions and criminal referrals to law enforcement authorities as part of a comprehensive strategy to address the proliferation of illicit commerce in small parcel shipments.[12]

Technological (Targeting) Solutions.

CBP must integrate technological advances in all processes as part of the improvements to operational models and strategies, at each step along the way from targeting to interdiction to product disposition. High-volume transaction environments must include state-of-the-art workflow systems and fully leverage technological solutions, as well as extract "big data" for analytics and trend recognition.

In this context, collected data should be used as a basis to introduce enhanced targeting, prediction, and decisional processes, and should be shared, as appropriate by CBP, with affected stakeholders to elevate private and public sector competencies. Information must not remain buried in detailed or unstructured data logs (generally referred to as a "data lake"), but rather modern computer science techniques should be employed to leverage and extract insights and trends from available data. Reports from available data should not be of a static or generic nature, focused almost exclusively on high-level data points such as country of origin, number of seizures (and corresponding value), and product category.

Additional research into trends at each POE, by product category, sector, and brand—including analysis of the corresponding country of origin, transshipment routes, evasive tactics employed, repeat offenders, and other illicit characteristics (e.g., such as identification of intermediary drop shippers or domestic finishers)—would provide law enforcement and other appropriate stakeholders a more complete picture of the state of anti-counterfeiting measures, and identify opportunities for further improvements. See the "Call for Research" at the conclusion of Section IV of this Strategic Plan for additional discussion.

ACTION NO. 3.4: Identify operational best practices in IP enforcement for express shipping operations. In order to build expertise and increase efficiency at all express locations, CBP will study, identify, and report on best operational practices in IP enforcement among existing express operations. CBP will also assess all opportunities to streamline processes and procedures, including by the adoption of advanced technological solutions, to effect seizures and forfeitures in the small parcel environment.

ACTION NO. 3.5: Assess the voluntary abandonment pilot program. CBP—along with the Commercial Customs Operations Advisory Committee (COAC), and in consultation with representatives of small and medium enterprises (SMEs) and IPEC—will evaluate the IPR voluntary abandonment pilot program's performance, with a particular focus on whether the program has demonstrated the capacity to reduce the resources required for administrative actions; effectively identify and exclude from the program repeat offenders and importers of potentially hazardous goods; enable appropriate post-abandonment civil investigations by rights holders; and not diminish law enforcement's ability to investigate and prosecute offenders as may be warranted under the circumstances. CBP should consider whether, subject to legal and administrative limitations, the release of standard data (name and address of manufacturer, exporter, and importer) to interested parties would result in material improvements to small shipment seizure and forfeiture proceedings.

ACTION NO. 3.6: Support access to data on patterns and trends. Strong, responsive public policy and proactive business measures to prevent IPR violations depend on high-quality data on current patterns and trends in illicit trade. CBP possesses information on supply chains and can identify patterns from its vast stock of movement data that can lead to actionable intelligence, both for criminal investigators as well as private sector, civil-based investigations. Within two years of the issuance of this Plan, CBP will identify opportunities to make non-public agency data more readily available to Federal partners and to the private sector where such release would be permissible

under current law and would not compromise sensitive law enforcement operations.

ACTION NO. 3.7: Review the suitability of current CBP user fee allocations. CBP and the Department of the Treasury, in consultation with OMB, will evaluate whether the allocation of user fees under 19 U.S.C. § 58c appropriately reflects CBP's current program requirements and costs, particularly with respect to small shipments. If the agencies determine that allocations under current law are insufficient or outdated, they will further evaluate options for adjusting the amounts, hierarchy, and allocation of funds to meet full cost recovery and maximize CBP program effectiveness. In addition, the agencies will examine the need for and viability of supplementary fees to complement the express consignment carrier and centralized hub facilities user fee commitments.

4. Implement Advance Targeting Capabilities in the International Mail Environment to Address Rising Threats in the Global Marketplace.

CBP receives advance data for packages sent via express consignment, but not for international mail parcels destined for the United States. This lack of advance targeting information, combined with the rapid flow of parcels, limits CBP's ability to properly identify international mail shipments that may contain counterfeit or pirated goods. Without the ability to conduct a full-risk analysis on shipments arriving through international mail in advance of their arrival, any U.S. border enforcement strategy is incomplete and subject to an unacceptable degree of risk.

While CBP has been working with the United States Postal Service (USPS) and the Universal Postal Union to address this risk through an advance data screening pilot program for some time, progress has been slow. Without a permanent advance targeting data program, law enforcement will continue to have significant difficulty excluding prohibited IPR items shipped through international mail.

If nations are serious in their resolve to address the growing risk of illicit trade in counterfeit goods—goods that place the health and safety of consumers at risk; jeopardize national security interests; undermine the rule of law; accrue to the benefit of criminal syndicates; and implicate serious ethical and social concerns—the time for action is now.

A combination of advanced data collection at the time of parcel drop-off or payment, coupled with photo-scanning technology of sender and recipient (consignee) information and adoption of barcoded labels (combining all mailing information, from package weight and size, to point of drop-off/pick-up, to delivery destination), must be considered. These and other data collection and parcel tracking methods have long existed, and have been successfully implemented in the express freight sector, leaving little explanation as to why modern systems have yet to be similarly adopted in the international postal environment. While available resources are understandably limited, a strategy must be put into place to move forward.

ACTION NO. 3.8: Evaluate the effectiveness of the CBP-USPS advance data pilot program. Within one year of the issuance of this Plan, CBP will, in coordination with USPS, evaluate the effectiveness of the advance data pilot for international mail. This program evaluation should discuss the systemic vulnerabilities that make advance international mail data critical to effective border enforcement; analyze the quality and timeliness of the data received, including to what extent actionable intelligence was received and used for targeting shipments; examine whether the advance data pilot effectively improved CBP's small-parcel interdiction efforts; and make recommendations for extending or expanding the pilot, including any recommended system modifications at CBP or USPS.

ACTION NO. 3.9: Study exploitation of the international mail environment by perpetrators of illicit trade. DHS, in consultation with USPS, IPEC, and relevant stakeholders, will study to what extent the international mail environment is being misused to conduct illicit trade. Specifically, DHS should seek to identify how and why foreign IP violators are using small mail parcels to ship their counterfeit goods directly to the U.S. consumers. If DHS finds that international mail is being exploited as a significant channel for the conduct of illicit trade, the agency will convene an interagency working group to meet quarterly to discuss developments in the international mail environment and opportunities to reduce the incidence of illicit trade conducted therein.

5. Assess Scope of, And Respond to, Importer Identity Theft in the Trade Environment.

As part of a layered risk-management approach to customs enforcement, CBP is continuously incorporating data generated through its targeting programs to establish optimal levels of screening scrutiny for particular shipments. As a way to evade law enforcement detection, counterfeit syndicates are known to steal the identifications of legitimate importers with strong shipment integrity track records in order to move containers more easily under those false identities.

Especially vulnerable are known and trusted shippers who have earned tangible importation benefits such as expedited cargo clearance. Counterfeit syndicates obtain identifications of legitimate importers and submit falsified documentation to gain release of their merchandise at the border. By posing as the known importer, illicit traders may swiftly move large quantities of high-value goods into U.S. and world commerce.

Not enough information is publically available to assess the scope and impact of importer identity theft domestically, or how criminal syndicates may use the tactic globally. As a result of some globally coordinated enforcement operations, preliminary evidence suggests that the tactic may be widely used, including in combination with other obfuscation schemes (see sidebar).[13] Enhanced international collaboration and information sharing would increase U.S. and other customs authorities' ability to safeguard against cross-border illicit trade.

ACTION NO. 3.10: Consultation with private sector stakeholders on the prevalence and nature of, and responses to, importer identity theft. Within 18 months of the issuance of this Plan, ICE and CBP will consult with private sector stakeholders on the prevalence and nature of – and responses to – importer identity theft, including: (1) tactics employed by illicit actors to gain access to identifications of known importers; (2) current efforts by the private sector to reduce the incidence of importer identity theft; and (3) possible options for changes to current Federal and private-sector processes to reduce the incidence of importer identity theft.

"Operation GRYPHON"
World Customs Organization (WCO)

Global Cooperation: 93 national Customs administrations, coordinated by the WCO, took part in the Operation beginning in October 2013.

Scope: Focus on trade in illicit tobacco across the range of customs control and clearance processes, including within duty-free outlets, free trade zones (FTZs), bonded warehouses, and means of transport.

Seizures: 593 million cigarettes, 77 tons of smoking tobacco, 31 tons of raw tobacco, 15 tons of water pipe tobacco, 5 tons of chewing tobacco, and 2.5 tons of hand rolling and pipe tobacco.

Criminal Tactics: Counterfeit cigarettes were transported in sea containers, as well as by land transport (trains and trucks). Operation GRYPHON confirmed that:

- Identity Theft: Criminals engaged in "identity theft" by using the identities of import and export companies with good reputations as a method to avoid raising the suspicion of customs officials.
- Free Trade Zones (FTZs): FTZs played an important role in the illicit smuggling schemes. Consignments arriving in these zones were subsequently repacked into other containers, enabling the illicit cigarettes to be lost or disappear. They then exited the zone as low-value goods, either misdeclared or concealed in other shipments.
- Conflict Zones: A large volume of containers was destined for conflict areas, such as Afghanistan, Syria, and Ukraine. Twenty-one containers bound for Syria could not be traced after arriving in the country – a clear case of smugglers taking advantage of conflict zones, where customs controls may be in temporary disarray.

See, e.g., World Customs Organization, "WCO News," at p. 7 (October 2014), accessed from http://www.wcoomd.org/en/media/wco-news-magazine/previous/~/media/1B6D8A89F61142AC9F4ADB8678DEF5C9.pdf; see also United States Department of State, "The Global Illicit Trade In Tobacco: A Threat To National Security," at p. 19 (December 2015), accessed from http://www.state.gov/documents/organization/250513.pdf.

6. Enhance Customs Recordation Systems and Public-Private Collaboration on Information Collection.

One of the unique aspects of combating trade in counterfeit and pirated goods is that it requires close partnership and coordination with the private sector whose rights are exploited to the detriment of the affected businesses, consumers, and national interests alike.

Customs enforcement officials rely on product information data to identify illicit merchandise shipped into the United States. Without thorough, accurate, and appropriately submitted product information, officers examining incoming containers cannot effectively differentiate genuine articles from counterfeits. CBP prioritizes enforcement of IP that has been recorded through the Intellectual Property Rights e-Recordation (IPRR) application (FIG. 50), which is done after they have been registered with the U.S. Patent and Trademark Office (USPTO) or the U.S. Copyright Office.[14] The information submitted by the rights holder through the e-recordation process is one of the most valuable tools CBP has for making infringement determinations.

With today's voluminous and fast-moving global trade, it is important that law enforcement continue to enhance its means of foiling ever-changing illicit trade practices. Federal law enforcement will never be able to seize its way out of the problem alone. Rather, effective IP enforcement must include tools and resources to identify and interdict counterfeit and pirated goods, and investigate and prosecute those who traffic in them. The need for industry support has evolved from strictly aiding in infringement determinations to serving as tactical partners alongside Federal agencies. Working in partnership with the private sector, Federal law enforcement officials are able to leverage industry knowledge and expertise to improve enforcement efforts.

No one knows how a product is being imitated better than the rights holder. Industry has access to established platforms for sharing this intelligence with Federal law enforcement.[15] Collaborating and sharing appropriate information with industry stakeholders gives law enforcement a more complete picture of the trade environment. Leveraging data from additional sources leads to more comprehensive risk profiles, better risk segmentation, and more actionable intelligence. Furthermore, the intelligence gained allows agencies like CBP and ICE to better utilize targeting capabilities, detect bad actors earlier in the supply chain, respond to risks on a real-time basis, and anticipate new threats before they fully emerge.

CBP's online IPRR recordation application invites, though it does not require, trademark and copyright

FIG. 50: Intellectual Property Rights e-Recordation (IPRR) Application



owners to furnish CBP with certain supplemental information, such as information on licensees and manufacturers, shipping channels, and shipping patterns. It has been CBP's experience, however, that such information is soon outdated. Although some rights holders are diligent about maintaining current data, some are not, and others choose not to supply that information.

CBP has recently upgraded IPRR to enable rights holders to renew recordations and update ownership information online. In considering further upgrades, CBP should consider developing an account-based platform to enable rights holders to access their information in real-time, which would increase the transparency and effectiveness of IPR enforcement. Rights holders should be encouraged to include product identification information when submitting a recordation application. In addition, CBP should encourage rights holders to develop product identification webinars that can be viewed live or on-demand by frontline officers working to authenticate recorded products.

ACTION NO. 3.11: Enhance the IP rights recordation system database (IPRR). Within two years of the issuance of this Plan, CBP will pursue enhancements to the IPRR database to improve internal functionality and promote external transparency.

ACTION NO. 3.12: Call for private sector best practices for partnering with CBP officials to enable rapid infringement determinations. Within one year of the issuance of this Plan, CBP will conduct outreach and report on impediments to voluntary submission of requested data and options for increasing IPRR participation, including education efforts targeted to industry highlighting the benefits of recordation. As part of this effort, CBP will engage with private sector stakeholders to discuss: the benefits and challenges of maintaining up-to-date recordations; submitting supplementary product identification materials; and providing training on IPRR systems and processes.

7. Invest in Anti-Counterfeiting Technology.

Given the rise of advanced manufacturing processes, the accessibility of global transportation networks, and other factors, we are now witnessing a proliferation of vast categories of counterfeit goods that are difficult to readily discern from a visual inspection. These illicit products—such as fake electronics, automotive and aircraft parts, pharmaceuticals, and consumer care products—pose significant risks to public health and safety, while also generating illicit revenue for criminal syndicates.[16] These illicit products cost governments and the private sector hundreds of billions of dollars annually, and undermine national interests when the products are intended for government or other sensitive operations and supply chains.[17]

The difficulty of product authentication—or put differently, counterfeit detection—is acutely felt by a number of entities. From frontline law enforcement personnel that are tasked with facilitating legitimate trade and preventing entry of counterfeit goods into the country, to intended end users who depend on the integrity or performance of the genuine article, and all the intermediaries in between (such as contractors, sub-contractors, wholesalers, retail outlets, service providers, etc.), effective product authentication remains an ongoing challenge.

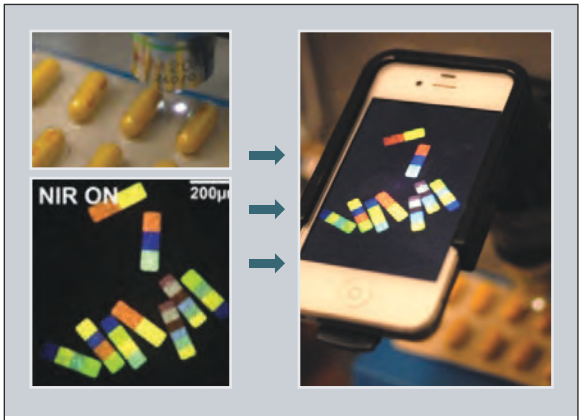
In light of these risks and challenges, an enhanced government response with the active participation of a wide range of actors is necessary to contribute to a multidisciplinary response to the problem. In particular, private sector stakeholders and technology providers may offer significant contributions for curbing counterfeiting, including by the development of technological solutions to safeguard domestic and global supply chains.[18]

Over the past few decades, a variety of anti-counterfeiting technologies have been developed, from barcodes to holograms; invisible pigments, inks, and infrared markers; radio frequency identification tags (RFIDs); and more recently, embedded nanotechnology-based solutions. Certain legacy anti-counterfeiting technologies reportedly face a number of limitations, including difficulty in confirming accuracy in the field; the fact that the technology may itself be copied or spoofed; high manufacturing costs or reliance on expensive proprietary decoders that require trained

users; or that the technology may prove difficult to scale and implement on a product-by-product basis.[19] For example, although a fake hologram may not fool the brand owner (or a well-trained law enforcement official), most untrained enforcement officials, supply chain intermediaries, retailers, and consumers are unlikely to be able to differentiate an authentic hologram from an imitation hologram any more than they may be able to readily distinguish a legitimate product from a sophisticated fake copy.

A number of promising technology-based anti-counterfeiting tools are emerging with expanded capacities and lower costs. For example, through funding by the National Science Foundation, the National Institutes of Health, the U.S. Army Research Office, and the U.S. Air Force, research is being conducted on the creation and use of micro-particles (FIG. 51), which are about 200 microns long and thus invisible to the naked eye, that may serve as unique product tags or micro-barcodes detectable by handheld a device, such as a smartphone.[20]

FIG. 51: Glowing Stripes—Example of Micro-Barcodes Applied to Drug Packaging.



A smartphone, equipped with a magnifying lens and infrared light source, acquires an image of the micro-barcodes embedded onto a pharmaceutical blister pack.

Source: Lincoln Laboratory, MIT

Similarly, the Defense Advanced Research Projects Agency (DARPA) is seeking modern, technological-based solutions to address the grave risks that counterfeit integrated circuits (ICs) pose to the security and integrity of electronic systems in the military supply chain.[21] DARPA's Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program, for example, seeks to eliminate counterfeit ICs from the electronics supply chain by making counterfeiting too complex and time-consuming to be cost effective.

The SHIELD program seeks to develop microscopic components that could be added into the packaging of an integrated circuit during manufacturing or in another trusted setting and later scanned from a handheld device such as a smartphone (or larger device for large shipments). These components, known as "dielets" (FIG. 52), would send an encrypted message with information from embedded sensors to prove their authenticity and provide confirmation as to whether they have been subject to any tampering. Once these and other promising developments are realized, then an untrained operator at any place along the supply chain will be able to confirm the authenticity of any component in the military supply chain and commercial sector alike, receiving high-confidence results immediately, on site, securely, and at nominal cost. This is one example of emerging technologies that must serve as part of the solution to address illicit activity in the global era.

FIG. 52: DARPA Concept—A high-frequency (HF) RFID silicon chip ("dielet").



Size on Display: At a size of 100x100 microns, the "dielet" fits on tip of Lincoln's nose on a penny (L), and easily passes through the eye of a needle (R).

When work on the project is completed in 2019, DARPA expects that the chip will be used to verify the authenticity of small electronics, including integrated circuits, used by both the defense and commercial industries.

Industry's partnership with law enforcement to develop, adopt, and implement innovative authentication technology is critical to frontline personnel's ability to spot illicit goods amid the free flow of legitimate commerce. These technological breakthroughs not only have the potential to aid in interdiction efforts, but may also reduce overall

transaction costs for rights owners and authorized intermediaries along the supply chain.

ACTION NO. 3.13: Engage with rights holders on technological solutions to aid in interdiction efforts. CBP, the National Intellectual Property Rights Center (IPR Center), IPEC, and other interested Federal agencies will meet at least annually with industry stakeholders to discuss potential new opportunities for employing technology to enhance identification and investigation of illicit trade.

ACTION NO. 3.14: Hold a "State of Authentication Technology" conference. The U.S. Interagency Strategy Planning Committees on IP Enforcement, in coordination with DARPA, the National Science Foundation, the National Institutes of Health, the U.S. Army Research Office, and other interested agencies, will organize and host a conference on the state of authentication technology. In addition to providing a forum for information sharing among Federal agencies, the conference will focus on development of and research into authentication technologies and opportunities for public sector adoption and deployment of authentication technologies.

8. Enhance Interdiction Through Specialized Task Forces.

While CBP generally trains all officers to identify illicit and pirated goods, practical limitations exist. For example, CBP officers are tasked with enforcing hundreds of laws. As a result, each officer is not necessarily a specialist at identifying counterfeit and pirated products, nor is every officer aware of the tactics and trends used to conceal illicit goods and evade detection.

Over a period of years, the use of specialized IPR task force personnel within CBP to identify and interdict counterfeit and pirated goods could result in significant intellectual property rights enforcement achievements. By increasing a team's knowledge of industry-specific issues, and adapting team composition to new trends identified in the trading environment, specialized task forces enable law enforcement personnel to quickly pivot to effectively address emerging risks.

CBP's Mobile Intellectual Property Enforcement Teams (MIPETs) highlight the significant enhancements to IPR enforcement made possible through the use of specialized task force personnel. MIPETs were developed by CBP as a way to combine the forces of agency IPR enforcement experts and frontline field personnel for aggressive, heightened targeted enforcement efforts—or "blitzes"—to maximize interdictions during a specific period of time.[22] With subject-matter experts available to quickly analyze the current state of IPR enforcement efforts at a port and serve as resources to field personnel during intense screening efforts, CBP is able to proactively and flexibly combat intellectual property crimes.

Opportunities exist to further support specialized IPR enforcement units and ensure that these mobile operations have a lasting impact on a host port by increasing staff knowledge of the dynamic nature of IPR-based illicit trade, practicing interdiction best practices and tactics, and establishing a benchmark for attainable seizure rates.

ACTION NO. 3.15: Expand the use of IPR task forces at POEs. Within one year of the issuance of this Plan, CBP will produce a plan for expanding the use of flexible, standing IPR enforcement task forces, such as MIPET, for deployment as needed in support of agency efforts to interdict counterfeit and pirated goods at all POEs. CBP will further assess ports following IPR enforcement task force actions to determine the effect on long-term interdiction rates.

9. Enhance Fines, Penalties, and Forfeiture Processes and Practices.

Trade in counterfeit and pirated goods is viewed as a low-risk, high-reward criminal activity since the likelihood of detection is viewed as low and the penalties imposed after detection can be difficult to collect from violators. As a result, if a seizure does not lead to civil penalties or criminal prosecution, the illicit actor's only cost is the loss of the seized shipment. Enforcement activities must endeavor to deter illicit conduct and reduce the overall profitability of counterfeit operations that undermine markets, public safety, and the rule of law.

Under Federal law CBP is authorized, after seizure and forfeiture, to assess civil penalties (fines) against any person found to import counterfeit merchandise for

sale or public distribution, in an amount not more than the value that the seized merchandise would have had if it were genuine.[23] Further, for second and subsequent seizures against the same party, CBP is authorized to impose penalties in an amount of up to twice the value that the merchandise would have had if it were genuine.[24]

The use of CBP-issued fines and penalties merits further attention, including an in-depth assessment of practical impediments to issuing or collecting fines, as well as opportunities to utilize existing civil penalty authorities for budgetary and law enforcement purposes. Although CBP-issued fines and penalties may prove difficult to collect in many circumstances, the expanded use of appropriately scaled CBP civil penalties may significantly increase deterrence of illicit trade activity and could increase resources available for IPR enforcement efforts.[25]

To further deprive criminals of their illicit profits, and to protect the Government supply chain, it is important for all Federal Government partners to be aware of the illicit trader's identity. Even in cases where it would be impractical for CBP to collect fines, CBP should consider ways to utilize existing fine and penalty authorities to establish which violators have had shipments seized, and to raise flags of caution to prevent additional illicit business from being conducted. To this end, CBP should continue to assess penalties against violators, while looking for opportunities to create a transparent violators list for use by Government agencies. By compiling and sharing information about known violators with those outside of the traditional targeting environment, such as Federal procurement officials, business with illicit traders may be deterred.

