E-Commerce Strategic Plan

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

Executive Summary

U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), through its leadership role at the National Intellectual Property Rights Coordination Center (IPR Center), has developed this strategic plan in recognition of the exponential growth of internet and global online marketplaces to conduct many different types of business and consumer transactions over the past decade. E-commerce has opened global sales markets to any consumer or business with internet access. The growth and popularity of online sales have changed how people purchase and receive many items that are used in daily life, from clothing and shoes to auto parts and household appliances. Consumers of these goods must have confidence that the items they receive are legitimate and safe, and not subject to prohibitions relating to their importation into the United States. Sometimes, however, the consumer unknowingly purchases an item that is potentially illicit and harmful.

The online market can be used for positive commercial purposes, but it is increasingly being exploited to facilitate the sale and trafficking of illicit goods, including but not limited to counterfeit goods, narcotics, firearms and fraudulent identity documents, as well as goods produced using forced labor. These illicit sales are occurring on internet sales platforms, social media sites and dark web marketplaces.

The framework and goals outlined herein emphasize an approach that leverages the assets of private industry and law enforcement partners alike in an effort to act as a force-multiplier and attack criminal activity in e-commerce using a multi-tiered approach. This strategic plan advocates for a cooperative enforcement approach to identify and dismantle those organizations, and prosecute those persons or entities that traffic in all manners of dangerous and illicit goods utilizing various e-commerce outlets including open-net websites, the dark web, point-to-point sales platforms, social media and a variety of payment processors and shipping methods.

Approved:

Derek Benner
Deputy Executive Associate Director (EAD) and
Senior Management Official performing the Duties of the EAD
Homeland Security Investigations

2/14/18
Date

Strategy Alignments

This Strategic Plan complements existing law and national strategy documents including the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA) (Pub. L. No. 114-125), the HERO Act of 2015 (Title III of S.178, Justice for Victims of Trafficking Act of 2015) (Pub. L. No. 114-22), the Intellectual Property Enforcement Coordinator (IPEC) Joint Strategic Plan on Intellectual Property Enforcement (FY 2017-2019), the U.S. Department of Homeland Security (DHS) Quadrennial Homeland Security Review (QHSR) and the ICE Strategic Plan 2016-2020. All of these documents stress the importance of working in a cooperative environment with both industry and other law enforcement partners. They also emphasize the importance of the sharing of information in order to accomplish a common goal of disrupting criminal activity through all avenues of e-commerce, including targeting the flow of illicit proceeds and tracking and interdicting the movement of illicit goods.

1. TFTEA Section 305 expressly codified the IPR Center's role as the lead office with in the U.S. Government for coordinating with other Federal agencies on intellectual property infringement investigations, law enforcement training, and private sector and public outreach on infringement of intellectual property rights, as well as ICE's role as the leader of this Center. Additionally, Section 305 of TFTEA mandates that the IPR Center work with federal agencies and private entities for training and sharing information and best practices.

2. The Justice for Victims of Trafficking Act of 2015, Title III codified the ICE/HSI Cyber Crime Center to provide investigative assistance, training, and equipment to support domestic and international investigations by ICE of cyber-related crimes. Section 302 further states that the Cyber Crime Center will operate a Cyber Crime Unit (CCU) which is mandated to oversee cyber security and operations, enhance the ability of ICE to combat criminal enterprises operating on or through the Internet and provide training and technical support in cyber investigations to ICE and its law enforcement partners.

3. The DHS 2014 QHSR outlines one of the Department's primary missions is to secure and manage our borders, through risk-based strategies, in an effort to protect the US against any threat to national and economic security and public safety. (QHSR, 2014, pp. 14-16) The QHSR broadly states the many dangers and the expanse of cybercrime through intellectual property theft and laundering of criminal proceeds and emphasizes that DHS, through ICE, is responsible for the deconfliction, training and enforcement of "cyber investigations related to online economic crime, digital theft of export controlled data, digital theft of intellectual property…" (QHSR, 2014, p. 84). It also emphasizes a need to improve "efficiency and effectiveness…through public-private partnerships." (QHSR, 2014 p. 16)