ACTION NO. 3.16: Evaluate use of IPR civil penalties. Within two years of the issuance of this Plan, DHS, in consultation with OMB, will conduct an assessment of civil penalties imposed under 19 U.S.C. 1526(f) to identify: (1) obstacles preventing the routine imposition of fees on, and collection of fees from, violators and assisting entities; and (2) optimal penalty levels necessary to produce a strong deterrent effect.

ACTION NO. 3.17: Identify opportunities to notify other interested partners of known violators. Subject to limitations on the sharing of sensitive law enforcement data, DHS will explore options for sharing data on known violators with other Federal agency personnel regardless of the imposition of fines and penalties on those entities.

10. Improve Administration of ITC Exlusion Orders.

CBP is responsible for administering exclusion orders issued by the U.S. International Trade Commission (ITC). The majority of ITC exclusion orders are presently patent-based. They direct CBP to exclude from entry articles that infringe valid patent claims.

Most exclusion order cases administered by CBP involve articles that were not directly reviewed or found to infringe by the ITC, namely, so-called "redesigned" articles. Consequently, CBP's role requires that it rule on whether a redesigned article is subject to an ITC order despite being different in some respect from the article originally excluded by the ITC.

The CBP rulings process, set forth at 19 C.F.R. part 177, is *ex parte*. This is appropriate for the typical customs transaction, but may be unsuited to the exclusion order context where there are two parties in interest: the complainant and the importer. Importers submit most ruling requests, and because CBP's current rulings process is *ex parte*, there is no authority for CBP officials to include the complainant in the proceeding. Consequently, the complainant may not become aware of the matter until CBP publishes its ruling, despite the complainant's potentially significant economic interest in the outcome of the proceeding.

There are opportunities to review CBP's administration and enforcement of ITC exclusion orders for enhancements by way of a possible *inter partes* proceeding at CBP that would afford CBP the opportunity to reasonably hear from both the importer and the complainant, and allow each to make appropriate arguments while rebutting those of the other.

ACTION NO. 3.18: Evaluate workability and options for implementing *inter partes* proceedings as part of CBP's exclusion order rulings process. Within one year of the issuance of this Plan, CBP will review and report on whether changes to the structure of the exclusion order rulings process are warranted, and make such recommendations for regulatory amendments as may be appropriate.

11. Expand and Enhance the Use of Post-Entry Audits.

Law enforcement officials use informed compliance site visits as one tool to help prevent the recurrence of IPR violations. These site visits are designed to have a deterrent effect.

Over the past ten years, the Federal Government's approach of providing stakeholder audit assistance related to IP compliance has evolved greatly. Early on, engagements included evaluating and testing internal controls over IPR, providing importers with informed compliance and ways to strengthen internal controls, and quantifying identified infringements through a review of books and records for potential penalty action. The audits, while beneficial, were resource-intensive investments.

In 2012, CBP piloted the IPR Strike Unit (ISU) as an efficient collaboration among DHS partners to target and address violations shortly after importation, before or during the detention phase. ISU engagements have largely replaced full post hoc IP audits because they are more collaborative, focused, and efficient. The most successful elements of the full audit model were maintained and enhanced under the ISU program.

Recently, CBP expanded the site visits to: (1) survey some repeat offender companies to inform them of their responsibilities with respect to compliance with IPR laws and regulations; (2) obtain an understanding of their importing practices related to IPR; and (3) determine if there are factors that may require further CBP consideration. This is an efficient way to assess risk and determine which companies warrant further action.

As interdiction methods and educational efforts continue to evolve, the use of post-entry audits via site visits with informed compliance remains a valuable tool to both help deter future violations and enable stronger enforcement actions if the violations are repeated. Additional procedures, including issuance of post-entry IPR penalties, may provide law enforcement with even greater tools to secure future compliance.

ACTION NO. 3.19: Evaluate the effectiveness of ISU in deterring IPR violations. CBP will examine the benefits of ISUs and surveys, and other possible real-time procedures, in contributing to the agency's ability to effectively assess risks and deploy resources in a targeted, efficient manner. CBP will recommend such expansion or enhancement of post-entry audit procedures as appropriate based on the results of this review.

ACTION NO. 3.20: Study options for reinforcing post-entry IPR penalties. Within two years of the issuance of this Plan, CBP will evaluate options for enhancing the deterrent effect of post-entry penalties. As part of this evaluation, CBP will examine the current usage and effectiveness of penalties to determine if they should be strengthened. In addition to offering options for prospectively strengthening post-entry penalty administration, CBP will report on the deterrent value of: (1) assessing penalties versus issuing warnings for a first violation; and (2) assessing escalating penalties on repeat violators, even if the second and subsequent violations are not to the same product or mark as in the first violation.

B. WORKING GLOBALLY: CUSTOMS EFFORTS TO CURB THE MOVEMENT AND TRADE OF COUNTERFEIT AND PIRATED GOODS AROUND THE WORLD.

Effective and efficient customs administrations are vital for the economic, social, and security development of nations around the world. Customs administrations play a critical role in trade facilitation and revenue collection, serving as one of the most important sources of revenue for most countries.[26] However, customs administrations also have a unique observation position: they are at the crossroads between fair trade, the economy, fiscal and budget issues, crime interdiction, and environmental concerns, to name but a few.

As key border agencies, the customs administrations' growing role in providing community protection and national security—by securing the supply chain from prohibited or unsafe imports, and in turn, denying the flow of illicit proceeds to producers and importers of counterfeit and pirated products—can make a major contribution to enhancing overall national competitiveness. Investors take note of markets where customs administrations result in the efficient delivery of high quality goods to market and the exclusion of substandard, illicit goods from competition with legitimate goods. Trading partners, likewise, rely on customs administrations to fulfill faithfully the terms

of the trade agreements that serve as pillars of global economic stability. Ensuring the highest quality administration of customs laws ensures the highest quality of trade, which is in the interest of all nations and market participants around the globe.

1. Promote Necessary Seizure Authority and Best Practices Around the World.

Each nation should endeavor to maximize its effectiveness at interdicting illicit goods. By adopting modern and effective interdiction authorities, international customs organizations will be able to conduct enforcement operations consistent with international norms. The United States and the WCO, for example, have long advocated for development of model legislation and best practices, but progress has been slow.[27] Two key subject matter areas that present a material opportunity for improvement are: (1) the implementation of *ex officio* authority, and (2) the confirmation that the clearance of goods includes those that are moving *in transit*.

Ex Officio Authority.

The ability of customs officers to act *ex officio* in interdicting infringing goods is critical to our success in curbing illicit trade. As recognized by the WCO:

> *"Customs' powers to act ex officio are a key feature of effective border enforcement regime(s). In the vast majority of cases, customs officers are the only ones to know when and which allegedly infringing goods are transported. Therefore unless customs are empowered and obliged to act on their own to stop suspected shipments at the borders, the border measures will remain ineffective."*[28]

There are different definitions of *ex officio*, but in the simplest terms, it means that customs officers have the authority to suspend the release of goods *absent* an application filed by the rights holder. There would still exist the need for a process—civil, judicial, or administrative—to reach a final determination, which could lead to forfeiture and destruction. However, at the critical first stage, customs officers are empowered to be able to act on their own initiative, relying on good training and skills, to stop infringing goods from entering into the stream of commerce.

Put differently, without *ex officio* authority, a nation is left powerless as it awaits the filing of an application by the rights holder, surrendering all national interests and control in curbing illicit trade by placing the decisional authority (to seize or not to seize) into the hands of a single rights holder. This arrangement does not, and cannot, withstand scrutiny in the modern global era and is inadequate for at least two reasons.

First, the rights holder may not have adequate resources to initiate an action in each and every implicated country, city, or port around the world. Unfortunately, the absence of actual *ex officio* authority in law (and applied in practice) is not limited to a small subset of nations, but rather, appears to be the norm for large segments of the world. Small and medium enterprises, for example, generally do not have the infrastructure in place to be responsive to customs-based inquiries the world over, especially within the allocated window of time (*i.e.*, generally 3-5 days). Even with a large, multinational company, the scope of global trade and container port throughput is so vast, that few if any companies can reasonably respond to all trade inquiries in a timely manner. There are over 100 ports in Latin America and the Caribbean alone, with the container port throughput for the top 20 ports (*FIG. 53)* in this region at approximately 48 million TEU (a standard unit of measurement, with each TEU equivalent to a container of 20 feet).

Secondly, as discussed in detail in Section I, above, a practice to release goods absent a complaint from rights holders effectively overlooks all the threats and hazards that the illegal import represents if permitted to enter the supply chain: consumer health and safety; the integrity of supply chains; sustaining fair competition and the rule of law; curbing the financing activities of criminal syndicates; sustaining environmentally responsible practices; and not facilitating the trade in forced or child labor-derived goods.

A well-developed *ex officio* implementation system involves CBP partnering with the private sector, other Federal agencies, and foreign governments. It includes gathering advance information for targeted screenings, stopping illicit goods at the point of entry or exit, and punishing those who violate law and regulations. Effective execution of *ex officio* authority saves valuable resources, takes significant pressure off the judicial system, and preserves national economic and security interests while providing due process to safeguard

FIG. 53: Example of Container Port Throughput Profile in 2015; Top 20 Ports in Latin American & the Caribbean.[29]



importers and rights holders. Likewise, legal options are preserved, allowing an importer to elect to have the case adjudicated in the judicial system.

In-Transit Authority.

Similarly, effective IP enforcement of transiting goods is critically important to preventing the diversion of infringing goods to neighboring countries. Some countries' legal systems take a hands-off approach to goods transiting through or being transshipped at their POEs bound for final destinations elsewhere, even where strong indications of criminal activity are present.

> "To ensure that Customs have the tools necessary to fight effectively the growing problem of cross-border counterfeiting and piracy, it is of paramount importance that Customs have the ability to suspend counterfeit and pirated goods destined for export and goods which are in transit. Practical experience…demonstrates the importance of customs intervention also with respect to goods in transit."
>
> *Source: WCO, "Model Provisions for Model Provisions for National Legislation to Implement Fair and Effective Border Measures*

To properly enforce IPR for in-transit goods moving under customs control from country to country, trading partners must share the obligation to intercept goods, even if they are destined for consumption in a foreign country. Rarely do shipments of goods go directly from the country of manufacture to the country of importation, especially those moving in containerized cargo. Rather, they transverse multiple jurisdictions on their journey to the consumer. Hong Kong and Turkey are prime examples of countries that see a significant volume of goods transiting through their countries.[30] While a good portion of this trade is legal, a global standard on the enforcement of IPR for in-transit goods must be developed.

ACTION NO. 3.21: Study the ability of customs administrations around the world to intercept in-transit goods, inspect suspicious merchandise, and seize infringing goods.

Within one year of the issuance of this Plan, CBP and ICE, in consultation with the Departments of Justice and State and the U.S. Trade Representative, will evaluate and report on the existence and implementation of in-transit customs authority worldwide. This global inventory of legal authorities and administration should include plans for regular Federal assessment and monitoring of global trading partners' in-transit authority.

ACTION NO. 3.22: Study the establishment of an alert protocol. Within two years of the issuance of this Plan, CBP will evaluate and report on the impact of allowing countries without in-transit authority to alert, possibly through the WCO's Customs Enforcement Network, the destination country of suspected infringing goods destined for their borders. The report should include a discussion of the benefits to U.S. trade and economic interests of such an alert protocol.

ACTION NO. 3.23: Promote global adoption of ex officio authority. Within one year of the issuance of this Plan, the IPEC will convene and chair a meeting of the U.S. Interagency Strategic Planning Committees on IP Enforcement to identify opportunities to promote *ex officio* authority in countries around the world.

2. Curb Illegal Operations Within Free Trade Zones.

Governments are increasingly facilitating trade and economic development by creating FTZs, which are free trading jurisdictions within a country characterized by relaxed customs controls, exemptions from import duties and taxes, and simplified administrative procedures. FTZs stimulate a multitude of economic benefits for the host country, including increased trade, new domestic business formation and employment, access to foreign investment, and enhanced opportunities for technology transfer.[31]

While FTZs are good for and strongly support international trade and development, their proliferation has also attracted the interest of criminal actors that take advantage of the relaxed oversight and softened customs controls to manufacture and distribute counterfeit goods.[32] These bad actors typically use FTZs to carry out at least one of three different types of illegal operations:

(1) Import shipments of counterfeit goods into FTZs, and then re-export counterfeit goods to other destinations (*i.e.*, FTZs are used to disguise original points of manufacture and become distribution points in the supply chain of counterfeit goods);
(2) Import unfinished goods and then further manufacture them in FTZs by adding counterfeit trademarks, or by repacking or re-labeling the goods, and then export those finished counterfeit goods to other countries; or
(3) Completely manufacture counterfeit goods in FTZs.[33]

These illicit merchants are exploiting the very ecosystem that governments have put in place to help FTZs contribute to economic development, and if this criminal activity is allowed to occur or is ignored, the underlying objectives of FTZs to promote trade and economic growth are undermined and weakened. Opportunities exist to collect and analyze additional information as to the nature and scope of illicit activity occurring within legitimate FTZs, and to promote enhanced IP enforcement mechanisms in these zones.

ACTION NO. 3.24: Identification of opportunities to curb IPR abuses in Free Trade Zones. Within 18 months of the issuance of this Plan, the U.S. Interagency Strategic Planning Committees on IP Enforcement will convene an interagency working group, including the Department of Labor and other relevant agencies, to discuss the extent and nature of IP infringement in FTZs and to identify opportunities for Federal agencies to engage in activities that could enhance IP enforcement in FTZs.

3. Support Modern Recordation Systems in Developing Countries

Many developing countries lack adequate means for electronically recording or searching for registered trademarks and copyrights by way of an online database, which in turn makes the interdiction of counterfeit and pirated goods more complicated and inefficient. The amount of information exchanged with and collected by customs authorities, if not automated, is overwhelming.

> "In Africa, for example, the average customs transaction involves 20–30 different parties, 40 documents, 200 data elements (30 of which repeated at least 30 times), and the rekeying of 60-70 percent of all data at least once. In most African countries, there are two complete sets of controls to be completed – one on each side of the border post – with numerous forms of documents to be filled and cleared. These administrative hurdles escalate trade costs…[and] also encourage illicit trade and corruption in order to bypass delays at customs and border posts."
>
> *Source: African Development Bank (AfDB), Border Posts, Checkpoints, and Intra-African Trade: Challenges and Solutions (Jan. 2012); United Nations Economic Commission for Africa (UNECA), Assessing Regional Integration in Africa IV (May 2010).*

As a result, it is important that we continue to support and strengthen the infrastructure of our global partners in combating counterfeit and pirated trade, making sure that they have the right tools in place to combat illicit trade in the 21st Century.

The United States relies extensively on electronic recordation systems to enforce IPR. By exploring the expansion of programs like the WCO's Interface Public Members reference tool for IPR violations, and the development of the United Nations' Automated SYstem for CUstoms DAta (ASYCUDA) Intellectual Property Module, international customs processes are able to modernize and increase the level of enforcement globally.[34]

For example, the ASYCUDA system currently used by 97 countries is a framework that provides developing countries with a customs system at relatively low cost, by reforming and streamlining the customs clearance process, increasing trade facilitation, and strengthening the institution in member states. By modernizing global customs practices, law enforcement officers are able to use technology to speed up and simplify the goods clearance process, while providing a greater focus on enforcement. Through the addition of an IP module into a system that manages the entire customs clearance process prior to the arrival of the goods, up to their warehousing and ultimate release, the risks and costs associated with counterfeit and pirated trade may be diminished.

Automating the customs clearance process increases speed and predictability by simplifying and standardizing the information coming into the system and the steps involved in determinations. By elevating global enforcement through shared and best practices, and use of electronic information systems like online databases with robust IPR-based modules, international shipping channels can become more secure.[35]

ACTION NO. 3.25: Support modern recordation systems in developing countries to enhance global enforcement of IPR. DHS and the Department of State will engage with international counterparts to identify opportunities for improving recordation systems, including the international interoperability of such systems.

4. Tackle the Growing Costs Associated with the Storage and Destruction of Counterfeit Goods.

The storage and destruction of counterfeit goods have become a major issue in a substantial number of countries.[36] Governments (*i.e.*, taxpayers) or right holders often bear the costs for the storage and destruction associated with seized counterfeit and pirated goods, while those entities that profit from illicit trade are generally subject to no disposal costs. Given the increase in illicit trade in counterfeit and pirated products, governments and rights holders are facing a growing and significant financial burden that needs to be solved without further delay.

FIG. 54: Over 100,000 counterfeit 'hover boards' (comprised of metals, plastics, rubber, electrical components, and lithium-ion batteries) and related parts are stored at CBP facilities, awaiting destruction.



Source: CBP (2016), Port of Chicago

In some countries, such as the United States, the Federal Government incurs the costs to store and destroy counterfeit and pirated goods, while other countries require the infringed rights holder to pay the costs for counterfeit and pirated goods seized by customs authorities.[37]

From a policy standpoint, taxpayers should not carry the burden of paying for costs associated with the storage and destruction of fake goods that have been shipped in violation of law in instances where the importer, exporter, or carrier transporting the infringing goods is in a position to bear the costs. Similarly, inequities exist when the costs of storage and destruction are placed on the victim of the crime (*i.e.*, the infringed rights holder), as the victim has committed no wrong and the enforcement of a country's laws represents a significant state interest (*e.g.*, promoting economic development; ensuring public health and safety; curbing the flow of illicit proceeds; supporting labor and environmental standards, *etc.*).[38] Moreover, rights holders in the form of small and medium enterprises (SMEs), as well as larger entities, may not be prepared to pay storage and destruction costs the world over for illicit goods that they did not manufacture and do not control.

> "Transport operators provide critical services that are subject to abuse as part of the counterfeiting supply chain. Counterfeit goods depend on land, air and sea shipping and transportation services to cross borders and reach foreign markets. These intermediaries are critical players…in stopping the flow of fake goods."
>
> *Source: International Chamber of Commerce (ICC-BASCAP), "Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain" (March 2015), p.16*

To address this problem, the roles of the individual players in the supply chain must be fully understood and opportunities to reasonably shift costs explored. Specifically, the United States and foreign countries must explore opportunities to pass costs directly to infringers, and where that is not possible or practical, to assess the role of importers, exporters, carriers, and others along the supply chain that profit (knowingly or

unknowingly) from the trade in counterfeit and pirated goods, and partner with these entities to pass costs onto the infringers.

The policy focus is two-fold: to minimize costs borne by taxpayers and right holders and, equally as important, to identify opportunities to implement policies that dis-incentivize practices that may support illicit trade in counterfeit goods, while incentivizing the adoption of best practices to increase accountability in the global shipping trade. The aim is to have the infringers held liable for storage and destruction costs and, whenever the identity of the infringer is unknown or the infringer refuses to pay such costs, to encourage and empower "economic operators" involved in the trade in infringing goods, such as carriers, to pass the costs onto the infringer by way of existing contractual relationships.[39]

Incentivizing Carriers to Address Costs Associated with Violative Shipments from their Customers

Carriers have a contractual relationship with, and financially benefit from, the entity (*i.e.*, exporter, importer-of-record, etc.) engaged in illicit trade. These intermediaries are well positioned to pass costs and penalties onto their respective customers by way of contractual obligations, including, for example, by imposition of fines, escrow and security deposits, and the like, especially on behalf of importers/exporters with no verifiable trade history.

Stronger cooperation between governments, right holders, and intermediaries—including land, air, and sea transport operators—may facilitate the effective identification of entities engaged in illicit activity, as well as provide opportunities for cost recovery.

ACTION NO. 3.26: Assess opportunities to shift storage and destruction costs to entities involved in the trade in infringing goods. DHS will assess the state of U.S. storage and destructions costs, and provide recommendations to the U.S. Interagency Strategy Planning Committees on IP Enforcement, and other appropriate Federal Government stakeholders, on how to shift the burden away from the Government (or rights holders) to the illicit trader that is directing the violative shipments into the United States. Consideration will be given to opportunities to develop voluntary practices with shippers to curb counterfeiters' abuse of their transport networks, including by way of an assessment of, for example, the role of enhanced due diligence and "Know Your Customer" processes, especially for new exporters in problem markets with little to no trading history.

ACTION NO. 3.27: Engagement with international community to consider measures to hold responsible entities accountable. The U.S. Interagency Strategy Planning Committees on IP Enforcement, along with other interested Federal offices and agencies, will consider opportunities for appropriate bilateral and multilateral dialogue, including in international fora such as the WCO, to promote a global approach to more effectively shifting costs to the illicit trader, working with transportation intermediaries to identify opportunities to promote exporter accountability.

5. Dispose of Infringing Goods in an Environmentally-Friendly Manner.

The growth in trade of counterfeit and pirated goods, coupled with the increasing effectiveness of customs authorities in detecting and confiscating infringing products, has given rise to new logistical and environmental dimensions as larger amounts of counterfeit goods are interdicted every year. The question of how to responsibly dispose of counterfeit items is particularly challenging with electronic, chemical, and pharmaceutical counterfeiting.[40]

The storage and environmentally-sound disposal of large quantities of illicit goods in hundreds of locations around the world presents a logistical challenge for governments and customs administrations everywhere. There is increasing recognition of the need to dispose of these goods in a safe and environmentally-sensitive way, which is resulting in adoption of disposal and destruction procedures that are more technically complex, costly, and onerous for governments and rights holders.[41]

The disposal of confiscated goods implicates two primary concerns: (1) the need to protect the IP owner and consumer alike from the existence of unlawful trade in fraudulent goods, while simultaneously depriving the

illicit trader or merchant of unwarranted profits; and (2) the need to manage the environmental impact of disposal of interdicted infringing goods. With respect to the first concern, disposal procedures must be effective and 100 percent secure to ensure that illicit goods are not re-introduced into the channels of commerce.[42]

With respect to the second concern, disposal procedures must ensure that illicit goods are discarded or destroyed in a manner that mitigates risks and damage to the environment. Current disposal options include recycling, open air burning, shredding, crushing, burying in landfill sites, and donation to charities. The methods adopted depend on the nature of the goods requiring disposal as well as the availability of appropriate disposal facilities. In many cases, even where appropriate facilities exist, environmentally-friendly disposal of counterfeits is complicated by the unknown origin and construction of components.[43] Minimizing the environmental impact of disposal requires specialized facilities, expertise, and high-level stakeholder collaboration.

In 2012, a first-of-its-kind workshop was supported by the United Nations Environmental Programme (UNEP) and the World Intellectual Property Organization (WIPO). This workshop was a critical first step toward an innovative and mutually supportive partnership between the two agencies to help build environmentally sound disposal capacity in key source and destination countries through technical assistance, partnerships, and exchanges of best practices and experiences.[44] This engagement must be continued.

ACTION NO. 3.28: Establish best practices for storage, destruction, and disposal of seized counterfeits. The U.S. Interagency Strategic Planning Committees on IP Enforcement will convene an interagency working group, including any additional appropriate Federal agencies, to develop standard operating procedures (SOPs) for storage, destruction, and disposal of seized counterfeits. These SOPs should focus on minimizing environmental impact without unduly burdening operational effectiveness and efficiency. The U.S. Interagency Strategy Planning Committees on IP Enforcement will also identify opportunities for Federal agencies to conduct pilot programs to recycle or reuse seized counterfeit goods. Recommended pilot programs will include appropriate safeguards to ensure that infringing goods are held securely and do not migrate into channels of commerce; create risks to the public or the environment; or prejudice the fulfillment of other statutory requirements, including revenue collection.

ACTION NO. 3.29: Educate IP enforcement professionals about storage and disposal options. DHS, in consultation with the USTR, Departments of State, Justice, and Agriculture, the Food and Drug Administration, and the Environmental Protection Agency and other relevant agencies, will develop training modules to raise awareness of options for the safe storage and disposal of seized counterfeit goods, with particular emphasis on pesticides, electronics, pharmaceuticals, and illegal drugs. DHS will consult with the International Trade Administration and Department of State to identify opportunities to share this training with international partners.

ENDNOTES

[1] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,"* at p. 6, accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/ipr_annual_report_FY%202015_final1.pdf.

[2] *See, e.g.,* R. Gil Kerlikowske, Commissioner, United States Customs and Border Protection, United States Department of Homeland Security, *"Commissioner Kerlikowske's Remarks at the University of South Florida"* (February 19, 2016), accessed from https://www.cbp.gov/newsroom/speeches-and-statements/commissioner-kerlikowske%E2%80%99s-remark-university-south-florida.

[3] *See, e.g.,* World Customs Organization, *"Illicit Trade Report 2013,"* at p. 69 (June 2014), accessed from http://www.wcoomd.org/en/media/newsroom/2014/june/~/media/WCO/Public/Global/PDF/Topics/Enforcement%20and%20Compliance/Activities%20and%20Programmes/Illicit%20Trade%20Report%202012/ILLICIT%202013%20-%20EN_LR2.ashx.

[4] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,"* at p. 19, accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/ipr_annual_report_FY%202015_final1.pdf; see also United States Department of Homeland Security, Customs and Border Protection, *"Intellectual Property Rights Seizure Statistics - Fiscal Year 2013,"* at p. 7, accessed from https://www.cbp.gov/sites/default/files/documents/ipr_annual_report_2013_072414%20Final.pdf.

[5] *See, e.g.,* World Customs Organization, *"Illicit Trade Report 2013,"* at p. 69 (June 2014), accessed from http://www.wcoomd.org/en/media/newsroom/2014/june/~/media/WCO/Public/Global/PDF/Topics/Enforcement%20and%20Compliance/Activities%20and%20Programmes/Illicit%20Trade%20Report%202012/ILLICIT%202013%20-%20EN_LR2.ashx.

[6] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,"* at p. 27 (finding that in FY2015, 52% of all seizures were from the express environment), accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/ipr_annual_report_FY%202015_final1.pdf.

[7] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,"* at p. 7, accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/ipr_annual_report_FY%202015_final1.pdf.

[8] Infographic provided by U.S. Department of Homeland Security, Customs and Border Protection. The infographic depicts U.S. Customs and Border Protection's intellectual property rights seizure process, and is for illustrative purposes only; a number of intermediary steps are not present. From a process management standpoint, an imported parcel containing counterfeit goods may go through several dozen "touch points" before a seizure is fully effected.

[9] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,"* at p. 7 (the $800 amount is based on a pilot program which resulted in the voluntary abandonment of 2,857 shipments, saving the Government $2.2 million in interdiction and processing costs), accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/ipr_annual_report_FY%202015_final1.pdf.

[10] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"Advisory Committee on Commercial Operations to U.S Customs & Border Protection - Government Report on Intellectual Property Rights Enforcement,"* at p. 1 (October 2015), accessed from https://www.cbp.gov/sites/default/files/documents/TERC%20IPR%20Issue%20Paper.pdf.

[11] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"Intellectual Property Rights Seizure Statistics - Fiscal Year 2015,"* at pp. 7,14 (finding that the pilot program resulted in 2,857 additional interdictions in FY 2015, the equivalent of 10 percent of average annual total seizures for containers of all sizes), accessed from https://www.cbp.gov/sites/default/files/assets/documents/2016-Nov/ipr_annual_report_FY%202015_final1.pdf.

[12] *See, e.g.,* Global Intellectual Property Strategy Center, P.C., Comment Letter to U.S. Intellectual Property Enforcement Coordinator, at p. 3 (September 25, 2015) (providing comments in response to IPEC's Federal Register notice of September 1, 2015), accessed from https://www.regulations.gov/document?D=OMB-2015-0003-0010.

[13] *See, e.g.,* World Customs Organization, *"WCO News,"* at p. 7 (October 2014), accessed from http://www.wcoomd.org/en/media/wco-news-magazine/previous/~/media/1B6D8A89F61142AC9F4ADB8678DEF5C9.pdf; *see also* United States Department of State, *"The Global Illicit Trade In Tobacco: A Threat To National Security,"* at p. 19 (December 2015), accessed from http://www.state.gov/documents/organization/250513.pdf.

[14] With respect to copyrights, The Trade Facilitation and Trade Enforcement Act of 2015 calls for the enforcement of a copyright, by the United States Customs and Border Protection, for which an application is pending in the United States Copyright Office "…to the same extent and in the same manner as if the copyright were registered with the Copyright Office, including by sharing information, images, and samples of merchandise suspected of infringing the copyright…." *See* Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. 114–125, § 304, 130 Stat. 122, 150 (2016) (codified as amended at 19 U.S.C. § 4343).

[15] *See, e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"e-Allegations" submission*, accessed from https://eallegations.cbp.gov/Home/Index2; *see also* United States Department of Homeland Security, National Intellectual Property Rights Coordination Center, *"Allegation of Counterfeiting and Intellectual Piracy" submission,* accessed from https://www.iprcenter.gov/referral.

[16] *See* Section I.

[17] *See* Section I.

[18] *See, e.g.*, United Nations Interregional Crime and Justice Research Institute, "*Ensuring Supply Chain Security: The Role of Anti-Counterfeiting Technologies,*" at p. 15 (February 2016) (finding that "…increased knowledge concerning technology developed to fight counterfeiting and ensure supply chain security may represent an important element to support national and international efforts aimed at fighting counterfeiting and illicit trade…"), accessed from http://www.unicri.it/topics/counterfeiting/anticounterfeiting_technologies/Ensuring_supply_chain_security_report.pdf.

[19] *See, e.g.*, Massachusetts Institute of Technology, Lincoln Laboratory, "*Colorful microparticles for anticounterfeiting: Glowing, smartphone-readable nanocrystals could authenticate products*" (February 2016), accessed from https://www.ll.mit.edu/news/REMcodes.html.

[20] *See, e.g.*, Massachusetts Institute of Technology, Technology Review, "*Tiny Particles Could Help Verify Goods: Chemical engineers hope smartphone-readable microparticles could crack down on counterfeiting*" (April 14, 2014), accessed from https://www.technologyreview.com/s/526621/tiny-particles-could-help-verify-goods/; *see also* Massachusetts Institute of Technology, Lincoln Laboratory, "*Colorful microparticles for anticounterfeiting: Glowing, smartphone-readable nanocrystals could authenticate products*" (February 2016), accessed from https://www.ll.mit.edu/news/REMcodes.html.

[21] *See, e.g.*, Bernstein, Kerry, *"Supply Chain Hardware Integrity for Electronics Defense (SHIELD),"* Defense Advanced Research Projects Agency, accessed from http://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense.

[22] *See e.g.,* United States Department of Homeland Security, Customs and Border Protection, *"CBP Seizes $12 Million in Counterfeit Goods in Operation Super Fake"* (February 4, 2015) (finding that Operation Super Fake, led by the United States Customs and Border Protection's Mobile Intellectual Property Enforcement Teams, resulted in the interdiction of nearly 700 shipments of counterfeit merchandise valued at $12 million as part of a Super Bowl XLIX focused blitz conducted over three days in January 2015), accessed from https://www.cbp.gov/newsroom/national-media-release/cbp-seizes-12-million-counterfeit-goods-operation-super-fake.

[23] 19 U.S.C. § 1526(f)(2).

[24] 19 U.S.C. § 1526(f)(3).

[25] Allen Gina, Assistant Commissioner, Office of International Trade, United States Customs and Border Protection, United States Department of Homeland Security, *"Statement Before the Senate Judiciary Committee"* (June 22, 2011), accessed from https://www.judiciary.senate.gov/imo/media/doc/11-06-22%20Gina%20Testimony.pdf.

[26] *See, e.g.*, The World Bank, "*Trade Logistics and Facilitation: The Role of Customs*," accessed from http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTTRANSPORT/EXTTLF/0,,contentMDK:22677049~menuPK:7327167~pagePK:210058~piPK:210062~theSitePK:515434,00.html.

[27] *See, e.g.*, World Customs Organization, *"Model Provisions For National Legislation To Implement Fair And Effective Border Measures Consistent With The Agreement On Trade-Related Aspects Of Intellectual Property Rights,"* accessed from http://www.asean.org/uploads/archive/20534-annex3.pdf.

[28] *See, e.g.*, World Customs Organization, *"Model Provisions For National Legislation To Implement Fair And Effective Border Measures Consistent With The Agreement On Trade-Related Aspects Of Intellectual Property Rights,"* at p. 125, accessed from http://www.asean.org/uploads/archive/20534-annex3.pdf.

[29] For more information, visit the Economic Commission for Latin America and the Caribbean, *"Ports Ranking. The Top 20 in Latin America and the Caribbean in 2015"* (issued June 13, 2016), accessed from http://www.cepal.org/cgi-bin/getprod.asp?xml=/perfil/noticias/noticias/4/54974/P54974.xml&xsl=/perfil/tpl/p1f.xsl&base=/perfil/tpl/top-bottom.xsl. The top 100 ports in Latin America and the Caribbean alone (as summarized in FIG. 55 on next page)—without consideration of ports in Asia, the Middle East, Europe, Africa or elsewhere—demonstrate the high volume and container port throughput, and the resulting burden on a rights holder when customs officers will not or cannot act without the lodging of an application by a rights holder.

[30] Office of the United States Trade Representative, *"2016 Special 301 Report"* (2016) p. 33, 56, accessed from https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.

FIG. 55: Latin American and the Caribbean Top 100 Port Rankings

Ranking	Port	Country	2015 (TEU)	Ranking	Port	Country	2015 (TEU)
1	Santos	Brasil	3,645,448	51	Acajutla	El Salvador	190,708
2	Colón	Panamá	3,577,427	52	TUP Pecem	Brasil	179,288
3	Balboa	Panamá	3,294,113	53	Port-au-Prince	Haití	178,452
4	Cartagena	Colombia	2,606,945	54	Lirquen	Chile	164,994
5	Manzanillo	México	2,458,135	55	Fort-de-France	Martinica	159,231
6	Callao	Perú	1,900,444	56	Barranquilla	Colombia	148,880
7	Guayaquil	Ecuador	1,764,937	57	Corinto	Nicaragua	138,006
8	Kingston	Jamaica	1,653,272	58	Zárate	Argentina	125,396
9	Buenos Aires	Argentina	1,433,053	59	TUP Super Terminais	Brasil	108,391
10	Freeport	Bahamas	1,400,000				
11	San Juan	Puerto Rico	1,210,503	60	Nieuwe Haven	Suriname	106,014
12	San Antonio	Chile	1,170,184	61	Puerto Castilla	Honduras	103,288
13	Limón-Moin	Costa Rica	1,108,573	62	Santa Marta	Colombia	102,037
14	Lazaro Cárdenas	México	1,068,747	63	Willemstad	Curacao	90,016
				64	Bridgetown	Barbados	86,508
15	Veracruz	México	931,613	65	Philipsburg	St. Maarten	-
16	Buenaventura	Colombia	911,533	66	Fortaleza	Brasil	79,808
17	Valparaiso	Chile	902,542	67	Vila do Conde	Brasil	78,422
18	Caucedo	Republica Dominicana	826,935	68	Antofagasta	Chile	77,467
				69	La Habana	Cuba	-
19	Montevideo	Uruguay	811,297	70	Progreso	México	67,653
20	Paranaguá	Brasil	782,346	71	São Francisco do Sul	Brasil	66,802
21	Rio Grande	Brasil	726,785				
22	TUP Portonave	Brasil	662,590	72	Ushuaia	Argentina	-
23	Altamira	México	647,369	73	Puerto Bolivar	Ecuador	60,207
24	Puerto Cortes	Honduras	624,302	74	Esmeraldas	Ecuador	59,413
25	Santo Tomas de Castilla	Guatemala	529,450	75	Puerto Plata	Republica Dominicana	58,410
26	TUP Itapoa	Brasil	501,523	76	Degrad-des-Cannes	Guayana Francesa	55,000
27	Coronel	Chile	471,426				
28	San Vicente	Chile	456,176	77	Georgetown-Cayman	Islas Caiman	54,607
29	TUP Chibatao	Brasil	450,544				
30	Puerto Cabello	Venezuela	438,244	78	Georgetown	Guayana	52,834
31	Puerto Barrios	Guatemala	432,141	79	Santo Domingo	Republica Dominicana	50,398
32	Haina	Republica Dominicana	417,642				
				80	Maracaibo	Venezuela	46,371
33	Suape	Brasil	398,166	81	Belize city	Belice	-
34	Puerto Quetzal	Guatemala	389,329	82	Natal	Brasil	37,607
35	Itajai	Brasil	323,565	83	Mazatlán	México	35,906
36	Port of Spain	Trinidad y Tobago	298,969	84	Imbituba	Brasil	30,602
				85	Rosario	Argentina	30,227
37	Rio de Janeiro	Brasil	297,991	86	Oranjestad	Aruba	-
38	Salvador	Brasil	283,500	87	Punta Arenas	Chile	29,677
39	Mariel	Cuba	260,000	88	Guanta	Venezuela	28,169
40	Caldera	Costa Rica	235,268	89	Belém	Brasil	28,029
41	Itaguai /Sepetiba	Brasil	228,173	90	Castries	Saint Lucia	-
				91	St John	Antigua y Barbuda	-
42	Iquique	Chile	227,099				
43	Arica	Chile	226,893	92	Bahia Blanca	Argentina	23,380
44	Puerto Angamos	Chile	223,124	93	Almirante	Panamá	22,346
				94	Madryn	Argentina	21,836
45	Point Lisas	Trinidad y Tobago	221,856	95	Matarani	Perú	20,002
				96	Campden Park	San Vicente & Grenadines	16,342
46	Paita	Perú	214,483				
47	La Guaira	Venezuela	208,484				
48	Jarry/ Pointe-a-Pitre	Guadalupe	201,948	97	San Lorenzo	Honduras	16,096
				98	Vieux Fort	Saint Lucia	-
49	Vitória	Brasil	193,917	99	San Andres	Colombia	13,711
50	Ensenada	México	193,424	100	El Guamache	Venezuela	12,917

Source: Infrastructure Services Unit | NRID | ECLAC | United Nation

[31] *See, e.g.,* International Chamber of Commerce, *"Controlling the Zone: Balancing Facilitation and Control to Combat Illicit Trade in the World's Free Trade Zones,"* at p. 9 (May 2013), accessed from http://www.iccwbo.org/advocacy-codes-and-rules/bascap/international-engagement-and-advocacy/free-trade-zones/.

[32] *See, e.g.,* Organization for Economic Cooperation and Development, *"The Economic Impact of Counterfeiting and Piracy,"* at p. 85 (June 2008) (stating that free trade areas have emerged as facilitators of intellectual property rights abuses, and that the lack of controls in these areas has made them attractive locations for parties engaging in trade of counterfeit and pirated products), accessed from http://www.oecd.org/sti/ind/theeconomicimpactofcounterfeitingandpiracy.htm.

[33] *See, e.g.,* International Trademark Association, *"INTA Model Free Trade Agreement: Measures To Halt The Transshipment And Transit Of Counterfeit Goods In Free Trade Zones,"* at pp. 29-30 (May 2011), accessed from http://www.inta.org/Advocacy/Documents/INTAModelFreeTradeAgreement.pdf.

[34] *See, e.g.,* United Nations Conference on Trade and Development, *"UNCTAD Trust Fund for Trade Negotiations, Technical Note No. 3: Use of Customs Automation Systems,"* at p. 4 (January 2011) ("the Automated System for Customs Data Management (ASYCUDA) is a computerized customs management system, developed by UNCTAD, which is fully integrated and covers the complete clearance process. The system handles manifests and customs declarations, accounting procedures, and transit and suspense procedures. ASYCUDA generates trade data that can be used for statistical economic analysis. It has been implemented in more than 90 countries and territories worldwide. A web-based version, ASYCUDA World, integrates state-of-the-art ICT technologies"), accessed from http://unctad.org/en/Docs/TN03_CustomsAutomationSystems.pdf.

[35] *See, e.g.,* Organization for Economic Cooperation and Development, *"OECD Trade Facilitation Indicators – United States"* (April 2014), accessed from https://www.oecd.org/unitedstates/united-states-oecd-trade-facilitation-indicators-april-2014.pdf.

[36] *See, e.g.*, World Intellectual Property Organization, Advisory Committee on Enforcement, Fifth Session, *"Addressing Costs and Balancing Rights,"* at p. 4 (September 2009), accessed from http://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_5/wipo_ace_5_7.pdf; *see also* Soentgen, Judith, *"Disposing Of Counterfeit Goods: Unseen Challenges,"* WIPO Magazine (November 2012), accessed from http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html.

[37] *See, e.g.*, U.S. Government Accountability Office, "*Intellectual Property: Observations on Efforts to Quantity the Economic Effects of Counterfeit and Pirated Goods,*" at p. 3 (April 2010) ("the federal government also incurs costs to store and destroy counterfeit and pirated goods. Seized goods have to be secured, as they have potential value but cannot be allowed to enter U.S. commerce. Storage may be prolonged by law enforcement actions, but the goods are generally destroyed or otherwise disposed of when they are determined to be illegal and are no longer needed. According to CBP officials, as seizures have increased, the agency's storage and destruction costs have grown and become increasingly burdensome. CBP reported that it spent about $41.9 million to destroy seized property between fiscal years 2007 and 2009"), accessed from http://gao.gov/new.items/d10423.pdf; *see also* Office for Harmonization in the Internal Market, *"Observatory Update on Storage and Destruction,"* at p. 7 (2014) (finding that in Greece, the intellectual property rights holder pays the expenses associated with the destruction of counterfeit goods, but these expenses can be recovered from the infringer), accessed from https://euipo.europa.eu/ohimportal/documents/11370/80606/Observatory+update+on+storage+and+destruction.

[38] *See, e.g.* International Trademark Association, *"INTA Bulletin: Customs Border Measures Around the Mediterranean"* (January 2011) (as one court in Israel opined, it is "inconceivable that a person whose rights were infringed will also be compelled to cover storage and destruction costs when he is not involved in the importation and only seeks to prevent the infringement of his rights"), accessed from http://www.inta.org/INTABulletin/Pages/CustomsBorderMeasuresAroundtheMediterranean.aspx (quoting *Dior v. Evivi et al.*, C.F. 6949-12-08 (March 11, 2009) (Israel)).

[39] *See, e.g.*, International Chamber of Commerce, "*BASCAP 25 Best Practices for IPR Enforcement,*" at p. 2 (September 2015), accessed from http://www.iccwbo.org/Data/Documents/Bascap/International-engagement-and-advocacy/Country-Initiatives/BASCAP-25-Best-practices-for-IPR-Enforcement-Version-24-September-2015/.

[40] *See, e.g.* World Intellectual Property Organization, *"The WIPO Disposal Study,"* at p. 11 (November 2013) ("Adjusted to include goods carried by air-cargo, the physical volume of infringing goods can be assumed to be the equivalent of 2.39 million TEU [a TEU is a full 20-foot maritime container]; or 6500 full 20ft containers passing through official controls each day."), accessed from http://artnet.unescap.org/tid/projects/infringing-goods-david.pdf.

[41] *See, e.g.*, Soentgen, Judith, *"Disposing Of Counterfeit Goods: Unseen Challenges,"* WIPO Magazine (November 2012), accessed from http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html.

[42] *See, e.g.*, World Intellectual Property Organization, "*Disposal and Destruction: An Examination of Challenges and Possible Solutions Prepared for the Sixth Session of the WIPO Advisory Committee on Enforcement,*" at p. 12 (September 2011), accessed from http://www.wipo.int/edocs/mdocs/aspac/en/wipo_ipr_pnh_11/wipo_ipr_pnh_11_ref_t3.pdf; *see also* TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Article 46, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) (providing that intellectual property infringing goods should be "disposed of outside the channels of commerce in such a manner as to avoid any harm caused to the right holder, or, unless this would be contrary to existing constitutional requirements, destroyed," and further, that "the simple removal of the trademark unlawfully affixed shall not be sufficient, other than in exceptional cases, to permit release of the goods into the channels of commerce"), accessed from https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

[43] *See, e.g.*, United Nations Office on Drugs and Crime, "*Focus on The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime,*" at p. 4 (January 2014), accessed from https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf.