4. The ICE Strategic Plan 2016-2020 mandates that "ICE will aggressively investigate intellectual property crime and trade fraud violations, including copyright and trademark crimes, dumping and countervailing duty evasion schemes, pharmaceutical smuggling, wildlife smuggling and border-related trade crimes. ICE will attack these crimes virtually in cyberspace and through traditional law enforcement techniques." (ICE Strategic Plan, 2016, p. 18) The ICE Strategic Plan also mandates that ICE will work in coordination with the 22 other members of the IPR

Center and will share information in an effort to promote a "coordinated U.S. government response". Additionally, it states that ICE will cultivate relationships with international partners, law enforcement counterparts, industry and the public. (ICE Strategic Plan, 2016, p.18)

5. Section 2 of the 2017-2019 IPEC Joint Strategic Plan lays out a course for "Helping to Promote A Safe and Secure Internet" to including the targeting of financial proceeds of counterfeiting through education and partnership with those payment services whether they are credit card companies, online payment services, online banks, or money transfer companies. The IPEC also encourages the formation of collaborative efforts between e-commerce platforms and law enforcement in an effort to share information on the individuals, businesses or organizations identified through various means of investigation or targeting.

   Included in the IPEC Strategic Plan are "action" statements that stress several important points, three points that directly influence the ICE/HSI E-Commerce Plan are:

   a. Action 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, 2016, p. 68)

   b. Action 2.21: Under this action item, the IPEC encourages "E-commerce platforms…to share complete selling history records to law enforcement upon the identification of a seller suspected of being engaged in significant counterfeiting operations" (IPEC, 2016, p. 79)

   c. Action 2.23: "Promote and expand U.S. law enforcement partnerships with e-commerce platforms to disrupt incidents of fraud" (IPEC, 2016, p. 79)

Mission statement

In accordance with existing federal law, and the stated strategies above, the mission of ICE/HSI as it pertains to e-commerce is to collaborate with our law enforcement counterparts and committed industry partners to identify, investigate, disrupt and dismantle transnational criminal organizations and prosecute individuals who facilitate the sale and importation of counterfeit, dangerous and illicit goods through exploitation of the online sales platforms, illicit websites, social media and the dark web.

Scope of the Issue

For purposes of ICE/HSI criminal investigations, e-commerce is the sale, reproduction, distribution, streaming, or any other unauthorized public performance, transmittal, conveyance, exchange, or transference of goods or copyrighted works over the internet, digital telecommunications network, or any other electronic means. E-commerce is a growing way to reach consumers and provide merchandise to an increasingly computer literate population. However, as with any advancement in products and services,

or marketing to the consumer, an element of criminality can potentially exploit those methods to sell illicit goods to the knowing or unknowing consumer. These illicit goods include, but are not limited to counterfeit goods, pirated works, regulated or counterfeit pharmaceuticals, narcotics, identity documents, forced labor-produced goods, and weapons purchased and shipped in international commerce.

Strategic Framework

ICE/HSI employs criminal enforcement resources, strategic partnerships and cooperation and external and internal training as part of its strategy against violations facilitated through e-commerce channels. These strategies can be worked in isolation or as part of a multi-layered approach.

1. **Criminal Enforcement –** ICE/HSI conducts criminal investigations into the importation and illicit sale of counterfeit and dangerous illicit goods being imported to or exported from the United States, as well as goods produced using labor types or materials prohibited under U.S. law. These investigations require substantial resources to investigate and prosecute, but are a very effective method to thoroughly dismantle counterfeiting and smuggling networks. As a result of these criminal investigations, the facilitators can be criminally prosecuted, their assets seized and their e-commerce presence removed.

   The identification of these violators is made easier through cooperation with industry and law enforcement partners, such as U.S. Customs and Border Protection (CBP). ICE/HSI partners with CBP to target shipments and packages entering the commerce of the United States, and works closely with its partner agencies to deconflict active or historical data through the IPR Center and the International Organized Crime Intelligence and Operations Center (IOC-2). Through IOC-2's connectivity to the Special Operations Division and OCDETF Fusion Center, ICE/HSI is able to affect deconfliction and coordination over a broad spectrum of law enforcement data and agencies.

2. **Partnerships with E-Commerce Platforms and Providers** - Disruption of a criminal entity or organization involve enforcement activity for a specified period of time in order to increase pressure on the criminal network. The increased law enforcement presence attempts to dissuade violators from continuing their illegal activity in that area. However, in order for any disruption techniques to be effective, ICE/HSI must form strategic partnerships with appropriate entities within the e-commerce industry and individual corporations. Only through the sharing of pertinent trends and violator data, and the way in which the violators conduct business, can ICE/HSI effectively and efficiently identify and prosecute criminal violators.