[44] *See, e.g.*, United Nations Environment Programme, *"Information Note"* (July 2012), accessed from http://www.unep.org/ozonaction/News/Features/2012/SoutheastAsiaexploressynergies/tabid/104354/Default.aspx.

SECTION 4

PROMOTE FRAMEWORKS AND POLICIES TO ENHANCE THE EFFECTIVE ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS



SECTION 4

SECTION 4 CONTENTS

PROMOTE FRAMEWORKS AND POLICIES TO ENHANCE THE EFFECTIVE ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS

A. Promote Governmental Frameworks for Coordinated and Effective Intellectual Property Enforcement 121

1. The U.S. Model: A "Whole of Government" Approach to Intellectual Property Enforcement 122

2. The "Specialized Office" Approach to Intellectual Property Enforcement 125

B. Enhance Capacity-Building, Outreach, and Training Programs on Intellectual Property Enforcement in Other Countries 129

C. Promote Enforcement of U.S. Intellectual Property Rights Through Trade Policy Tools 131

D. Supporting Innovation and Technological Advancements: The Need for Tools for Effective and Predictable Patent Protection Domestically and Abroad 134

1. Enhancing Domestic Patent Protection 134

2. Enhancing Domestic Design Protection 136

3. Enhancing the Effectiveness of Patent Systems Abroad 137

a. Reducing Patent Pendency 137

b. Promoting Effective, Transparent, and Predictable Patent Systems 138

c. Enhancing Effectiveness of Design Systems Abroad 139

E. Broader Recognition of the Essential Role Universities Play in Innovation 140

F. Support Strategies that Mitigate the Theft of U.S. Trade Secrets 141

G. Promote Supply-Chain Accountability in Government Acquisitions 142

H. Calls for Research 143



INTRODUCTION

Today's IP enforcement environment is experiencing accelerated change brought about by fast-paced technological innovation, changes in methods of doing business and globalization. Strategies that served a country well in the past may be ill-suited to addressing new IP enforcement challenges. This section of the Strategic Plan identifies opportunities to refine elements of administrative frameworks and policies that promote effective IP enforcement, both in the United States and abroad.

A. PROMOTE GOVERNMENTAL FRAMEWORKS FOR COORDINATED AND EFFECTIVE IP ENFORCEMENT.

Illicit actors, including sophisticated transnational criminal organizations (TCOs), are realizing unlawful profits by exploiting weaknesses in IP enforcement regimes around the globe. They target and misappropriate trade secrets; exploit copyrighted content online; and move counterfeit, infringing and pirated merchandise across borders, all to the detriment of the artist, the innovator, and the creative and innovative industries at-large. Those actors engaging in IP-based illicit activity can take advantage of outdated, siloed government organizational structures that are often unable to monitor and respond effectively to rapidly changing environments and criminal tactics.

Our global environment, marked by increased international trade and a borderless online environment, creates an opportunity for IP enforcement entities, domestically and abroad, to assess the effectiveness and efficiency of their respective organizational structures and capabilities. Such strategic assessments ought to examine *how* the entity is organized to be responsive to, and stay ahead, of an ever changing enforcement environment. They may consider how the entity fashions itself to enable it to more successfully achieve its IP-enforcement goals and obligations under law.

Outdated organizational structures invariably become stale, resulting in significant inefficiencies and an institutional unwillingness—and sometimes inability—to press for the adoption of better practices to realize larger-scale achievements. As with the private sector, public institutions must not only develop competencies, but they must also strive continually to renew and

expand competencies to achieve congruence with a changing environment in order to realize maximum efficiency. The demands on the state require a dynamic administrative framework.

As an example of how a government can provide a more effective, agile response to combat IP-based illicit activity, the United States Government has adopted two distinct but complementary organizational approaches to IP enforcement: a **"Whole of Government"** and a **"Specialized Office"** approach. Each will be discussed in turn in the sections that follow.

1. The U.S. Model: A "Whole of Government" Approach to Intellectual Property Enforcement.

Entities that target and misappropriate trade secrets; systematically unlawfully exploit copyrighted content for commercial profit; or engage in the global trade of counterfeit, pirated or patent-infringing products have one thing in common: they take advantage of the lack of a coordinated government response. As a result, a "Whole of Government" approach—and its attendant enhanced *inter-agency* and *inter-institutional* coordination—to combat the unlawful exploitation or misappropriation of IP is key to achieving an effective enforcement environment.

A "Whole of Government" approach to IP enforcement seeks to break down silos that can exist amongst government agencies, maximizing appropriate collaboration. The approach leverages the resources, skills, and authorities of each individual governmental entity, and better ensures a comprehensive response to IP theft, as compared to an agency-by-agency approach that can often be fragmented. It also entails appropriate collaboration between government and private industry, trade associations, civil society—including consumer groups and labor unions—and other governments the world over.

The U.S. Government has adopted a "Whole of Government" approach for both an IP enforcement *policy coordination* standpoint and from an *operational enforcement* perspective. This Strategic Plan addresses each in turn, with the objective of illuminating these models domestically, as well as internationally, for purposes of continued support and development, in order to enhance collaboration in the global marketplace.

Whole-of-Government Approach to IP Enforcement Policy Coordination.

With regard to IP enforcement policy coordination, the "Whole of Government" approach is embodied, for example, in the Office of the Intellectual Property Enforcement Coordinator (IPEC).

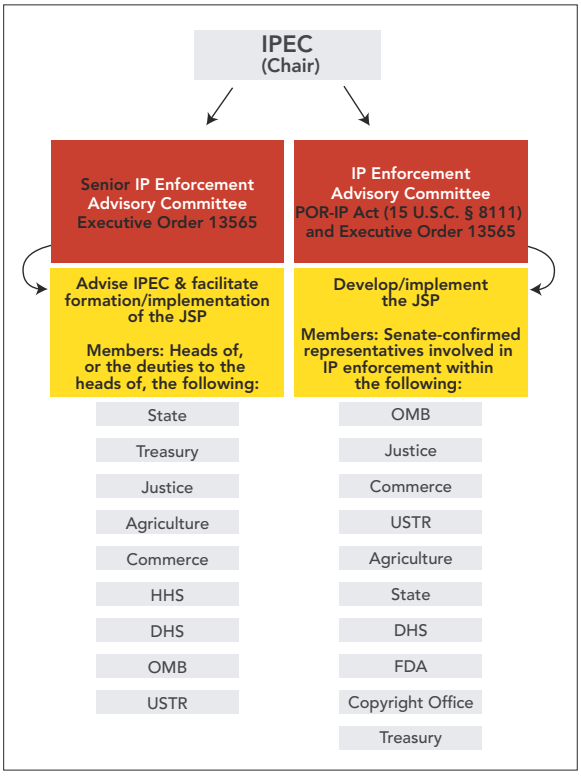
The IPEC was created by Congress in the PRO-IP Act of 2008. It is headed by the Intellectual Property Enforcement Coordinator, who is appointed by the President of the United States, and subject to confirmation by and with the advice and consent of the U.S. Senate. The IPEC was placed in the Executive Office of the President (EOP) to elevate the issue of IP enforcement, with particular emphasis on counterfeit and infringing goods, to the highest levels of the U.S. Government. Its placement in the EOP was also to coordinate the understanding of and approach to IP enforcement of each Government office and agency, where each agency has its own subject matter expertise and areas of responsibility—whether it be diplomacy, trade, criminal or civil law enforcement, etc. The IPEC coordinates the agencies identified in the PRO-IP Act to enable the agencies to work together to advance strategic, multi-disciplinary coherence at a national level.

The IPEC's responsibilities and authority are derived from two sources of law: (1) the PRO-IP Act of 2008, a Federal statute passed by Congress; and (2) Executive Order 13565 issued by President Obama in 2011. These authorities mandate the IPEC to chair the U.S. Interagency Strategic Planning Committees on IP enforcement and coordinate the interagency development of this Joint Strategic Plan.

Congress and the President found the establishment of the committees and the development of the Joint Strategic Plan necessary to coordinate the Government's work to reduce the proliferation of counterfeit goods and commercial-scale piracy and to enable the relevant agencies to work together more efficiently to identify impediments to effective IP enforcement both in the United States and internationally. In connection with the development of the Joint Strategic Plan, from its post in the EOP, the IPEC engages across the U.S. Government, with the private sector, other stakeholders, and with foreign governments, where appropriate, to coordinate this National strategy to protect U.S. IP from unlawful exploitation and theft.

The IPEC carries out this work principally through two mechanisms. First, the PRO-IP Act directs the IPEC to convene and chair an interagency *Intellectual Property Enforcement Advisory Committee*, composed of Senate-confirmed representatives as appointed by the heads of designated Federal departments and offices (FIG. 56) to develop and coordinate implementation of the Government's Joint Strategic Plan on IP Enforcement every three years.[1] Second, Executive Order 13565 empowers and directs the IPEC to convene and chair a *Senior IP Enforcement Advisory Committee*, composed of the "heads of, or the deputies to the heads" of designated Federal departments and offices (FIG. 56) who advise the IPEC and facilitate formation and coordinate implementation of the Joint Strategic Plan.[2]

FIG. 56



In addition to the two IPEC-chaired interagency committees, the IPEC has a formalized consultation role with two agencies: (1) with the USTR's Interagency Trade Enforcement Center for matters relating to the enforcement of U.S. trade rights involving IP pursuant to Executive Order 13601; and (2) with the Attorney General of the United States for reporting incidents of theft of trade secrets occurring abroad pursuant to the Defend Trade Secrets Act of 2016, 18 U.S.C. §1832. The IPEC also consults with the Department of Justice's Task Force on Intellectual Property, a department-wide initiative chaired by the Deputy Attorney General to confront the growing number of domestic and international IP crimes in a coordinated manner.[3]

Through these and other mechanisms, the United States seeks to bring broad coherence to IP enforcement policy at the national level, while minimizing duplication of efforts and affirmatively confronting shortcomings in IP enforcement. This "Whole of Government" model represents a conceptually straightforward framework to continue to advance coherence in the multi-disciplinary nature of IP enforcement and thereby increase governmental effectiveness in responding to illicit IP-based activities that undermine a variety of national interests. Opportunities exist to promote and support modern, whole-of-government frameworks internationally to enhance the effectiveness of the global response to the serious threats outlined throughout this Joint Strategic Plan.

Whole-of-Government Approach to Intellectual Property Law Enforcement Operations.

Alongside and complementary to the "Whole of Government" *policy coordination* approach to IP enforcement detailed above, the U.S. Government has also adopted a comprehensive and coordinated *operational* approach to combat IP-based crime. The "Whole of Government" *operational* approach is exemplified in the United States by the DHS/ICE-led IPR Center.[4]

The ICE IPR Center brings together 23 agencies (FIG. 57), consisting of 19 key Federal agencies, in addition to four international law enforcement partners (namely, INTERPOL, Europol, the Royal Canadian Mounted Police, and the Mexican Revenue Service (El Servicio de Administracion Tributaria, or SAT)) in a task force setting that allows for the sharing of law enforcement information and leads in real-time.

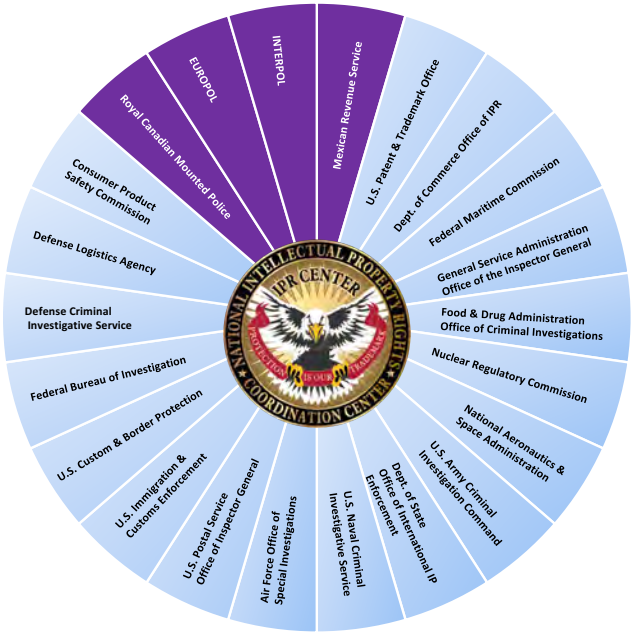
The ICE IPR Center relies on enhanced interagency and inter-governmental cooperation as well as engagement with the private sector. The task force structure enables the ICE IPR Center to share case-specific information in real time to combat IP crime and to leverage effectively the resources, skills, and

authorities of each participating agency and provide a comprehensive response to IP theft. The collaboration allows law enforcement to use resources as efficiently as possible by de-conflicting cases and using each agency's comparative advantage to most effectively conduct investigations.

The ICE IPR Center has facilitated development and deployment of several highly-effective targeted, multi-agency enforcement efforts, and has become an indispensable partner to CBP, the Department of Justice, and the Food & Drug Administration on the Federal side, and to the private sector that now has a single point of contact within the Federal Government for law enforcement matters affecting their IP-related law enforcement concerns.[5]

The "Whole of Government" approaches to IP enforcement at the *policy* and *operational* levels constitute important innovations in efforts to combat counterfeiting and commercial piracy at national and international levels. While there may be several factors that contribute to a given country's challenges in effective IP enforcement, it is worth noting that countries that lack meaningful intra-governmental coordination—either at the policy level, or operational level, or both—are often among the countries that are facing some of the most pressing challenges in the area of effective and efficient IPR enforcement.[6] There exist opportunities to further promote these

FIG. 57: IPR CENTER



"Whole of Government" frameworks with foreign government partners as part of an effort to increase the effectiveness of partnerships and collaborative strategies to combat IP crime.

Spotlight: California State Board of Equalization – TRaCE Task Force

The "Whole of Government" operational approach has also been adopted at the state level. For example, the State of California's Tax Recovery and Criminal Enforcement (TRaCE) Task Force is a program facilitated by California Assembly Bill 576, bringing together state and federal resources to collaboratively combat illegal business activities.

The TRaCE Task Force is comprised of investigators and special agents from multiple state agencies working together to investigate, prosecute and recover revenue lost to the underground economy covering a convergence of multiple threats, including the manufacture, importation, distribution, and sale of counterfeit and pirated products. By adoption of a coordinated approach, the TraCE Task Force has been able to combat IP crimes by effectively pursuing multiple criminal penalties that may apply to a given offense—for example, copyright infringement coupled with evasion of business, payroll and/or income taxes—to arrive at higher penalties.

Source: California's Tax Recovery and Criminal Enforcement (TRaCE) Task Force (http://www.boe.ca.gov/trace/)

Spotlight: USTR as "Whole-of-Government" Example

While the "Whole-of-Government" approach detailed above is multi-disciplinary in nature, within the specific discipline of *trade*, the USTR serves as an example of a "Whole-of-Government" approach to IP enforcement from a trade policy development and enforcement lens.

The USTR is the Cabinet member who serves as the President's primary advisor on matters of trade policy. As relevant here, the USTR is charged by Congress to engage the rest of the Federal Government to assess annually the state of IP protection and enforcement abroad. It does this interagency work through the Special 301 Review pursuant to Section 182 of the Trade Act of 1974 (19 U.S.C. § 2242) (as amended).

The USTR relies on the Trade Policy Review Group (TPRG) and the Trade Policy Staff Committee (TPSC), which are administered and chaired by the USTR and composed of 19 Federal agencies and offices (one of which is OMB, which includes IPEC). Through these and other mechanisms, the USTR works to (1) identify the effectiveness of our trading partners' protection and enforcement of IPR; (2) negotiate enforceable IP commitments with other countries; and (3) undertake specific enforcement actions to enforce trade-related IP rights.

As noted above, USTR also serves as a member of the Senior IP Enforcement Advisory Committee set forth in the PRO-IP Act, effectively reinforcing government-wide IP enforcement policy coordination.

2. The "Specialized Office" Approach to Intellectual Property Enforcement.

In addition to the "Whole of Government" approaches, another key government approach to successful IPR protection and enforcement is the IP enforcement "Specialized Office." This approach enables the application and evolution of substantive organizational expertise and knowledge that is needed to operate effectively in the face of the dynamic IP environment domestically and abroad. The "Whole of Government" and "Specialized Office" organizational structures are complementary, and indeed often overlap.[7] Both have proven highly effective in driving policy and operational improvements in IPR enforcement in the United States.

An IPR-specialized unit or task force develops a significant technical expertise and experience in IPR matters, and thereby is often well-positioned to develop strategically appropriate IP policies for its respective department. Indeed, vested with highly specialized expertise in areas of criminal exploitative IPR trends and tactics, for example, a "Specialized Office" may serve as an engine of policy development to address the evolving technological and legal landscape of IP enforcement. A "Specialized Office" does not operate alone and it materially benefits from the strength and resources of the home agency, which may carry a significant portion of the day-to-day workload. Rather, the focus is on a governmental framework that encourages a collaborative approach between specialized expert IPR units and the often larger home agencies whose support is necessary for achieving results.

In the U.S. Government, the Departments of Justice, State, and Commerce include several examples of specialized offices and programs that focus on, and are dedicated to, IPR protection and enforcement.

From a prosecution standpoint, one notable specialized unit is the **Computer Crime and Intellectual Property Section (CCIPS)** in the Justice Department's Criminal Division. CCIPS "is responsible for implementing the Department's national strategies in combating computer and IP-based crimes worldwide."[8] In addition, CCIPS works closely with the Justice Department's Computer Hacking and Intellectual Property (CHIP) network, which consists of Assistant United States Attorneys who are specially trained in the investigation and prosecution of IP and computer crimes.[9]

The Justice Department also operates the **Intellectual Property Law Enforcement Coordinator (IPLEC)** program, under which seasoned Justice Department prosecutors are stationed in select U.S. embassies and consulates overseas in order to: assess the capacity of law enforcement authorities throughout the region to enforce IPR; develop and deliver training and other capacity building formats to enhance the ability of justice sector personnel to enforce IPR; assist in developing or strengthening institutions dedicated to enforcing intellectual property rights; monitor regional trends in IP protection and computer crimes; and provide expert assistance in support of U.S. Government IP and computer crime policies and initiatives in the region.[10]

FIG. 58: Example of International "Specialized Office" Approach.

Europol and the European Union Intellectual Property Office (EU IPO) joined forces on July 2016 to launch the "Intellectual Property Crime Coordinated Coalition" (IPC3).



The IPC3 serves as a highly-specialized, IP-dedicated resource within Europol that enjoys broad transnational reach as it supports several international operations targeting counterfeiting and piracy. IPC3 provides operational and technical support to law enforcement agencies and other partners in the EU and beyond by facilitating and coordinating cross-border investigations and enhancing the harmonization and standardization of legal instruments and operating procedures to counter IP crime globally.

Source: Europol

Supporting state and local law enforcement is also critical to combating IP theft. In coordination with the Department of Justice Task Force on Intellectual Property, the Office of Justice Programs (OJP) initiated the Intellectual Property Theft Enforcement Program (IPEP) in 2009, which is designed to build the capacity of state and local criminal justice systems to address criminal IP enforcement through increased prosecution, prevention, training, and technical assistance availability. The program is administered by the Bureau of Justice Assistance (BJA), a component of OJP. Since IPEP's inception, OJP has awarded $22,077,022 in program grants, pursuant to Section 401 of the PRO-IP Act, which authorizes OJP to make grants to eligible state or local law enforcement entities for training, prevention, enforcement, and prosecution of IP theft and infringement crimes. Under the program, grant recipients establish and maintain effective collaboration and coordination between state and local law enforcement, including prosecutors and multijurisdictional task forces, and appropriate Federal agencies, including the FBI and United States Attorneys' Offices. The information shared under the program includes information about the investigation, analysis, and prosecution of matters involving IP offenses as they relate to violations of state and local criminal statutes. State and local enforcement agencies have received $16,785,348 in Federal support to date.

In addition to supporting and increasing coordination and cooperation of enforcement efforts among federal, state, and local law enforcement entities, IPEP funds national training and technical assistance (TTA) and public education campaigns. The National White Collar Crime Center (NW3C) is the TTA provider for IPEP. TTA for state and local law enforcement focuses on supporting the training needs of the local IP offices and providing continuing education for the greater law enforcement community on promising IP crime investigative and prosecutorial practices, health and safety issues resulting from counterfeit products, negative economic ramifications of IP crime, and the connection between IP crime and organized crime, gangs, and terrorism.

The FY 2005 Department of State Appropriations Act elevated the State Department's Intellectual Property Division (within the Bureau of Economic and Business Affairs) to office-level status and renamed it as the **Office of International Intellectual Property Enforcement,** with the goal of enhacing U.S. Government responsiveness to industry's growing need for IPR protection abroad. The office works closely with U.S. diplomats serving abroad to ensure that the interests of American rights holders are represented overseas and to highlight the integral role that IPR protection plays in supporting innovation, global economic growth, and the rule of law.[11]

In addition, the Department of Commerce has established the **Office of Intellectual Property Rights** within the International Trade Administration, an entity

FIG. 59



Source: U.S. Department of Justice, Bureau of Justice Assistance
Additional details available at: https://www.bja.gov/ProgramDetails.aspx?Program_ID=64#horizontalTab2

which works to advance IPR enforcement interests in domestic and international forums through its participation in interagency and intergovernmental working groups.[12]

Two other prominent examples of specialized offices are the main U.S. IP agencies, namely, the **U.S. Patent and Trademark Office (USPTO)** and the **U.S. Copyright Office.** While all U.S. trading partners similarly enjoy patent, trademark, and copyright-focused offices ("Intellectual Property Offices," or IPOs), not all countries fully utilize the IPO's subject matter expertise beyond internal, office-based practices.

The USPTO and the U.S. Copyright Office are active participants in helping to develop effective IPR enforcement policies for the United States. In the United States, the USPTO is responsible for advising the President, through the Secretary of Commerce, on National and certain international IP policy issues. In addition, the USPTO is responsible for advising Federal departments and agencies on matters of domestic and international intellectual property policy, including patents, trademarks, copyrights, and trade secrets.[13]

Within the USPTO, the Office of Policy and International Affairs (OPIA) has primary responsibility for analyzing, developing and advocating intellectual

2015 Forum: "Promoting IPR Enforcement Policy in Latin America: The Role of the IPO"

In April 2016, the White House Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC) and the Mexican Institute of Industrial Property (IMPI) co-hosted an event that brought together senior leadership from IP offices (IPOs) representing 12 countries—Belize, Brazil, Chile, El Salvador, the Dominican Republic, Guatemala, Mexico, Paraguay, Panama, Peru, Uruguay and the United States—for the first-ever forum of its kind on enforcing intellectual property rights (IPR) in Latin America.

The forum explored the role of the Latin American IPOs in promoting IPR enforcement and policy on the national level in order to produce a set of recommendations for participants on implementing these strategies in their respective jurisdictions.

See International Trademark Association, "Workshop Fosters Collaboration Among Latin American IP Offices on Enforcement" (May 1, 2016) accessed from http://www.inta.org/INTABulletin/Pages/IP_Office_Workshop_7108.aspx

property policy, through its teams of policy experts in all areas of IP, including patents, trademarks, copyrights, trade secrets and enforcement.[14] OPIA coordinates policy positions taken by the USPTO for the Office of the Under Secretary and Director, working with other components of the USPTO as relevant. OPIA provides leadership and expertise in international negotiations for the United States on non-trade related intellectual property matters, including at the World Intellectual Property Organization, and serves as advisors to USTR in trade negotiations. It also provides intellectual property training and education through its Global Intellectual Property Academy, economic research through its Office of Chief Economist, and legislative development through its Office of Governmental Affairs. These efforts are further advanced by its **Intellectual Property Attaché Program**, which stations IP experts in U.S. embassies, consulates and missions around the world who work to improve IP systems internationally for the benefit of U.S. stakeholders.[15]

The Office of Policy and International Affairs, within the Copyright Office, assists the head of the Copyright Office (the Register of Copyrights) with domestic and international policy analyses, legislative support, and trade negotiations. It also represents the Copyright Office at meetings of government officials concerned with the international aspects of copyright protection.[16]

International cooperation on enforcement between the specialized U.S. offices focused on IP and their foreign counterparts is an important component of U.S. enforcement strategy, whether it be to share and promote best practices for IP enforcement or to support foreign IPOs' efforts to serve as catalysts for policy review across their governments to help make IPR-related improvements in enforcement as warranted.

Coordination at the policy and law enforcement operational levels—combined with specialized offices working in tandem with other government offices with broader mandates—ensures a comprehensive, coherent government approach to effective IP enforcement domestically and abroad. Opportunities exist to promote, expand and further support these models in the United States, as well as in other countries. By promoting and supporting modern governmental frameworks for IPR enforcement, the United States and other countries may more effectively work to minimize weaknesses in the global IP enforcement regime, increase the effectiveness of IPR enforcement activities, and remain responsive to rapidly changing environments and criminal tactics.

ACTION NO. 4.1: Promote domestic support of "Whole of Government" and "Specialized Office" approaches to IPR protection and enforcement. The U.S. Interagency Strategic Planning Committees on IP Enforcement will explore opportunities for enhanced support and expanded adoption of the discussed "Whole of Government" and "Specialized Office" approaches to IPR protection and enforcement both within the Federal Government and by State governments. The U.S. Interagency Strategic Planning Committees on IP Enforcement will identify opportunities to promote, enhance support for, and/or expand these organizational models domestically. In identifying such opportunities, due consideration will be given to steps requisite to implement the recommended approach, and what Federal or state resources are available to support successful deployment of the "Whole of Government" model.

ACTION NO. 4.2: Promote and support foreign governments' adoption of "Whole of Government" and "Specialized Office" approaches to IPR protection and enforcement. IPEC will coordinate with the other offices and agencies of the Federal government who serve on the U.S. Interagency Strategic Planning Committees on IP Enforcement to identify opportunities to actively promote abroad, where appropriate, the "Whole of Government" and "Specialized Office" approaches to IPR protection and enforcement, exploring appropriate opportunities for enhanced support and expanded adoption by trading partners. The Committees will consider opportunities to work with foreign governments as well as with regional, international, and non-governmental organizations (NGOs), and industry associations to promote these approaches as best practices for the enforcement of IPR worldwide.

B. ENHANCE CAPACITY-BUILDING, OUTREACH, AND TRAINING PROGRAMS ON INTELLECTUAL PROPERTY ENFORCEMENT IN OTHER COUNTRIES.

As described in more detail in the opening pages of this Strategic Plan, illicit IP-based activities stretch across the globe and are not confined within national boundaries. For example, traffickers of counterfeit goods may manufacture fakes in one country, exploit another country for purposes of transiting and re-labeling the counterfeit goods, and target numerous other countries as markets for consumption. Actions that unlawfully exploit copyrighted content or patents, or misappropriate trade secrets, often have an international footprint as well.

The global nature of these and other IP-based illicit activities necessitates an IPR strategy that involves enhanced international collaboration, including supporting the capabilities of other governments to engage in effective IP enforcement.

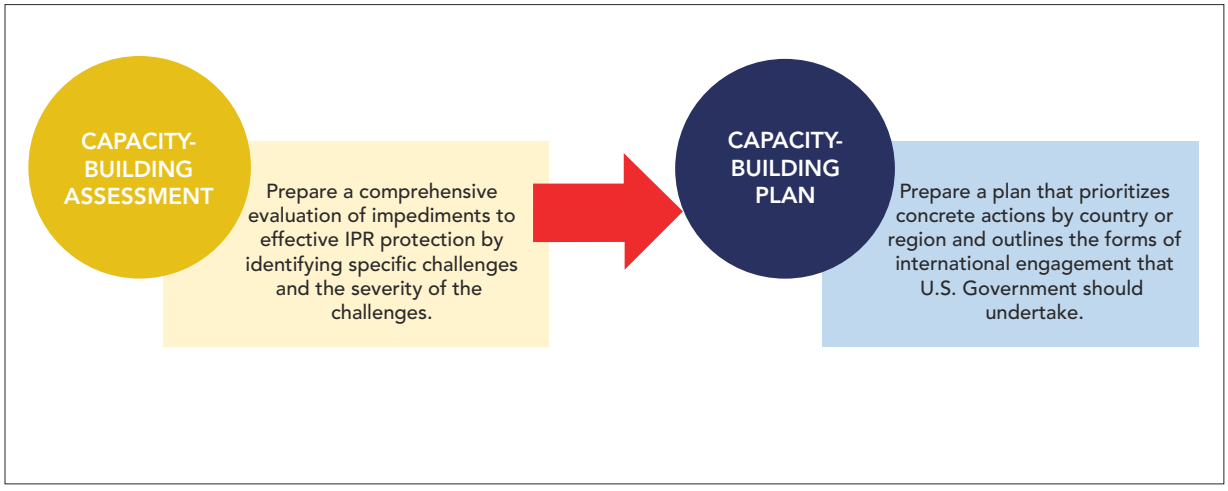
For the reasons outlined in this Strategic Plan, the adequate and effective protection of intellectual property rights is an important priority in U.S. economic foreign policy. Transparent and effective intellectual property systems provide stable expectations that facilitate foreign direct investment and trade in the kinds of products and services that result in voluntary transfer of technology and skills. The United States Government is continuously working with foreign countries, as appropriate, to address specific deficiencies or embrace best practices in intellectual property protection. This engagement ranges from formal economic dialogues to collaboration in multilateral organizations to bilateral work through our Embassies and foreign commercial services officers or Department attaches all over the world. Different countries face different challenges and opportunities, and U.S. economic engagement is tailored to our broader relationship with each country.

A deliberate and strategic approach to capacity-building, outreach, and training is a necessary ingredient for the U.S. Government's international engagement to be effective in strengthening the abilities of other countries to meaningfully protect IPR. The discussion of how to promote this coordination within foreign governments abroad should be understood in the context of (i) a **Capacity-Building Assessment**, comprised of a comprehensive evaluation (on a country-by-country, regional, or other basis that reflects domestic priorities) of the specific nature and severity of the impediments to effective IPR protection; and (ii) a **Capacity-Building Plan** that prioritizes and outlines the forms of international support that the U.S. Government should undertake in relation to capacity-building.

A review of capacity-building, outreach, and training efforts during the two years immediately preceding this Plan[17] revealed that opportunities exist to continue to better understand and evolve how U.S. collaboration may be most effective in the short- and long-term.

At the most fundamental level, IP-related **Capacity-Building** exercises are carried out with the objective to help enhance a country's *operational effectiveness* in IPR protection and enforcement, as well as forward-looking discussions and consultations that assist governments upon request as they contemplate new laws, regulations, or policies, as appropriate.

FIG. 60



Spotlight: International Cooperation and Information Sharing in Action

There are many examples of effective international cooperation in IPR protection and enforcement, including bilateral and multi-lateral dialogues and frameworks, including by way of the Department of Homeland Security's *National Intellectual Property Rights Coordination Center* ("IPR Center") and *Europol's Intellectual Property Crime Coordinated Coalition* (IPC3). From worldwide scans of international mail for illicit pharmaceuticals sold over the Internet[18] to seizures of counterfeit contaminated food and drink products in the retail supply chain,[19] coordinated international enforcement efforts make significant headway against illicit trade, build relationships amongst enforcement officers that support productive sharing of data and trend analysis, and offer government agencies the opportunity to observe their counterparts' novel approaches to difficult enforcement challenges.

Due to the transnational nature of illicit IPR-based threats, international engagement focused on **Cooperation and Information Sharing** is also important. This tier of engagement does not focus on the type of assistance described above. Rather, it focuses on ensuring that government IPR enforcement agencies and personnel have the necessary data and relationships to effectively spot trends, address challenges with international dimensions, and maximize the impact of domestic resources and operations by offering opportunities to form regional and global partnerships under existing laws and legal structures. Cooperation and information sharing between countries is critical for effective IPR protection and enforcement. Greater effort is needed to promote cooperation and joint operations, as well as enhanced structured dialogue between stakeholders and governmental entities.

Opportunities exist to strengthen capacity-building, cooperation, and information-sharing between countries on IP enforcement. These opportunities must continue to be pursued in a deliberate and strategic manner.

ACTION NO. 4.3: Develop a comprehensive assessment for capacity-building and/or cooperation on IP enforcement in appropriate countries or regions. Guided by the list of countries identified by USTR under 19 U.S.C. § 2242(a), the relevant members of the U.S. Interagency Strategic Planning Committees on IP Enforcement will assess some of the challenges to effective IPR protection and enforcement, as appropriate. The assessment will include a discussion of whether the identified challenges would be best addressed through enhanced capacity-building, cooperation and information sharing, or by other means.

ACTION NO. 4.4: Coordinate IP enforcement capacity-building programs that are responsive to the findings of the capacity-building assessments. In following up on these assessments, the government programming will include:

- attention to those countries that have been identified as appropriate for capacity building and assistance;
- focus on those countries for which the provision of capacity-building support is likely to result in a meaningful improvement in their level of IPR enforcement;
- consideration of the challenges faced in a particular country with respect to improving its level of IPR enforcement;
- consideration to avoid duplication of other IP enforcement-related capacity-building support that the agency, or another agency, has already provided to that country. In addition to coordination through the U.S. Interagency Strategic Planning Committees on IP Enforcement, all agencies delivering IP enforcement-related training and capacity-building programs may consider cost-effective collaborative efforts in planning such programs to prevent undue duplication. Such measures could include, for example, that the agency continues to co-sponsor and support other IP enforcement capacity-building programs, and that the agency provides forward-looking or summary quarterly submissions of accurate and up-to-date information through the Global Intellectual Property Education Database, at http://usipr.uspto.gov.[20]

ACTION NO. 4.5: Continue ongoing implementation of capacity-building assessments. Relevant Federal departments and agencies will endeavor to include and implement appropriate actions in their strategic plans on IPR

protection and enforcement for the designated country or region, including making resource allocations as appropriate, for carrying out their international engagements through capacity-building, cooperation and information sharing, and other means.

ACTION NO. 4.6: Enhance opportunities for information sharing with foreign governments. The U.S. Interagency Strategic Planning Committees on IP Enforcement, in consultation with such other agencies and offices as may be appropriate, will coordinate as appropriate to identify areas in which prospective sharing of information between the United States and a foreign government that is not currently underway may materially enhance the Federal Government's ability to enforce U.S. IPR domestically and abroad.

C. PROMOTE ENFORCEMENT OF U.S. INTELLECTUAL PROPERTY RIGHTS THROUGH TRADE POLICY TOOLS.

America's trade policy has a significant impact on the strength and growth of the U.S. economy and the livelihood of millions of Americans. Ninety-five percent of the world's consumers live outside U.S. borders. Our Made-in-America products and services are in demand, making American exports a vital pillar of our 21st century economy.

Exports play an indispensable role as a driver of the U.S. economy. In 2015, the U.S. realized a record in volume of American exports for the fifth year in a row, selling $2.34 trillion in goods and services abroad.[21] When taking a closer look at the nature of U.S. exports, we see that intellectual property (IP) intensive industries account for approximately $842 billion (in 2014), or more than 50 percent of total U.S. merchandise exports.[22] Our exports, as well as our domestic economy, are fueled by the technological innovation and output from our creative sectors. From household brands to the music and movies that inspire us, and the technologies and innovation we rely on each day, American ingenuity serves as a foundation upon which we grow our economy and contribute to the world around us. Protection of the intellectual property rights behind these exports remain an important U.S. Government priority.

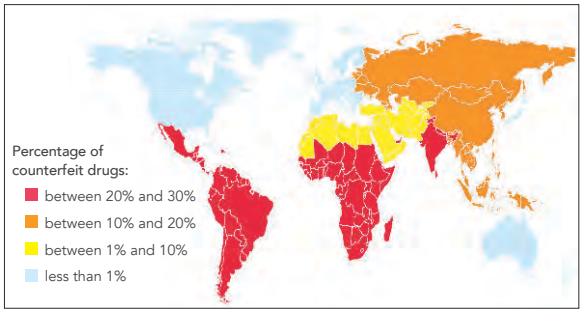
As discussed in greater detail in Section I, these exports support U.S. business and higher-paying jobs. In order to support exports, our trade policy promotes open markets and a fair, level playing field for trade. Our trade policy must also promote high standards that support the rule of law and our country's values.

> One prominent study found that if IPR protection in China were improved to a level comparable to the United States, U.S. net employment may increase by 2.1 million jobs and American companies would benefit from an estimated $107 billion in additional annual sales.
>
> *Source: U.S. INTERNATIONAL TRADE COMMISSION, Report on China and the Effects of Intellectual Property and Indigenous Innovation Policies on the U.S. Economy (Investigation No. 332-519)*

Illicit IP-related activity—in addition to undermining opportunities in the marketplace—imposes significant negative social costs. As noted throughout this Strategic Plan, trade in counterfeit goods, for example, introduces significant risks into global supply chains, subverts human rights (by reliance on forced labor, child labor, or sweatshop-like working conditions), threatens individual health by causing or failing to treat serious illnesses, and can generate environmental disasters by way of unregulated manufacturing conditions or use of unregulated products, all the while proceeds of illicit trade flow to criminal syndicates who undermine rule of law in a variety of ways.[23]

These threats and abuses of the rule of law are not limited to, or self-contained within, developed economies. It must not be overlooked that the attendant harms associated with illicit trade are often felt by

FIG. 61: A Worldwide Issue, With Disproportionate Geographic Impact



Source: European Commission, at http://ec.europa.eu/internal_market/indprop/docs/conf2008/wilfried_roge_en.pdf.

developing countries, as well.[24]

Low- and middle-income countries, and those in areas of conflict or civil unrest, face considerable difficulties in securing their supply chains from illicit trade in counterfeit and pirated goods, and as a result, criminal networks target, corrupt, and work to actively undermine such markets. By way of example, an enforcement operation organized by the World Customs Organization in partnership with the Institute of Research against Counterfeit Medicines (IRACM) (*Operation Vice Grips 2*) was conducted simultaneously at 16 major African seaports in July 2012, with 110 maritime containers being inspected. Of these, 84 containers (or 76 percent) "were found to contain counterfeit or illicit products," resulting in "the seizure of more than 100 million counterfeit products of all categories."[25] These and other disproportionate effects in vulnerable markets must be addressed collaboratively by the international community, and trade policy must bridge regulatory and enforcement gaps between developed and developing economies.

The Office of the U.S. Trade Representative, in coordination with the U.S. interagency, uses U.S. trade policy tools to support U.S. exports, integrity in the global marketplace, and effective enforcement of U.S. intellectual property rights including: (1) the promotion of strong IP standards, consistent with U.S. law, in the drafting, negotiation, monitoring, and enforcement of international trade agreements and in bilateral and multilateral dialogues with U.S. trading partners; (2) the annual "Special 301" review of the global state of intellectual property rights protection and enforcement to encourage and maintain enabling environments for innovation and investment; and (3) the "Out-of-Cycle Reviews of Notorious Markets" to increase public awareness of and guide related trade and other enforcement actions in physical and online markets that exemplify global counterfeiting and piracy concerns.

To combat the intellectual property crimes and enforcement shortcomings in the international marketplace, the USTR annually assesses the state of IP protection and enforcement abroad in the Special 301 Review pursuant to Section 182 of the Trade Act of 1974, as amended (19 U.S.C. § 2242).[26] This review allows for various designations of countries, including as a "Priority Watch List" country or a "Watch List" country. The USTR works proactively with various trading partners to address the concerns raised in the Special 301 report.

Trade agreements and strong enforcement tools are necessary in order to set high standards that support the rule of law. Through such effective trade policy tools and agreements, we work to ensure that our workers, our businesses, and our values are shaping globalization and the 21st century economy.

ACTION NO. 4.7: Use Special 301 tools to address international IP and trade challenges. USTR, in collaboration with Federal agencies, will continue to review IP protection and enforcement frameworks of our trading partners and identify challenges to effective protection and enforcement of IPR, and obstacles to market access for U.S. persons that rely on IP protection.

CHINA IN FOCUS: A SNAPSHOT VIEW OF IPR POLICIES AND PRACTICES

> "Effective IPR enforcement remains a serious problem throughout China. IPR enforcement is hampered by lack of coordination among Chinese government ministries and agencies, lack of training, resource constraints, lack of transparency in the enforcement process and its outcomes, procedural obstacles to civil enforcement, and local protectionism and corruption."
>
> *USTR Report to Congress on China's WTO Compliance (Dec. 2015), p. 120*

As detailed by the U.S. Government in annual IPR-related reporting, China's weak protection of intellectual property presents serious implications for global commerce. Between FY 2005 and FY 2015, the Department of Homeland Security seizures related to intellectual property right (IPR) violations leapt from 8,022 to 28,865, with products originating in China and Hong Kong (often used as a transit point from goods originating from the mainland) accounting for 83% of all IPR seizures in 2015. These violations of intellectual property rights cause significant business losses, undermine U.S. competitiveness in the world marketplace, undermine the rule of law, and in many cases, threaten public health and safety, among other attendant harms.

China has undertaken a wide-ranging revision of its framework of laws and regulations aimed at protecting the intellectual property rights of domestic and foreign right holders. However, inadequacies in China's IPR protection and enforcement regime continue to present serious barriers to U.S. exports and investment and to affect our markets at home.[27] The U.S. Government again placed China on the 'Priority Watch List' in USTR's Special 301 report, and several Chinese markets were among those included in USTR's 2015 Notorious Markets List, which identifies online and physical markets that exemplify key challenges in the global struggle against piracy and counterfeiting.

China continues to present a complex and contradictory environment for protection and enforcement of IPR. Welcome developments include repeated affirmation of the importance of intellectual property by China's leadership, an ongoing intellectual property legal and regulatory reform effort, and encouraging developments in individual cases in China's courts.

At the same time, progress toward effective protection and enforcement of IPR in China is undermined by unchecked trade secret theft, market access obstacles to ICT 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 is a leading concern for businesses operating in China, as intellectual property infringements are difficult to prevent and remediate, and may cause businesses to choose not to invest in China or offer their technology, goods, or services there.

As the USTR reports indicate, China's IPR-related policies and practices cause particular concern for the United States and U.S. stakeholders across a wide variety of areas, including, but not limited to trade secrets, ICT policies, technology transfer requirements and incentives, widespread piracy and counterfeiting in China's e-commerce markets, software legalization, counterfeit goods, technical standards involving IPR, anti-monopoly law enforcement, and IPR protection for pharmaceutical innovations.

At the same time there have been some positive developments. In the context of Chinese President Xi Jinping's September 2015 visit to Washington, D.C., the United States and China made a seires of cyber commitments, including that neither state would engage in the cyber-enabled theft of intellectual property for commercial gain. Since that commitment, we have seen

a number of other countries seek and reach agreement with China on similar commitments of their own, including Germany and the United Kingdom. Adherence to the U.S.-China bilateral cyber commitments is an important part of the overall U.S.-China relationship, and it is reviewed through the year, including during the semi-annual meetings of the U.S.-China High Level Joint Dialogue on Cybercrime and Related Issues.

Further, as noted in other U.S. Government reports,[28] recent examples include, in 2015, China's leadership continued to affirm the importance of developing and protecting intellectual property and emphasized that stronger protection and enforcement of IPR are essential to achieving China's economic objectives. China expressly committed not to "conduct or knowingly support misappropriation of intellectual property, including trade secrets and other confidential business information with the intent of providing competitive advantages to . . . [its] companies or commercial sectors." China also committed not to "require the transfer of intellectual property rights or technology as a condition of doing business . . . ." As part of its legal reform effort, China continued to develop draft measures on a wide range of subjects, including on copyright, patents, trade secrets, drug review and approvals, anti-monopoly law enforcement as it relates to intellectual property, and regulations on inventor remuneration. To date, the proposed reforms include many welcome changes but also aspects that are of great concern. China continues to review its Copyright Law, and revisions aligned with international norms and best practices would put China on a stronger footing to encourage growth in, and investment by, industries relying on copyright protection. Another positive development is that the Office of the National Leading Group on the Fight Against IPR Infringement and Counterfeiting, established by the State Council and chaired by China's relevant Vice Premier, continues to play an important and positive role in intellectual property, and it extended its online enforcement campaign into 2015. Also welcome is China's three-year pilot program to study the merits of specialized intellectual property courts, currently including courts in Beijing, Shanghai, and Guangzhou. However, given the high levels of counterfeiting and piracy in China, more needs to be done.

Relevant U.S. agencies will continue to engage China constructively by way of informal and formal meetings and dialogues, including the U.S.-China Strategic and Economic Dialogue (S&ED), the U.S.-China Joint Commission on Commerce and Trade (JCCT), and other engagements between our IP, enforcement and innovation agencies to ensure effective enforcement, non-discriminatory treatment and a fairer market for U.S. rights in China.