3. **Engagements with Payment Processors –** The sale of counterfeit, pirated and/or dangerous goods via the internet are lucrative crimes for those who perpetrate them. Seizing or stopping the transmission of proceeds through electronic payment processors, credit card issuing and acquiring banks, as well as money services businesses (MSBs), eliminates the economic advantage of these types of criminal activity and serves as a deterrent for those considering these crimes. In order to

accomplish this, HSI must form strategic partnerships with the appropriate entities within the payment processing, online money transmission, and other financial industries.

4. **Websites and Social Media –** Organizations distribute dangerous and illicit goods through infringing internet websites and social media sites. ICE/HSI is focused on developing long term investigations that identify targets and assets in the United States and financial schemes used in operating infringing websites domestically and internationally. Through this Strategic Plan, ICE/HSI seeks to arrest and prosecute offenders as well as seize assets, websites and domain names. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for managing and addressing the fundamental functions of the internet. ICANN is responsible for establishing policies and enforcing contractual agreements with registrars and registrants. ICE/HSI, as a member of the Governmental Advisory Committee (GAC), engages and provides advice to ICANN so as to establish polices that do not contradict national laws and international agreements and make the internet safer for all users.

5. **External Education and Outreach Campaigns -** Too often, counterfeiting, in many forms, is viewed as a victimless crime. People are willing to participate in such fraud schemes because they fail to recognize the harm that it can bring to the U.S. economy or the consequences to the end user of substandard products or fake identity documents, as well as the legal concept that intellectual property requires protection like other types of personal property. ICE/HSI brings the issues and vulnerabilities associated with counterfeiting to light. ICE/HSI's education and outreach initiatives provide the means for law enforcement, industry and the public to understand the dangers of counterfeit products, in all forms, and the reporting process; enabling them to be a stakeholder in the solution.

6. **Internal Training Opportunities –** In order for ICE/HSI to continue to grow and remain a key player in the e-commerce and cyber investigative realm, ICE/HSI must place a high priority on providing the most up-to-date and relevant training to agents who are tasked with cyber investigations, to include online e-commerce markets and social media, and investigations on the dark web illicit marketplaces. Any cyber training program will be updated frequently in order to stay current with the ever-changing landscape of the internet and online methods of e-commerce.

Consequences

The proliferation of counterfeit and dangerous goods being sold on various e-commerce platforms can have serious repercussions on the well-being of consumers and industry alike. From the impact of counterfeit tainted pharmaceuticals or counterfeit substandard mechanical parts that do not perform as designed, consumers are put at risk, as well as the name, reputation, and financial stability of the legitimate rights holder.

1. **Human/Consumer Impact**

The human impact of counterfeit and illicit goods being sold through any e-commerce entity is wide ranging, from the loss of money resulting from buying substandard products to the adverse health consequences, up to and including death, by buying and using potentially dangerous counterfeit or illicit items such as auto parts, cosmetics or pharmaceuticals. In either situation, the individual suffers a personal loss and will potentially lose confidence in the legitimate brand name they believed they were purchasing.

Also, the consumer may unknowingly purchase goods produced using forced labor, thereby perpetuating and increasing the numbers of forced laborers worldwide and the illicit profits gained by criminal organizations and individuals using exploited individuals in their supply chains.

In addition, the sale of Personally Identifiable Information (PII), financial credentials or fraudulent identity documents on the dark web creates a legal and personal hardship for the individual victim whose sensitive information is available to be purchased for illicit use. This loss can damage the economic and personal security of citizens, as well as erode confidence in an entity the consumer believed would protect his/her personal information.

2. Economic/Business Impact

Counterfeits and illicit sales are a substantial threat not only to the consumer, but to the industries that produce legitimate products and go through the very costly process of creating, testing and protecting their intellectual property, and researching their supply chains for threats and violations of corporate standards. Due to the wide availability of counterfeits in the e-commerce marketplace, the counterfeiter can become a competitor of the legitimate rights holder.