D. SUPPORTING INNOVATION AND TECHNOLOGICAL ADVANCEMENTS: THE NEED FOR TOOLS FOR EFFECTIVE AND PREDICTABLE PATENT PROTECTION DOMESTICALLY AND ABROAD.

Patent-intensive industries are a driving force in the U.S. economy. According to a recent Department of Commerce report, the value added by patent-intensive industries in 2014 was $881 billion, which was 5.1 percent of U.S. gross domestic product.[29] Supporting efficient and predictable patent protection policies that promote investments in research and development is key to the continued growth of innovative economies.

Without effective mechanisms to protect intellectual property rights, including patents and trade secrets, competitors could simply sit back and copy, rather than invest the time and resources required to invent and innovate. Research and development would be even riskier investments, with little to no assurance that such investments would or could be commercially put into use. Simply put, facilitating efficient and predictable patent protection policies harnesses the drive and ingenuity of our innovators and helps ensure that our economy remains innovative and competitive.

1. Enhancing Domestic Patent Protection.

Balanced policies that support strong patent rights and reward innovation and entrepreneurship, while minimizing the occurrence of abusive patent litigation, are key to an effective patent system.

As USPTO leadership has underscored,[30] patent quality is central to fulfilling the purpose of the U.S. patent system, which as stated in the U.S. Constitution is to "promote the Progress of Science and useful Arts."[31] High quality patents promote efficient licensing, investment in research and development, and future innovation. Patent owners and the public benefit from having clear notice of the boundaries of the issued patents.

USPTO's Enhanced Patent Quality Initiative plays a fundamental role in institutionalizing best practices associated with patent quality at all stages of the patent examination process.[32] The initiative, among other advantages, raises Patent Examiners' awareness of available search tools, improves resources to identify relevant prior art, identifies best practices to enhance the clarity of prosecution records, and captures data about the correctness and clarity of Patent Examiners' work products that will facilitate future decision-making. Quality examination practices at the outset is key to building confidence in the patent system and promoting innovation.

Supporting the development of high quality patents also has the additional benefit of helping to reduce issues that can lead to costly and often needless litigation. There has been significant attention focused during recent years on reportedly abusive patent litigation tactics by way of certain companies, commonly referred to as Patent Assertion Entities (PAEs) or Non Practicing Entities (NPEs). It has been reported that abusive litigation tactics can be used to threaten companies to extract unwarranted licensing fees or settlements based on patent claims that may be deemed inapplicable or invalid if subject to legal scrutiny.[33]

Shortly prior to the issuance of this Strategic Plan, the Federal Trade Commission issued a report—*"Patent Assertion Entity Activity: An FTC Study"*—examining non-public information and data covering the period 2009-2014 from entities using the agency's authority under Section 6(b) of the FTC Act.[34] The FTC report spotlights the business practices of PAEs, and provides an enhancement of our understanding of PAEs with additional empirical foundation for ongoing policy discussions.

The U.S. patent system has undergone a number of significant changes in recent years which have focused on reducing abusive litigation tactics in the patent space. These changes include U.S. Supreme Court rulings affecting patent-eligible subject matter; the implementation of new post-grant review procedures at the USPTO established by the America Invents Act (AIA); changes to the Federal Rules of Civil Procedure which raised the pleading standards for patent cases; adoption of local model rules to better manage patent litigation; and U.S. Supreme Court rulings regarding the award of attorneys' fees.[35]

The AIA represents the most significant legislative change to the U.S. patent system since 1952, and established a unique forum to potentially curb abusive patent litigation.[36] The Patent Trial and Appeal Board (PTAB), created under the AIA, reviews the patentability of claims challenged by accused infringers in AIA trial proceedings. By challenging the patentability of patent claims being asserted by PAEs at the PTAB, stakeholders can take affirmative steps to curb abusive patent litigation practices. The USPTO continues to engage with stakeholders on how to further develop the PTAB rules and procedures to make it a more effective and fair alternative to the costly and arduous litigation procedures of traditional courts, and the PTAB is already producing tangible results.

In addition, an amendment to the Federal Rules of Civil Procedure (which went into effect in December 2015) has raised the pleading standards for patent cases. As a result, plaintiffs will need to do more than simply provide defendants notice of infringement claims. Parties alleging patent infringement now need to adhere to the requirements set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), which require a complaint to allege "sufficient factual matter, accepted as true, to state a claim that is plausible on its face" and "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged" (*Iqbal*, *id.* at 678).

New technologies continue to challenge the patent system. Continued prospective analysis and stakeholder collaboration on how emerging technologies may impact the patent landscape is an important USPTO priority. The USPTO implements a multi-prong approach for addressing issues related to emerging technologies including: (1) enhancing patent quality by delivering expert technical training on emerging technologies to patent examiners through its Patent Examiner Technical

Training Program (PETTP) and other initiatives; (2) providing inter-agency leadership and technical expertise on emerging technology initiatives; and (3) facilitating discussions with stakeholders on the impact of emerging technologies on the patent system. The USPTO is closely monitoring the intellectual property implications of technologies such as additive or "3D" printing, the "Internet of Things," and blockchain.

The goal is to carefully monitor the impacts of recent changes to the U.S. patent system, coupled with the continued collection and review of empirical data, to assess policy options that balance the important needs of patent holders with the goal of reducing truly frivolous litigation.

ACTION NO. 4.7: Continue implementation of the Enhanced Patent Quality Initiative. USPTO will continue implementation of its Enhanced Patent Quality Initiative and seek input from stakeholders on ways to further improve correctness, clarity and consistency of patent examination. USPTO will use stakeholder input, as well as data collected and lessons learned from implementation of the initiative, to promote continuous process improvement.

ACTION NO. 4.8: Promote continued collaboration between rights holders and the USPTO to benchmark post grant proceedings. Benchmarking post grant proceedings under the AIA will help stakeholders understand the changing landscape of patent litigation and how patents are being challenged and evaluated. USPTO will continue investing in a data driven strategy when evaluating the effectiveness of the new post grant proceedings and reforms to the PTAB.

ACTION NO. 4.9: Promote continued training and dialogue regarding emerging technologies on the patent system. USPTO, with assistance from stakeholders, will continue to deliver expert technical training on emerging technologies to patent examiners. The USPTO will also continue to lead and provide technical expertise on inter-agency initiatives related to emerging technology and create new avenues for dialogue with stakeholders on the impact of emerging technologies on the patent system.

ACTION NO. 4.10: Provide expert technical assistance to Congress on any necessary patent reform efforts. USPTO, in coordination with the White House and other Executive Branch agencies, will continue to provide expert technical assistance to Congress in support of patent reform efforts, with the goal of promoting targeted, balanced improvements, as necessary, that curtail abusive patent litigation practices while maintaining robust patent enforcement.

2. Enhancing Domestic Design Protection.

Balanced policies that support strong industrial design rights and reward ornamental innovation and entrepreneurship are key to an effective design patent system, and contribute to a strong economy.

Over the past years, new and emerging industrial designs have gained prominence in the commercial market. Graphical user interfaces (GUIs), icons, transitional images, and animated images embodied in articles of manufacture are routinely the first level of user interaction that drive purchases and success of many consumer products today. The USPTO, with assistance from stakeholders, is reviewing legal frameworks and office practices to meet user needs to protect designs embodied in these and other emerging technologies and to identify where legal frameworks and office practices could be enhanced.

Technical advances, such as the growing prevalence of 3D printing, electronic transmissions and virtual reality, also impact the enforcement of design rights. It remains uncertain how some designers can rely on the current industrial design legal framework to effectively enforce their rights in light of these emerging technical means for infringement. The USPTO recognizes these impending challenges and consults with the public to identify legal and procedural gaps that may require action by courts, Congress, the USPTO or others.

USPTO's Enhanced Patent Quality Initiative includes a program designed to enhance domestic design protection. The Design Patent Publication Quality program seeks to improve the quality of drawings in published design patents. Degradation of finally printed patent grant images, relative to their incoming patent application images, is significant in design patents especially because the drawings define the claimed invention.

ACTION NO. 4.11: Monitor the use of the design patent system to protect designs embodied in or applied to technologies. USPTO will continue to consult with designers and other stakeholders and monitor the current legal framework as it pertains to protecting designs embodied in new and emerging technologies.

3. Enhancing the Effectiveness of Patent Systems Abroad.

As U.S. companies continue to expand into foreign markets, it is important for the U.S. to promote strong and effective patent protection and enforcement worldwide, reflecting the importance of patents to innovation and economic growth. A wide range of tools should be used to identify opportunities and challenges facing U.S. innovative industries in foreign markets. Some examples include:

a. Reducing Patent Pendency.

Patentees face a number of challenges around the world, including significant time lapses between the filing of patent applications and the issuance of patents (the "patent pendency" period). Long patent pendency periods can substantially curtail the effective term of the patent, diminishing its value and effectiveness as an incentive for innovation and investment.

Long patent pendency periods reduce incentives for investment in research and development efforts, hinder innovation, and hamper job growth prospects.[37] Shortening the patent pendency period can assist the patent holder to timely commercialize or otherwise obtain value from the exclusive right for the technology, thereby increasing the value of the patent. Also, shortening the patent pendency period reduces uncertainty for third parties, including the public, regarding the scope and enforceability of any patent that may eventually issue.

While many of the underlying problems leading to long pendency periods in some countries can only be corrected by that country's government (*e.g.*, by adequately funding the patent office to permit needed hiring of patent examiners and to upgrade facilities and processing systems), opportunities exist to improve patent examination efficiency through streamlining of the international patent system. The international patent system, as it currently stands, includes considerable redundancy. Because patent rights are territorial, innovators must obtain patents separately in each country where they want the invention protected. This means that the innovator must file separate, substantially identical patent applications in each country, and those countries' patent offices must then separately examine those same applications.

Government policies must support efficient patent systems around the world that benefit domestic and foreign innovators and contribute to economic growth. For example, improved operations of patent offices, including such actions as the digitization of records, upgrading online search and e-filing capabilities, and hiring adequate patent examiners remain attractive opportunities for enhancing patent systems. The USPTO has been meeting since 2007 with its counterparts from Europe, Japan, Korea and China (known as the "IP 5") to explore approaches for enhancing cooperation on patent administration issues. According to WIPO statistics, the IP5 offices receive almost 80 percent of all patent applications filed worldwide, and as a result, improved practices and systems among the "IP 5" may lend themselves to global adoption.[38]

To streamline the patent system and avoid duplication of examining efforts, the USPTO and several other offices around the world are engaged in "work sharing" cooperation. The idea behind work sharing is that one patent office can reuse the work another patent office has already done in examining the same application to speed up its own examination. The USPTO's primary work sharing vehicle is the "Patent Prosecution Highway" (PPH). Under the PPH, when an applicant receives a ruling from a first participating patent office that at least one claim in the application it examined is allowable, the applicant may request fast track examination of corresponding claim(s) in a corresponding patent application that is pending in a second participating patent office. The USPTO currently has PPH partnerships in place with thirty-one other patent offices around the world. PPH provides a promising solution to long patent pendency time periods, and expansion and enhancement of the program will strengthen patent systems globally.

Promoting Efficient Patent Systems

Bilateral cooperative agreements between the USPTO and foreign intellectual property offices have served as an effective mechanism for enhancing patent systems through capacity building, training, and sharing of best practices. These agreements enable dissemination of technical knowledge, enhancement of institutional expertise, and understanding of accepted standards to promote patent system improvements.

By way of example, the USPTO and the Mexican Institute of Industrial Property (IMPI) renewed a Memorandum of Understanding on April 12, 2016, institutionalizing the exchange of technical expertise for purposes of strengthening each country's patent system.

In order to maximize work sharing efficiencies, the USPTO is working with partner offices around the world to promote harmonization of key patent issues; namely, the definition and scope of prior art, the grace period, and publication of applications. Practically speaking, the success of work sharing hinges on the ability of patent examiners to examine applications based on foreign work products in an efficient and comprehensive manner. Harmonization of patent examination aspects of patent law complements work sharing by making the work product of one office (*i.e.*, search and examination reports) more reliable for use by another office in examining a corresponding application. More reliability instills greater confidence in the quality of the work product, which, in turn translates to more effective reuse, in terms of work avoided, by the later examining office. To advance discussions on substantive patent law harmonization, a group of like-minded countries known as Group B+ has been working together to explore how to best make progress. In 2015, the Group published an Objectives and Principles Document, which includes higher level objectives for the patent system and principles directed to specific issues relevant to patent-examination. The Group has also issued a number of studies that explore each jurisdictions' laws and the policies underpinning differing practices.

The USPTO is also exploring other ways to increase prosecution efficiencies. Together with their IP5 partners, the USPTO has begun working on the possible alignment of certain office procedures, including procedures involving unity of invention, citation of prior art, and written description. Work on these topics is intended to drive towards convergence on a procedural level, which will then complement the work that IP5 is doing on work sharing and other technical matters.

ACTION NO. 4.12: Facilitate capacity building and technical assistance. USPTO will continue to engage with counterpart offices on providing targeted training, technical expertise, and information sharing to improve the patent systems in key markets abroad.

ACTION NO. 4.13: Support the Patent Prosecution Highway (PPH) System. USPTO will seek new PPH partnerships, as necessary and appropriate, and will enhance existing PPH arrangements to promote greater efficiency in the international patent system.

ACTION NO. 4.14: Continue working to advance substantive patent law harmonization. USPTO will continue to work with its counterpart offices and with stakeholders to advance discussions on substantive patent law harmonization to promote more efficient patent prosecution and more effective work sharing internationally.

b. Promoting Effective, Transparent, and Predictable Patent Systems.

The absence of effective, transparent and predictable patent rights and policies reduce incentives for robust research and development efforts, undermines innovation, and hamper job growth prospects. The U.S. supports and encourages efforts which provide transparency and predictability with respect to patent rights and policies, thus preserving the incentives that ensure access to, and dissemination of, the fruits of innovation and creativity. This is described further in USTR's Special 301 Reports.

The increased globalization of trade, coupled with the intricacy of doing business in or with countries around the world, have given rise to an ever increasingly complex set of regulations and regulatory structures. Nontransparent—or worse, arbitrary—practices have the potential to hinder research and development, market access, foreign direct investments and other expenditures, especially in innovative technologies impacting agriculture, medical, and computer—related fields. These practices make it challenging to secure and enforce patents and other intellectual property rights critical to fostering innovation, economic growth, and global competitiveness.

Patent Policy and Transparency

In 2015, China "unveiled proposals in the pharmaceuticals sector that seek to promote government-directed indigenous innovation and technology transfer through the provision of regulatory preferences….[A] State Council measure issued in final form without having been made available for public comment calls for expedited regulatory approval to be granted to innovative new drugs where the applicant's manufacturing capacity has been shifted to China."

Source: USTR Report to Congress on China's WTO Compliance (Dec. 2015), p. 9

As the OECD has summarized, transparency is primarily understood in the international investment policy community "as making relevant laws and regulations publicly available, notifying concerned parties when laws change and ensuring uniform administration and application," and for other practitioners "it may also involve offering concerned parties the opportunity to comment on new laws and regulations, communicating the policy objectives of proposed changes, allowing time for public review and providing a means to communicate with relevant authorities."[39] Essentially, transparency and stakeholder participation "allow governments to avoid unintended consequences and facilitate stakeholder compliance with legislative and regulatory changes."[40]

It is particularly the case that foreign firms and similar investors seeking access to a market must have adequate information on new and revised regulations so that they can base their decisions on accurate assessment of potential costs, risks and market opportunities. However, as the Office of the U.S. Trade Representative (USTR) has explained in its 2016 Special 301 Report, lack of transparency in IP-related rulemaking continues to be a problem as some foreign government regulatory agencies fail to make drafts of new rules widely and adequately available for public comment in the first instance, or fail to ensure that laws and regulations are administered in a uniform, impartial and reasonable manner.

When the latest U.S. patented technology is infringed abroad because of lax patent protection and unpredictable legal standards, it threatens innovative economies worldwide. It is imperative that when formulating policies to promote innovation, all stakeholders must take account of the increasingly cross-border nature of commercial research and development, and champion transparent and fair practices. Ensuring open market access and effective intellectual property enforcement are indispensable for continued innovation and growth of the global economy.

ACTION NO. 4.15: Support efforts to strengthen promotion of transparent and fair trade practices. USTR and the USPTO, in collaboration with the relevant members of the U.S. Interagency Strategic Planning Committees on IP Enforcement, will continue to promote and enhance efforts to advance transparent and fair trade practices related to intellectual property, including by bilateral and multilateral discussions prioritizing these issues; facilitating workshops with trading partners focusing on best practices that provide fair and equitable market access; and considerations for effective enforcement of intellectual property rights.

c. Enhancing Effectiveness of Design Systems Abroad.

As U.S. companies and designers continue to expand products into foreign markets, it is important for the U.S. to also promote strong and effective design protection and enforcement worldwide, reflecting the importance of design innovation to economic growth.

The USPTO leads a global strategy to assist industrial designers by promoting and furthering the development of highly-efficient and interoperable industrial design protection systems around the world. Through multi-lateral efforts at the Industrial Design Forum, or "ID5", the USPTO looks to build mutual understanding and collaboration with the other four largest design offices on initiatives aimed at promoting awareness of, and improving the work efficiency, quality and user-friendliness of industrial design systems globally. These initiatives include encouraging a twelve-month grace period for design applicants, ensuring protection is available for designs that are embodied in only a portion of an article/product (so called "partial designs"), mitigating inefficiencies and costs associated with filing design applications in multiple jurisdictions by implementing enhanced priority document exchange systems, and initiating consideration internationally of new and emerging technological designs (graphical user interface (GUI) and icon designs, etc.).

The recent U.S. membership in the Hague System provides significant and immediate cost savings as well as increased competitiveness abroad for U.S. designers. The Hague System is an international design application registration system, similar to the PCT System for utility patents and the Madrid System for trademarks. Despite the Hague System only taking effect in May of 2015 with respect to the U.S., the U.S. has already moved into second position behind the European Union as the most frequently designated jurisdiction in international design applications.[41] As more countries become members, the Hague System will continue to increase the benefits and the improved efficiencies it provides to design innovators.

ACTION NO. 4.16: Promote strong and effective design protection worldwide. USPTO will continue to advocate for and advance strong, effective and user-friendly industrial design protection systems at the Industrial Design 5 Forum (ID5) and through other multilateral or bilateral initiatives.

ACTION NO. 4.17: Support Hague System for the International Registration of Industrial Designs. USPTO will continue to support the improvement and expansion of the Hague System, thereby enhancing a global mechanism for industrial design applicants to efficiently pursue protection for industrial design innovation across the globe.

E. BROADER RECOGNITION OF THE ESSENTIAL ROLE UNIVERSITIES PLAY IN INNOVATION

In addition to their essential role as centers of knowledge, learning, and scholarship, universities around the world are engines for innovation. Universities are often the first step in the innovation lifecycle, but too often the big idea does not make it to the marketplace. The promise of innovation that is first conceived by professors, researchers, and students in university laboratories frequently goes unrealized.

Universities play an essential role in the innovation life cycle. Universities mobilize their research resources and IP assets to foster the pursuit of learning and develop partnerships to drive innovation, and catalyze and fund further research and innovation. IPRs, including most notably, patents, facilitate the commercialization of innovations by enabling the innovators to attract investors. Examples of U.S. policies that encourage and incentivize university innovation in partnership with industry include the Stevenson-Wydler Technology Innovation Act, the Bayh-Dole Act, and the America Invents Act.

With a patent, the invention becomes a tradable commodity, a product that can be licensed or sold. Technology partnerships leverage technology transfer by providing universities with additional researchers to find solutions to problems, manufacturing knowledge, knowledge of adaptations required for marketing to comply with local laws and regulations.

Universities have therefore become not only laboratories of ideas, but also incubators of start-ups and spin-offs. Where public sector funding can be scarce and grants can be highly-competitive to secure, the IP-revenue generated from university technology partnerships can be critical to the sustainability of continued university research.

As just one example, the first modern three-point seatbelt that is found in most vehicles today was developed by Roger Griswold and Hugh DeHaven at the Aviation Safety and Research Facility at Cornell University in New York and was the result of intensive

crash injury research. The device would later be perfected by Nils Bohlin at Volvo. Other seatbelt research would be conducted at the University of Minnesota by James "Crash" Ryan in 1963, further pushing forward the science of safety.

But this kind of success story does not exist in isolation and cannot survive without the proper regulatory framework.

ACTION NO. 4.18: Foster broader recognition of the promise of university-led research and development as a driver of innovation. The Federal Government will work with other countries, bilaterally and through appropriate multilateral fora, to advocate for IP systems that help enable university-led research to drive innovation.

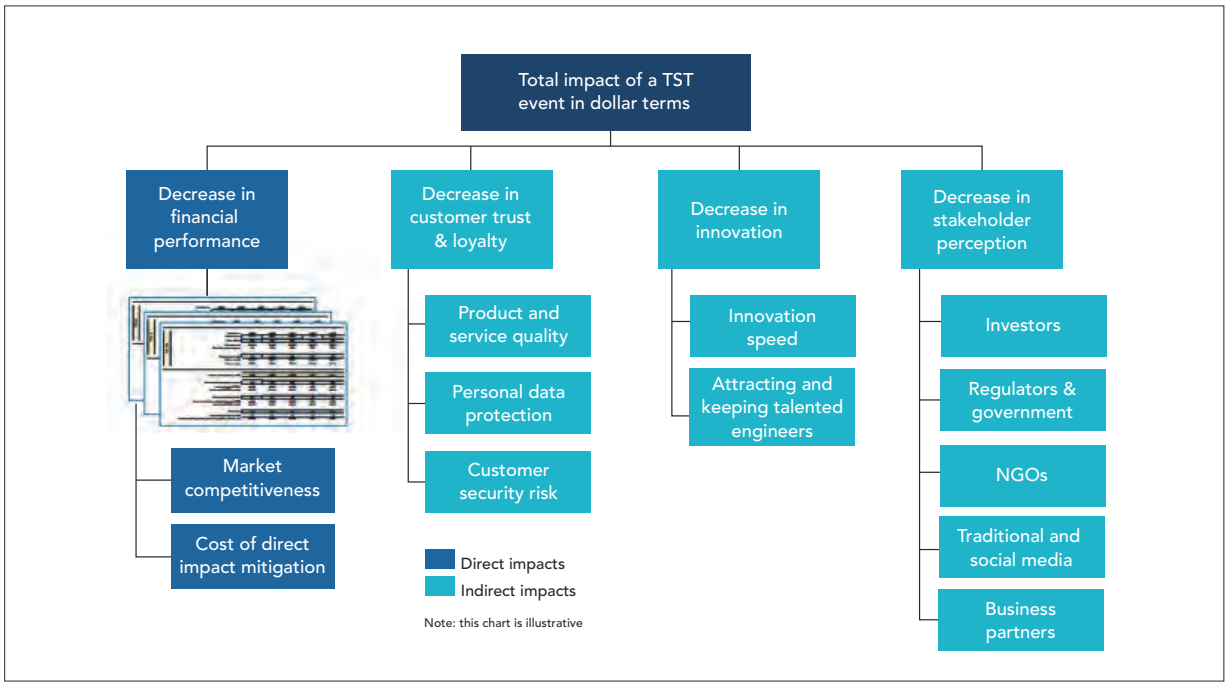
F. SUPPORT STRATEGIES THAT MITIGATE THE THEFT OF U.S. TRADE SECRETS.

U.S. companies face a growing and persistent threat by individuals, rival companies, and foreign governments that seek to steal some of their most valuable intangible assets—their trade secrets.[42] Trade secrets consist of non-public, commercially valuable information, including confidential formulae, programs, devices, processes or techniques for manufacturing a product.[43] "Protecting the trade secrets of American businesses sustains the integrity and competitiveness of the American economy, and encourages the development of new products, including advanced technologies."[44]

As reported in the U.S. "Strategy on Mitigating the Theft of U.S. Trade Secrets," issued in February 2013, "[e]merging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is escalating."[46] However, the exact cost of trade secret theft has gone largely unknown due to the difficulty in measuring such losses.[47]

Advancements in technology, increased mobility, globalization, and the anonymous nature of the Internet together contribute to growing challenges in protecting trade secrets. Bad actors acquire trade secrets in a variety of ways. In addition to taking photos, making sketches, or asking detailed technical questions about technologies on display at conferences, conventions and trade shows—methods that have been exploited for years—rogue actors are increasingly targeting the electronic information databases of U.S. companies, law firms, academia and financial institutions. Indeed, hacking is emerging as the preferred method of trade secret theft, given that, through a single breach, one person can steal

FIG. 62: Economic Impact of a Trade Secret Theft Event.[45]



Source: The Center for Responsible Enterprise and Trade and PricewaterhouseCoopers LLP.

copious amounts of information with relative anonymity while masking their geographic location.[48] Moreover, many of these targeted attacks reportedly originate overseas, in countries where the laws are weak or poorly enforced, or governments lack the ability or are unwilling to crack down on those responsible.[49]

If not addressed adequately, trade secret theft will continue to harm the global economy and put our national security at risk. Trade secret protection should be an important priority not just for businesses, but also for the Federal Government, which can help mitigate trade secret misappropriation through improved coordination, law enforcement, diplomacy, and public education and outreach efforts. For additional discussion of trade secret theft, see Section II of this Strategic Plan.



On April 01, 2015, President Obama signed an Executive Order declaring that certain malicious cyber-enabled activities constitute a serious threat to the U.S.' national security and economic competitiveness, including specifically the misappropriation of trade secrets for commercial or competitive advantage or private financial gain.

By sanctioning malicious cyber actors, the Executive Order aims to disrupt both the supply side (by authorizing sanctions on those who perpetrate the acts), as well as the demand side (by authorizing sanctions against entities that knowingly receive or use the stolen trade secrets), effectively limiting an entity's ability monetize the stolen trade secrets.

See: Executive Order 13694 (April 01, 2015).

ACTION NO. 4.19: Prioritize diplomatic efforts to protect trade secrets overseas. The Department of State, USPTO, USTR, and other relevant members of the U.S. Interagency Strategic Planning Committees on IP Enforcement will work together on a strategy for further diplomatic engagement to protect U.S. trade secrets internationally.

ACTION NO. 4.20: Monitor the Federal Government's efforts to address trade secret theft. The U.S. Interagency Strategic Planning Committees on IP Enforcement, in consultation with the National Security Council and the Office of Management and Budget, will annually solicit from its members and other relevant Federal agencies and offices any recommended measures that could be implemented to enhance efforts to combat U.S. trade secret misappropriation

ACTION NO. 4.21: Identify opportunities for IP enforcement agencies to support the Cybersecurity National Action Plan. Following the release of the Cybersecurity National Action Plan (CNAP) in 2016, the U.S. Interagency Strategic Planning Committees on IP Enforcement will review the strategy to enhance cybersecurity awareness and protections and maintain economic and national security.[50] In light of the growing threats posed by cyber-enabled theft of trade secrets, the U.S. Interagency Strategic Planning Committees on IP Enforcement will identify opportunities to support the CNAP implementation, and its application to cyber-based IP risks, through agency work. Additionally the U.S. Interagency Strategic Planning Committees on IP Enforcement will ensure alignment with existing cybersecurity incident response policies in the event of IP theft that also represents a cyber incident.

ACTION NO. 4.22: **Enhance education programs related to economic espionage and trade secret theft.** Within two years of the issuance of this Plan, the U.S. Interagency Strategic Planning Committees on IP Enforcement will coordinate an evaluation of whether gaps exist in Federal education and public awareness campaigns with respect to prevention of economic espionage and trade secret theft. The U.S. Interagency Strategic Planning Committees on IP Enforcement will develop a plan for addressing any such gaps.

G. PROMOTE SUPPLY-CHAIN ACCOUNTABILITY IN GOVERNMENT ACQUISITIONS.

Each year, the Federal Government spends more than $6 billion on software through more than 42,000 transactions,[51] which range "from large delivery orders

on established contracts to individual purchases from commercial catalogs."[52] As a matter of law, and as a strong example for our trading partners and the international community, it is important that Federal agencies use software in accordance with applicable copyright protections and software licenses.

The U.S. has prioritized this principle, as underscored by the Presidential executive order on "Computer Piracy" (E.O. 13103)[53] which sets forth "the policy of the United States Government that each executive agency shall work diligently to prevent and combat computer software piracy in order to give effect to copyrights associated with computer software." In accord with this policy, the Executive Order directs each agency to ensure that "the agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws" and that "the agency has present on its computers and uses only computer software not in violation of applicable copyright laws."

As part of the Administration's "category management" initiative, OMB issued a policy in 2016 to further enhance the Federal Government's acquisition and management of software.[54] Issued jointly by the U.S. Chief Acquisition Officer and the U.S. Chief Information Officer, the policy leverages private-sector best practices to improve Federal Government processes."[55] In addition to achieving taxpayer savings, operational efficiencies, and better performance, these improvements in how the U.S. buys and uses software will further ensure that Federal agencies comply with the terms of applicable software licenses.[56] Through the implementation of the category-management policy, and related policies[57] and statutes,[58] the Federal Government will strengthen the oversight of its acquisition and use of software, and thereby continue to ensure compliance with applicable copyright protections and licenses. Opportunities exist to promote these and other best practices with trading partners to minimize, and indeed, avoid, the use of unlicensed or pirated software or other copyrightable content.

ACTION NO. 4.23: Support and promote government software licensing best practices. The U.S. Interagency Strategic Planning Committees on IP Enforcement, in consultation with the U.S. Chief Acquisition Officer, and the U.S. Chief Information Officer, and such other agencies and offices as may be appropriate, will assess opportunities to support enhanced accountability in Federal government software acquisition and licensing practices.

H. CALLS FOR RESEARCH.

Public policy is at its best when well-grounded in sound research and data. Given the profound technological and legal changes that have taken place over the past several years, it is critical that academics, researchers, the private sector, and others continue to rigorously study the IPR ecosystem to identify areas of concern, emerging trends, and opportunities for enhanced enforcement mechanisms.

Research is needed into the precise nature and dimensions of the various challenges in IP enforcement in order to improve the effectiveness and targeting of policy, including legal reform, trade policy, and capacity building. By analyzing data and evidence, stakeholders will have increased power to identify and implement effective IPR. The United States, along with international partners, must continue to assess and adopt measures that prevent, protect, and provide effective remedies to address violations of intellectual property, including in the forms of commercial-scale piracy, trade secret theft, and trade in counterfeit goods.

In order to do so, countries need to collect reliable statistics; accurately assess, in detail, the limitations, obstacles and impediments to effective IP enforcement; share best practices; and engage stakeholders and other experts to develop international guidelines to harmonize concepts, establish statistical definitions, and inform stakeholders and the public on the progress that is being made.

Federal agencies, trade organizations, academic institutions, and the private sector all have roles to play in increasing the volume and quality of research in this area. Promising private sector initiatives include: **technology and data analysis tools** to conduct trend analysis and identify opportunities for effective, targeted solutions; **research and collaborative efforts** to promote cross-stakeholder collaboration and public-private partnership, particularly on information sharing; **engagement of senior corporate leaders** to promote enhanced corporate, social, and moral leadership

throughout the company; and **best-practice sharing** across industries to foster open, collaborative industry dialogue and a corporate culture of transparency.

Domestic and international think-tanks and academic institutions, particularly business and public-policy schools, have a role to play in uncovering innovative solutions to difficult international trade, public diplomacy, and entrepreneurial challenges.[59] Increasing scientific research, data collection, and analysis will enhance our understanding of the scope and impact of various IPR enforcement challenges and the most effective means to address them.

Among many other worthy areas of focus, the following illustrative, non-exhaustive list is submitted for purposes of public research and consideration. Through enhanced research, we can ensure that public policy in the years ahead will continue to improve and remain strategically aligned with evolving threats.

Additional Research on Illicit Trade in Counterfeit Goods is Needed…

- **To assess the magnitude of counterfeit goods in the domestic and global supply chains.** The OECD and others have made valuable contributions to our understanding of the scope and scale of counterfeit trade. Additional research will continue to advance our understanding of the magnitude and dimensions of the issue. Additionally, much of the current research is limited to cross-border trade of tangible goods, and excludes significant categories of domestically produced and consumed counterfeit goods and digital piracy.

- **To measure impacts to the U.S. economy, competitiveness, and strategic markets.** Research is needed on the impact of counterfeit trade to the economy and jobs market, including: negative effects on U.S. industry such as lost sales, lost brand value, added costs of doing business, and reduced ability to sustain highest levels of innovation; negative effects on U.S. government such as lost tax revenue, IP enforcement expenses (*i.e.*, interdiction, seizure, investigation, prosecution, and incarceration), storage and disposal costs for counterfeit goods, and economic and social risks of counterfeits entering critical private or public supply chains.

- **To measure the nexus between transnational organized crime (TOC) and illicit trade.** A more analytical understanding of the scope and scale of TOC and the methods by which illicit trade is used to generate revenue for entities involved in TOC would be of benefit to the development of policy.

- **To understand the nature of illicit manufacturing operations.** Research into the structure and composition of facilities engaged in the manufacture of counterfeit goods would enable policymakers to target legislative and regulatory efforts most effectively. For example, what entities are driving increases in illicit trade: (1) rogue and unlicensed/unregulated factories engaged in counterfeit trade; (2) licensed factories, operating openly, but engaged in unlawful side-businesses/activities; or (3) authorized factories, with a present relationship with rights holder(s), engaged in impermissible "second shift" production?

- **To assess the scope of exploitation of transit points and Free Trade Zones (FTZs).** Additional research and quantitative analysis are needed to evaluate the extent to which transit points and FTZs are exploited by illicit traders; the manner in which they are exploited; and the extent to which particular factors influence the relative exploitation of such points and zones. In addition to scope and tactics employed by illicit traders, what is the nature of cooperation between national customs authorities and the special authorities of their FTZs in connection with the targeting of traffickers in counterfeit goods?

- **To emphasize the role of the private sector in helping to minimize the criminal exploitation of commercial platforms and services.** This Strategic Plan acknowledges the hazard faced by banks, online marketplaces, online advertisers, social networks and others whose platforms can be vulnerable to exploitation by illicit traders or pirates. More high-quality research is needed into approaches responsive to this threat, as well as opportunities for additional voluntary industry initiatives and public-private partnerships for securing these essential platforms against illicit activities.

- **To identify the extent of risk to public health and safety.** Significant public health and safety concerns have been identified in connection with the production, sale, and distribution of counterfeit goods; however, there has not been a comprehensive assessment of the scope and nature of these threats to the individual.
- **To identify environmental consequences of illicit trade.** Research is urgently needed to evaluate the extent to which the manufacture, use, and disposal of illicit goods (from fertilizers, pesticides to other products containing heavy metals, for example) contributes to the degradation of the natural environment.
- **To identify the nexus between counterfeit trade and exploitative labor practices.** Violations of fundamental human rights have been documented in connection with the manufacture of counterfeit goods, including the use of child labor, forced labor (including human trafficking for the purpose of forced labor), and sweatshop working conditions. Additional research is required to understand the labor force associated with counterfeit trade, at the point of manufacture and distribution/sale. With a fuller understanding of the scope of the problem, better tailored policy solutions may be applied. Researchers might choose to focus on: (1) what preventive measures might be implemented to protect the most vulnerable people; and (2) how labor exploiters recruit victims and what should be done to stop their iniquitous practices.
- **To assess the impact of voluntary initiatives.** This Strategic Plan, like its predecessors, recommends that certain challenges be addressed through enhanced corporate leadership and voluntary industry initiatives. However, there is modest research available to policymakers evaluating the impact of voluntary initiatives in curbing IP abuses, or whether particular voluntary initiative strategies have demonstrated greater effectiveness than others.
- **To assess trends and analytics behind counterfeit trade via "small parcels."** What are the preferred platforms and channels used to advertise, sell, and distribute (ship) individual or small shipments of counterfeit goods via postal or express mail services? To what extent are individual sellers of counterfeit goods, distributed via individual small parcels, part of, or working with, larger transnational organized counterfeiting networks? What are frameworks to effectively respond to the growth in millions of micro-counterfeit sales transactions that travel via air shipments?
- **To assess trends on consumer knowledge and attitude in transactions involving counterfeit goods.** As a result of technological advances in materials and manufacturing practices, the infiltration of counterfeit goods in online portals, and the growing diversity of fake products (e.g., counterfeit auto parts, medicines, personal care products, electronics, food and beverage, etc.), what is the volume of counterfeit transactions—by product category or sales technique—that rely on an element of consumer deception or fraud (e.g., an unwitting purchase)?
- **To assess common characteristics of illicit traders.** For example, what is the trading history of importers of seized containers of counterfeit goods? Are they new entrants in trade? How long were companies in existence? Was a misappropriation of another importer's (trusted) identity involved? What transport lines are preferred by illicit source, product category, etc.?
- **To use "big data" in order to better understand, and minimize, illicit trade in counterfeit goods.** How to increase transparency and better insight into e-commerce and other digital transactions in order to understand the characteristics of the illicit trader, including for purposes of enhanced risk-targeting and predictive analytics? What techniques could be employed to enhance the usefulness of customs, enforcement or private sector data?
- **To understand crime syndicates' exploitation of the global financial system to support counterfeit trade, including by way of trade-based money laundering.** What is the global scope of trade-based money laundering involving counterfeit goods?
- **To assess how rogue actors may exploit social media and similar channels in support of illicit counterfeit trade.** For example, to what extent do illicit actors use social media tools to generate web traffic; divert consumers to e-commerce websites where they sell their goods; utilize in-site "buy buttons" facilitating purchases directly from page

posts and ads; or rely on pseudonymous product reviews, blog entries or fabricated social media profiles to provide an aura of legitimacy?

Research on Patents is Needed...

- **To assess the effects of recent amendments to the Federal Rules of Civil Procedure.** Research into the effects on pleadings of the December 2015 reforms to the Federal Rules of Civil Procedure is needed to assess the impact of those changes and whether further changes are necessary or advisable.
- **To assess the effects of recent judicial decisions on the patent landscape.** Researchers are urged to evaluate the effects of recent Supreme Court decisions on the patent landscape, including: pleading standards as set forth in *Bell Atlantic Corp v. Twombly* and *Aschcroft v. Iqbal*; effects of litigation resulting from awarding of attorney's fees as set forth in *Highmark* and *Octane Fitness*; and whether post-grant review of patent eligibility have improved patent quality and/or impacted the frequency of frivolous litigation.
- **To analyze litigation patterns.** Policymakers would benefit from a greater understanding of patent litigation trends and patterns. For example, research focused on the causes of any increases in patent litigation both prior to and immediately after passage of the American Invents Act in 2011 would assist policymakers in understanding whether any increases were related to upticks in false marking cases or incentives resulting from the AIA's change to the joinder rule.
- **To analyze litigation's effects on the innovation economy.** Research is needed to evaluate whether there is any relationship between patent litigation and various measures of innovation in the economy, including whether the patent litigation climate impacts the value of a patent.
- **To consider factors affecting awarding of damages.** There is some indication that non-practicing entities (NPEs) may receive higher total damages than practicing entities (PEs). Research is needed into this possible difference, including root causes, and the effects of any settlement calculus employed by NPEs.

Research into Commercial-Scale Piracy is Needed...

- **To assess the economic scope and magnitude of digital piracy.** Beyond any top-line numbers, what is the magnitude of the harm suffered by the copyright owner? What is the impact on employment in the creative sectors? Who are the entities that profit from, or may be unjustly enriched by, the unauthorized exploitation of copyrighted materials?
- **To develop a clearer picture of rogue online actors.** Topics that research might tackle include: (1) the structure and composition of entities deliberately facilitating the dissemination (downloading or streaming) of copyrighted content; (2) the business models employed by illicit actors to derive revenue from acts of commercial piracy; and (3) the evasive tactics employed to enhance resiliency from court orders and injunctive remedies.
- **To assess the nature of intermediary exploitation by criminal actors.** Further research is needed on the extent to which intermediaries—including website hosting platforms, online marketplaces, banks, payment processors, social networks, and others—are exploited by criminal actors, and the size of revenue that may be generated by intermediaries as a result of third-party illicit activity.
- **To examine the range of attendant harms and risks to the public.** What is the relationship between pirated content and incidents of malware, phishing, or other threats to the public?
- **To collect and compile data on the effectiveness of existing remedies, including the state of domestic and foreign injunctive relief and damages.** What is the state of injunctive relief and damages for commercial-scale piracy operations, domestically and abroad, and how have illicit actors responded or evolved to these legal actions? What trends exist?
- **To assess effectiveness of voluntary initiatives.** What framework should be used to assess the effectiveness of voluntary initiatives and industry best practices in light of rapidly changing virtual and technological environment?

- **To understand how to put "big data" to work to better understand, and minimize, commercial exploitation of copyrighted content.** How to increase transparency and better insight into criminal exploitation across ad networks, payment processing, and other digital transactions in order to understand the characteristics of the illicit actor, and support efforts to preserve the integrity of the exploited platforms and services? For example, available generalized and anonymized data on terminated advertising or payment processing accounts (such as, for example, duration of account, dollar flow, general geographical location, etc.) may improve benchmarking of enforcement initiatives and enable stakeholders to identify opportunities for further advancement of underlying policy objectives.
- **To understand common tactics employed by operators of websites that promote counterfeit goods or unauthorized content.** For example, how do illicit actors exploit various domain environments to successfully evade law enforcement through "domain name hopping" and other strategics?

Research on Trade Secret Theft is Needed…

- **To assess the magnitude of trade secret theft.** Research is needed into the scale and economic impacts of trade secret theft on the U.S. economy, including the impact to the competitiveness of U.S. exports, national economic interests, and the jobs market.
- **To assess the degree of cybersecurity preparedness in the private sector.** Further research is needed on the share of U.S. businesses, including SMEs, that are actively engaged in cybersecurity prevention, monitoring, and resiliency planning.
- **To determine global remedies and procedural difficulties faced by rights holders.** Comprehensive comparative legal analysis of trade secret protections and procedures around the world would increase many rights holders' understanding of the markets in which they operate. Analysis of experiences prosecuting trade secret rights abroad, including effectiveness of administration of trade secret laws, would also benefit rights holders and policymakers.

ENDNOTES

[1] Section 301 of the Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("PRO-IP Act"), Pub. L. No. 110-403 (2008), codified at 15 U.S.C. §8111.

[2] Section 1 of Executive Order No. 13565, *"Establishment of the Intellectual Property Enforcement Advisory Committees"* (February 8, 2011), accessed from 76 FR 7681 (February 11, 2011) at https://www.gpo.gov/fdsys/pkg/FR-2012-03-05/pdf/2012-5366.pdf.

[3] The Department of Justice (DOJ) Intellectual Property Task Force (FIG. 63) serves as a variety of a "Whole of Government" structure within one particular Federal department. The Task Force convenes the Federal Bureau of Investigation, the Civil Division, the Criminal Division, the National Security Division, the Office of Justice Programs, the Office of Legislative Affairs, and several other Justice DOJ components together in one IP-focused task force that is chaired by the Deputy Attorney General, and reports to the Attorney General.

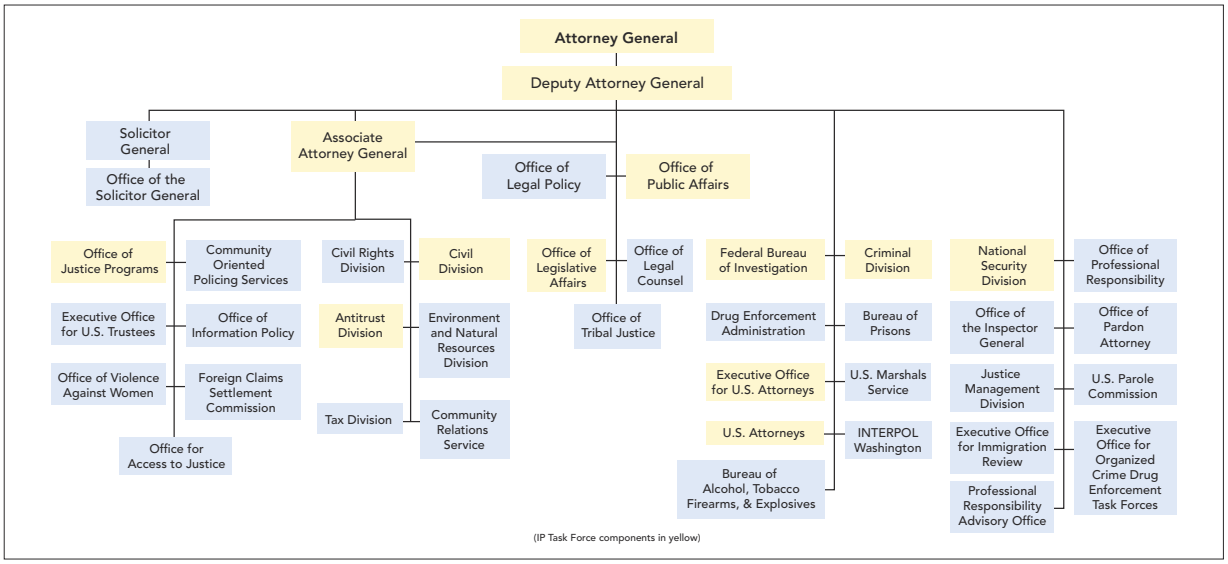
At the same time, the DOJ IP Task Force serves as a "Specialized Office" unit that is tasked to affirmatively develop and advance DOJ's response to the criminal exploitation of intellectual property rights. The Task Force "seeks to support prosecutions in priority areas, promote innovation through heightened civil enforcement, achieve greater coordination among federal, state, and local law enforcement partners, and increase focus on international enforcement efforts, including reinforcing relationships with key foreign partners and U.S. industry leaders." The DOJ IP Task Force "also supports state and local law enforcement's efforts to address criminal intellectual property enforcement by providing grants and training." *See* United States Department of Justice, Intellectual Property Task Force, *"Mission Statement,"* accessed from http://www.justice.gov/iptf/mission-statement.