According to the Organization for Economic Cooperation and Development (OECD) and European Union Intellectual Property Office (EUIPO) in 2013, international trade in counterfeit and pirated goods accounted for 2.5% of world trade, or $461 billion. In comparison, OECD reported in 2008, that counterfeit goods accounted for 1.9% of global trade or $200 billion. (OECD/EUIPO, 2016)

3. Governmental Impact

While many see the personal and industrial impacts resulting from the sale of counterfeit and illicit goods, the impact on local, state or federal governments may be overlooked. From decreased tax revenue to the increased cost of IP enforcement, government operational budgets are affected. In a 2017 article on Intellectual Property Theft, the National Crime Prevention Council reported the U.S. economy loses $58 billion each year to copyright infringement alone, included in that number is $16 billion in the loss of revenue to copyright owners and $3 billion in lost tax revenue to the United States. (National Crime Prevention Council, 2017)

Government supply chains are also put at risk by in the introduction of counterfeit and dangerous goods. In a Department of Commerce (DOC) report concerning counterfeit electronics in the

Department of Defense (DoD) supply chain, counterfeits were most commonly encountered through "parts brokers… independent distributors and Internet-exclusive suppliers." (US Department of Commerce, 2010, p. 18) In addition, federal government regulations, and an increasing number of state and local government regulations, prohibit the procurement of goods produced using forced labor, and contractors and corporations are required to state for the record that the goods being purchased by any of those entities were not produced using forced labor.

Another significant impact is clear threat to the national security and public safety of the United States through the sale of counterfeit travel and identity documents through e-commerce or other means. The duty of protecting our national borders and properly vetting those who may attempt to make entry in the United States is made more challenging when officers and agents must identify and take action against counterfeit or false identity documents.

Strategic Goals

1. **Promote Collaboration Among Law Enforcement and Industry**

To successfully fulfill its mission in the growing e-commerce environment, ICE/HSI must promote its cooperative relationships with industry, in particular e-commerce marketplaces to include Business-to-Business (B2B), Business-to-Consumer (B2C), and Consumer-to-Consumer (C2C) platforms. In order to nurture these relationships, ICE/HSI must identify industries that are currently operating in the e-commerce environment and encourage their cooperation and willingness to work with law enforcement in a manner where they will exchange information and trust that the relationship will be mutually beneficial.

As part of this, ICE/HSI must be cognizant of new emerging marketplaces online. For example, many established "brick and mortar businesses" are initiating their own online marketplaces. These marketplaces may complement existing in-store sales, but also create a third-party sales platform as well. It is through the third-party sellers that exploit the e-commerce sales platforms that ICE/HSI regularly sees the introduction of counterfeit and dangerous goods into the market.

2. **Utilize Existing Enforcement Tools Such as "Operation In Our Sites" (IOS) To Disrupt Criminal Activities and Educate Consumers**

IOS remains as a viable tool for ICE/HSI, by targeting organizations that distribute counterfeit, pirated, dangerous and/or illicit products through the internet. IOS must continue to focus on developing and supporting long term investigations that identify targets in the United States, assets and financial schemes used in operating infringing websites and social media accounts domestically and internationally.

The criminally seized domain names are redirected to the IPR Center seizure banner.

This banner provides a conduit for the public to provide information on IPR violations and also serves as a method of educating the public about IP theft.

In furtherance of IOS, ICE/HSI also engages with social media platforms in an effort to take enforcement action, including the removal of online social profiles that are found to sell, distribute or stream counterfeit, pirated and/or illicit goods and products

Building upon the successes of IOS, ICE/HSI must continue to engage with our domestic and international partners in law enforcement and industry and establish an effective partnership with ICANN. The IPR Center will continue to develop new and innovative strategies to protect intellectual property rights and seeks to adapt to the ever changing environment on the internet.

3. Target Financial Transactions

The root of most illicit activity is the financial gain anticipated by the violator(s). The most effective strategy is to target the illicit proceeds at any one of the multiple points of a financial transaction. Money must transmit in one manner or another, in order to pay for manufacturing, wholesale supply, shipping of goods, and retail sale.

Since Fiscal Year 2012, ICE/HSI has directly engaged financial institutions, money service businesses, digital payment processors, and brokerage firms through ICE/HSI relationships with the National Cyber-Forensics and Training Alliance (NCFTA) and other private sector partnerships that focus on information sharing between partner industries and industry with government. This information should be used by ICE/HSI to supplement ongoing investigations or as a method to begin a preliminary investigation and fact finding. ICE/HSI has also initiated contact with online payment processors to include credit card issuers, acquiring banks and online payment portals.