[4] The National Intellectual Property Rights Coordination Center ("IPR Center") was initially established administratively, and was later established in statute in Section 305 of the Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, 130 Stat. 122 (2016). As the IPR Center's website explains:

> "The mission of the IPR Center is to ensure national security by protecting the public's health and safety, the U.S. economy, and our war fighters, and to stop predatory and unfair trade practices that threaten the global economy. To accomplish this goal, the IPR Center brings together 23 partner agencies, consisting of 19 key federal agencies, INTERPOL, Europol and the governments of Canada and Mexico in a task-force setting. The task force structure enables the IPR Center to effectively leverage the resources, skills, and authorities of each partner and provide a comprehensive response to IP theft."

National Intellectual Property Rights Coordination Center, *"About the IPR Center,"* accessed from https://www.iprcenter.gov/about-us. In addition, the "IPR Center partners employ a strategic approach to combat IP Theft" that includes investigation, interdiction, and outreach and training. Through their coordinated activities, the IPR Center partners achieve results "greater than the sum of its parts." *Id.* For example, the IPR Center participates in *Operation Pangea*, which "target[s] the advertisement, sale, and supply of counterfeit and illicit medicines and medical devices that threaten worldwide public health and safety." National Intellectual Property Rights Coordination Center, "Operation Pangea Fact Sheet" (July 2011), accessed from https://www.iprcenter.gov/reports/fact-sheets/Operation%20Pangea%20Fact%20Sheet%20FINAL%20-%20IPR%20DIRECTOR%20APPROVAL.pdf.

FIG. 63: Department of Justice – Intellectual Property Task Force



[5] For examples of the IPR Center's recent notable accomplishments, *see* Office of the Intellectual Property Enforcement Coordinator, *"Annual Report for Fiscal Year 2015 Under Section 304 of the PRO IP Act of 2008,"* (April 29, 2016), accessed from https://www.whitehouse.gov/sites/default/files/omb/IPEC/fy2015ipecannualreportchairmangoodlatteletter.pdf.

[6] *See, e.g.,* U.S. Chamber of Commerce, Global Intellectual Property Center, *"Infinite Possibilities, U.S. Chamber International IP Index"* (February 10, 2016), accessed from http://www.theglobalipcenter.com/wp-content/themes/gipc/map-index/assets/pdf/2016/GIPC_IP_Index_4th_Edition.pdf.

[7] The IPR Center is a notable example of an organizational structure and entity that, in addition to embodying the "Whole of Government" approach (by bringing together 23 different agencies and components), has developed highly specialized expertise and experience in IPR enforcement tactics by its dedication to IPR-related crimes.

[8] United States Department of Justice, "*About the Computer Crime & Intellectual Property Section,*" accessed from http://www.justice.gov/criminal-ccips.

[9] *See* United States Department of Justice, *"PRO IP Act Annual Report FY 2015,"* at p. 10, accessed from https://www.justice.gov/iptf/file/876191/download.

[10] *See* United States Department of Justice, *"Regional Intellectual Property Law Enforcement Coordinator (IPLEC)"* (vacancy announcement), accessed from https://www.justice.gov/legal-careers/job/intellectual-property-law-enforcement-coordinator-iplec-2. As of this Plan's publication, there are five IPLEC positions; the IPLECs are posted to U.S. embassies in Bangkok, Thailand; Sofia, Bulgaria; Bucharest, Romania; Sao Paula, Brazil; and Hong Kong, China.

[11] *See* United States Department of State, *"Intellectual Property Enforcement,"* accessed from http://www.state.gov/e/eb/tpp/ipe/.

[12] *See* United States Department of Commerce, International Trade Administration, *"Office of Intellectual Property Rights,"* accessed from http://trade.gov/mas/ian/oipr/index.asp.

[13] 35 U.S.C. § 2(b)(9) (PTO "shall advise Federal departments and agencies on matters of intellectual property policy in the United States and intellectual property protection in other countries.").

[14] *See* United States Patent and Trademark Office, "Intellectual Property (IP) Policy," accessed from http://www.uspto.gov/intellectual-property-ip-policy.

[15] As of this Plan's publication, there are 14 IP attaché positions located throughout the world. Most of the attachés have regional responsibilities; there are three attachés for China; and there are separate attachés for the World Trade Organization and for the United Nations' World Intellectual Property Organization. *See* United States Patent and Trademark Office, "Intellectual Property (IP) Attaché Program," accessed from https://www.uspto.gov/ipattache.

[16] *See* United States Copyright Office, *"Office of Policy and International Affairs,"* accessed from http://copyright.gov/about/offices/.

[17] *See* the Annual Reports for the Office of the Intellectual Property Enforcement Coordinator for Fiscal Years 2014 and 2015, required under Section 304 of the PRO-IP Act of 2008 (15 U.S.C. § 8114), accessed from https://www.whitehouse.gov/sites/default/files/omb/IPEC/fy2014ipecannualreportchairmangoodlatteletter.pdf and https://www.whitehouse.gov/sites/default/files/omb/IPEC/fy2015ipecannualreportchairmangoodlatteletter.pdf.

[18] *Operation Pangea* "target[s] the advertisement, sale, and supply of counterfeit and illicit medicines and medical devices that threaten worldwide public health and safety." National Intellectual Property Rights Coordination Center, "Operation Pangea Fact Sheet" (July 2011), accessed from https://www.iprcenter.gov/reports/fact-sheets/Operation%20Pangea%20Fact%20Sheet%20FINAL%20-%20IPR%20DIRECTOR%20APPROVAL.pdf. *See also* INTERPOL, "Operations" (*Operation Pangea* is "an international week of action tackling the online sale of counterfeit and illicit medicines" that "brings together customs, health regulators, national police and the private sector from countries around the world"), accessed from http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea.In June 2015, 236 agencies from 115 countries participated in *Operation Pangea VIII. Id.*

[19] *Operation Opson V* took place in March 2016 with the participation of 57 countries. The effort yielded more than 10,000 tons and 1 million liters of hazardous food and drink. INTERPOL, *"Largest-ever seizures of fake food and drink in INTERPOL-Europol operation"* (March 30, 2016), accessed from http://www.interpol.int/News-and-media/News/2016/N2016-039.

[20] As the USIPR website explains, the Global Intellectual Property Education Database (USIPR) is:

> "maintained by agencies of the United States Government who provide training and technical assistance relating to protecting intellectual property rights. The database is a tool designed to permit the US Government Agencies to deposit international and domestic intellectual property enforcement training materials or catalogs in a shared database so that all federal agencies have access to them to provide greater consistency and to avoid duplication and waste of resources. These shared goals and others are included in the 2010 Joint Strategic Plan on Intellectual Property Enforcement, June 2010."

United States Patent and Trademark Office, "Welcome to IPR Training Activity Database," accessed from http://usipr.uspto.gov/Search.aspx. *See also* United States Patent and Trademark Office, "About USIPR" ("The USIPR Training Program Database is comprised of U.S. government agencies that provide IPR-related informational programs, training, and technical assistance to foreign officials and policy makers. Many Programs are offered to help developing countries comply with their obligations under the World Trade Organization (WTO) Agreement on Trade Related Aspects of Intellectual Property, commonly known as 'TRIPs.' These programs also help the United States meet its TRIPs obligation to provide technical assistance to developing and least developed members of the WTO."), accessed from http://usipr.uspto.gov/About.aspx.

[21] *See* The White House, *"The Trans-Pacific Partnership: What You Need to Know about President Obama's Trade Agreement"* ("Last year, we broke the record in American exports for the fifth year in a row, selling $2.34 trillion in goods and services abroad.") accessed from: https://www.whitehouse.gov/issues/economy/trade.

[22] *See* United States Department of Commerce, "*Intellectual Property and the U.S. Economy: 2016 Update* (2016)," at p. 27, accessed from http://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.

[23] *See* Section 1.

[24] *See*, e.g., World Health Organization (WHO), "*Substandard, spurious, falsely labelled, falsified and counterfeit (SSFFC) medical products*" (Updated January 2016) ("No countries remain untouched by this issue — from North America and Europe through to Sub Saharan Africa, South East Asia, and Latin America. What was once considered a problem suffered by developing and low income countries has now become an issue for all. . . . *However, it is low- and middle-income countries and those in areas of conflict, or civil unrest, with very weak or non-existent health systems that bear the greatest burden of SSFFC medical products.*") (emphasis added), accessed from http://www.who.int/mediacentre/factsheets/fs275/en/.

[25] *See* World Customs Organization (WCO), *"High-impact Customs operation tackles illicit medicines in Africa"* (October 25, 2012), accessed from http://www.wcoomd.org/en/media/newsroom/2012/october/high-impact-customs-operation-tackles-illicit-medicines-in-africa.aspx.

[26] Pursuant to Section 182 of the Trade Act of 1974, as amended (19 U.S.C. § 2242), the Office of the United States Trade Representative (USTR) is required to identify "those foreign countries that deny adequate and effective protection of intellectual property rights, or deny fair and equitable market access to United States persons that rely upon intellectual property protection." To aid in the administration of the statute, USTR created the "Special 301 Priority Watch List" and the "Special 301 Watch List" under the Special 301 provisions. Placement of a trading partner on the Priority Watch List or the Watch List indicates that particular problems exist in that country with respect to IPR protection, enforcement, or market access for persons relying on IPR. Countries placed on the Priority Watch List are the focus of increased bilateral attention concerning the specific problem areas. Additionally, under Section 306 of the Trade Act of 1974, as amended (19 U.S.C. § 2416), USTR monitors a trading partner's compliance with measures that are the basis for resolving an IPR-based investigation under Section 301 of the Trade Act, as amended (19 U.S.C. § 2411). USTR may apply sanctions if a country fails to satisfactorily implement such measures.

[27] See Office of the United States Trade Representative, "*Report to Congress on China's WTO Compliance*," at p. 9 (December 2015), accessed from https://ustr.gov/sites/default/files/2015-Report-to-Congress-China-WTO-Compliance.pdf.

[28] *See* Office of the United States Trade Representative, "*2016 Special 301 Report*," (2016), accessed from: https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.

[29] United States Department of Commerce, *"Intellectual Property and the U.S. Economy: 2016 Update,"* at p. 22 (September 2016), accessed from http://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.

[30] *See* Michelle K. Lee, Under Secretary of Commerce for Intellectual Property and Director of the USPTO, "*Enhanced Patent Quality Initiative: Moving Forward*" (November 6, 2015), accessed from http://www.uspto.gov/blog/director/entry/enhanced_patent_quality_initiative_moving.

[31] U.S. Const., art. 1, sec. 8, cl. 8 (among the powers of Congress is "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").

[32] *See* United States Patent and Trademark Office (USPTO), "*Request for Comments on Enhancing Patent Quality*," 80 FR 6475, at 6476 (February 5, 2015) ("As the USPTO commences its enhanced patent quality initiative, the USPTO is targeting three aspects of patent quality, termed the 'patent quality pillars.' These pillars are: (1) Excellence in work products, in the form of issued patents and Office actions; (2) excellence in measuring patent quality, including appropriate quality metrics; and (3) excellence in customer service."), accessed from https://www.federalregister.gov/articles/2015/02/05/2015-02398/request-for-comments-on-enhancing-patent-quality; USPTO, "Enhanced Patent Quality Initiative" (USTPO webpage on the Initiative), accessed from https://www.uspto.gov/patent/initiatives/enhanced-patent-quality-initiative-0.

[33] *See* Executive Office of the President, Council of Economic Advisers, Issue Brief on "*The Patent Litigation Landscape: Recent Research and Developments*" (March 2016), accessed from https://www.whitehouse.gov/sites/default/files/page/files/201603_patent_litigation_issue_brief_cea.pdf; Yeh, Brian T., Congressional Research Service, "An Overview of the 'Patent Trolls' Debate" (April 16, 2013), accessed from http://fas.org/sgp/crs/misc/R42668.pdf.

[34] *See* Federal Trade Commission, "*Patent Assertion Entity Activity: An FTC Study*" (October 6, 2016), accessed from https://www.ftc.gov/reports/patent-assertion-entity-activity-ftc-study.

[35] *See* Executive Office of the President, Council of Economic Advisers, Issue Brief on "*The Patent Litigation Landscape: Recent Research and Developments*," at pp. 5-7 (March 2016), accessed from https://www.whitehouse.gov/sites/default/files/page/files/201603_patent_litigation_issue_brief_cea.pdf; Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011); *Alice Corp. v. CLS Bank Int'l*, 134 S.Ct. 2347 (2014) (patent eligibility); The National Law Review, "New Federal Rules of Civil Procedure: 3 Must Read Changes" (December 23, 2015) (discovery), accessed from http://www.natlawreview.com/article/new-federal-rules-civil-procedure-3-must-read-changes; *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 134 S. Ct. 1749 (2014) (attorneys' fees), and *Highmark, Inc. v. Allcare Health Mgmt. System, Inc.*, 134 S. Ct. 1744 (2014) (attorneys' fees).

[36] Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011).

[37] *See, e.g.*, Farre-Mensa, Joan, *et al.*, *"The Bright Side of Patents,"* NBER Working Paper 21959 (February 2016), accessed from http://www.nber.org/papers/w21959.pdf. In the Abstract, the authors explain that: "We examine whether patents help startups grow and succeed . . . We find that patent approvals help startups create jobs, grow their sales, innovate, and reward their investors. Exogenous delays in the patent examination process significantly reduce firm growth, job creation, and innovation, even when a firm's patent application is eventually approved. . . ."

[38] *See* World Intellectual Property Organization, "*IP5 Statistics Report 2011*," (2011) at p.80, accessed from http://www.fiveipoffices.org/statistics/statisticsreports/statisticsreport2011edition/PCT.pdf.

[39] *See, e.g.*, Organization for Economic Co-operation and Development (OECD), "*Public Sector Transparency and The International Investor*," at p. 37 (2003), accessed from https://www.oecd.org/investment/investment-policy/18546790.pdf.

[40] *See* Office of the U.S. Trade Representative, "*2016 Special 301 Report*," at p. 10 (April 2016), accessed from https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.

[41] This is based on the design-application statistics for 2016 (January through September) on the website of the World Intellectual Property Organization (WIPO). During this period, the top five jurisdictions – among the designated contracting parties – were the European Union (3,089 design applications), the United States (1,624), Switzerland (1,462), Turkey (1,033), and Japan (878). WIPO, "*Statistics under the Hague System*," accessed from http://www.wipo.int/hague/en/statistics/monthly_stats.jsp?type=DALL&name=6&count=COUNT. The website for the United States Patent and Trademark Office (USPTO) has additional information about the Hague System. *See* USPTO, "*Hague Agreement Concerning the International Registration of Industrial Designs*," accessed from https://www.uspto.gov/patent/initiatives/hague-agreement-concerning-international-registration-industrial-designs.

[42] *See* Office of the National Counterintelligence Executive, "*Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*" (October 2011), accessed from https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[43] *See* 18 U.S.C. § 1839(3) (definition of "trade secret"); The Uniform Trade Secret Act, § 1(4) (definition of "trade secret"), accessed from http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[44] Leslie R. Caldwell, Assistant Attorney General, Criminal Division, United States Department of Justice, "*Kolon Industries Inc. Pleads Guilty for Conspiring to Steal DuPont Trade Secrets Involving Kevlar Technology: Kolon Sentenced To Pay $360 Million in Restitution And Fines*" (April 30, 2015), accessed from https://www.justice.gov/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar.

[45] This Figure is found in The Center for Responsible Enterprise And Trade and PricewaterhouseCoopers LLP, *Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats*, p. 20 Figure 8 (February 2014), accessed at http://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf.

[46] Executive Office of the President, "*Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*," at p. 1 (February 2013), accessed from https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[47] *See* The Commission on the Theft of American Intellectual Property, "*The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*," (May 2013), accessed from http://www.ipcommission.org/report/ip_commission_report_052213.pdf; Government Accountability Office, "*Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*," (April 2010), accessed from http://www.gao.gov/new.items/d10423.pdf.

[48] Defense Security Service, United States Department of Defense, "*Targeting U.S. Technologies: A Trend Analysis of Reporting From Defense Industry*," (2012), accessed from http://www.dss.mil/documents/ci/2012-unclass-trends.pdf.

[49] President Barack Obama, "*A New Tool Against Cyber Threats*" (April 1, 2015), accessed from https://medium.com/@PresidentObama/a-new-tool-against-cyber-threats-1a30c188bc4#.dkbljtcbx.

[50] *See* The White House, "*Fact Sheet: Cybersecurity National Action Plan*" (February 6, 2016), accessed from https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[51] Office of Management and Budget, "*Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing*" (OMB Memorandum M-16-12; June 2, 2016), accessed from https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf.

[52] Anne Rung, United States Chief Acquisition Officer, and Tony Scott, United States Chief Information Officer, "*Applying Category Management Principles to Software Management Practices*" (June 2, 2016), accessed from https://www.whitehouse.gov/blog/2016/06/02/applying-category-management-principles-software-management-practices.

[53] Executive Order 13103 of September 30, 1998, on "*Computer Piracy*" (63 FR 53273; October 5, 1998), accessed from https://www.gpo.gov/fdsys/pkg/FR-1998-10-05/pdf/98-26799.pdf.

[54] Office of Management and Budget, "*Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing*" (OMB Memorandum M-16-12; June 2, 2016), accessed from https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf.

[55] Anne Rung, United States Chief Acquisition Officer, and Tony Scott, United States Chief Information Officer, "*Applying Category Management Principles to Software Management Practices*" (June 2, 2016), accessed from https://www.whitehouse.gov/blog/2016/06/02/applying-category-management-principles-software-management-practices.

[56] OMB Memorandum M-16-02 includes the following directions to each agency: (1) "No later than 45 days after issuance of this memo, appoint a software manager, that is responsible for managing, through policy and procedure, all agency-wide commercial and COTS [commercial-off-the-shelf] software agreements and licenses"; (2) "Maintain a continual agency-wide inventory of software licenses, including all licenses purchased, deployed, and in use…"; and (3) "Analyze inventory data to ensure compliance with software license agreements, consolidate redundant applications, and identify other cost-saving opportunities." Office of Management and Budget, "*Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing*," at p. 3 (OMB Memorandum M-16-12; June 2, 2016), accessed from https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf.

[57] An example of a related policy is the OMB memorandum of November 18, 2013, on "*Enhancing the Security of Federal Information and Information Systems*" (OMB Memorandum M-14-03), accessed from https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf. This initiative included the establishment by the General Services Administration and the Department of Homeland Security of "a government-wide Blanket Purchase Agreement (BPA) under Multiple Award Schedule 70, which Federal, State, local and tribal governments can leverage to deploy a basic set of capabilities to support continuous monitoring of security controls in Federal information systems and environments of operation" (p. 2). In addition to enhancing the Federal Government's ability to identify and respond to the risk of emerging cyber threats, continuous monitoring also enables agencies to collect better and more timely information about what types of software are being used by agency staff (and by how many agency staff). Such information is critical to informing the agency about its software needs and to identifying any uses by agency staff of software that is in excess of the applicable license or for which the agency has not obtained the necessary license.

[58] An example of a related statute is Section 406 of the Cybersecurity Security Act of 2015, which directs the Inspectors General to collect information and submit a report to Congress regarding the computer security of specified types of Federal computer systems. In the report, the Inspector General shall include a description of the "policies and procedures followed [by the agency] to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software" (subsection (b)(2)(D)(4)). The Computer Security Act of 2015 is found at Division N of Pub. L. No. 114-113 (2015), and Section 406 ("Federal Computer Security") is at 129 Stat. 2984-2985.

[59] Several of these research categories have been identified, and promoted, by the World Economic Forum. *See* World Economic Forum, "*State of the Illicit Economy: Briefing Papers*" (October 2015), accessed from http://www3.weforum.org/docs/WEF_State_of_the_Illicit_Economy_2015_2.pdf.

THIS PAGE IS INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

With thanks to, and great appreciation for, the many people who contributed to the preparation of *Supporting Innovation, Creativity & Enterprise: Charting a Path Ahead (Joint Strategic Plan on Intellectual Property Enforcement FY 2017-2019)*, including from the Office of the Intellectual Property Enforcement Coordinator:

Philippa Scarlett
Terri Payne
Steven D. Aitken
Shaun Keller
Andrea Goel
Anjam Aziz
John Levock
Jacqueline Rudas
J. Todd Reeves
Jelani Hayes
Matthew Beck
Taylor Barnard-Hawkins
JoEllen Urban

We also wish to acknowledge the following OMB staff for their assistance: Lois Altoft; Crystal Brown; James Chase; Oscar Gonzalez; Abdullah Hasan; Julie Miller; Grant Schneider; and Samantha Silverberg.

This work would not have been possible without the support of the Federal departments, offices, and agencies that provided timely, extensive, and insightful feedback to the Committee during the drafting of this Strategic Plan.

We also wish to thank the many organizations and individuals that submitted comments in response to the Federal Register Notice soliciting input into this Strategic Plan.



Office of the Intellectual Property Enforcement Coordinator