ICE/HSI will continue to foster these relationships as a means to share viable, actionable intelligence. Additionally, ICE/HSI agents assigned to the IPR Center can be utilized on investigations as a means to interact with industry and gather further intelligence for active ICE/HSI cases. As more payment processors trust and collaborate with law enforcement and halt or intercept the flow of illicit proceeds, the more complicated it will become for criminal actors and organizations to transmit their illicit proceeds.

4. Training For Agents To Match The Changing E-Commerce Environment

In the changing e-commerce and cybercrime environment, there is a need for regular training opportunities in order to sustain current knowledge with changing trends and technologies both in the law enforcement realm and in the advancing technology used to market and ship goods. One particularly complicated, and growing, area of e-commerce is the dark web.

The ICE/HSI Cyber Crimes Center (C3) has developed a multi-course cyber training curriculum for agents conducting online investigations. This training is for cyber investigations on the open

net, as well as the dark web. ICE/HSI will expand this training and create opportunities to ensure more agents and intelligence research specialists (IRSs) are trained in cyber investigations. The difficulty in this lies in the ever changing cybercrime environment where new technologies and methods are being created faster than ICE/HSI personnel can be trained. ICE/HSI will continue to make a concerted effort to keep this training up to date and available to all eligible agents and IRSs who are interested in taking these courses and working online investigations. C3 will also continue to work with external partners to facilitate ICE/HSI personnel receiving outside training for topics that are not included in the current HSI Cyber Training Program courses.

Emerging Threats and Challenges

1. **Transnational Criminal Organizations**

Transnational criminal organizations have expanded their illicit activities through the perceived anonymity of the internet and have exploited technology to further their crimes and international reach. These organizations use legitimate e-commerce venues to sell illicit and counterfeit goods and to launder money through electronic transfers and digital currency. Additionally, they utilize computer intrusion techniques to harvest PII which is ultimately sold through illicit websites where cryptocurrencies are the only approved mechanism for payment.

The technical knowledge and resources to commit these crimes are readily available, and have been exploited with the intent to mislead and steal from hard working individuals and companies.

2. **Dark Web Illicit Marketplaces**

The dark web is an emerging threat to the effectiveness of law enforcement agencies, both in the United States and around the globe, and their ability to identify and dismantle illicit marketplaces. The structure of the dark web is largely hidden networks that require specific software, configurations or restricted access to search or participate in activities or illicit e-commerce markets.

While many of these markets have come under the scrutiny of domestic and international law enforcement agencies and some have been disrupted or completely dismantled, these investigations require significant time and resources, and rarely identify the majority of users and sellers in the illicit markets as they migrate from market to market. However, some success has been found on the dark web, including the takedowns of The Onion Router (TOR) sites, SilkRoad and AlphaBay, through collaboration with HSI field offices, C3, and several invested law enforcement partners at the IPR Center. These investigations were successful in that several agencies, working in partnership, identified and brought effective enforcement action against the administrators and dismantled these illicit marketplaces, using the broad range of their investigative and prosecutorial authorities.

The e-commerce markets on the dark web touch many ICE/HSI programmatic areas such as Contraband Smuggling, Counter Proliferation, Cyber Crimes, Financial, Human Trafficking and Identity and Benefit Fraud through various frauds and the sale of weapons, narcotics, and identity and financial documents and credentials

3. Social Media

Another challenge facing law enforcement is the presence of counterfeit and dangerous goods being advertised and sold on social media platforms, where criminals can easily conceal their identity and contact details.

Unlike many of the e-commerce sales platforms that serve the primary purpose of individual business and sales, many social media websites are set up primarily for personal interaction and networking with friends and family. Social media accounts set up for legitimate business advertising and communications with customers are common, but generally point a customer to a website for sales instead of selling directly through the platform. As social media networks are easy to establish and user-friendly, many individuals and illicit businesses have begun to set up pages that advertise and sell counterfeit goods through their accounts.

ICE/HSI components must continue to reach out to social media platforms in an effort to discuss the dangers of counterfeit and illicit goods being marketed and sold on their platforms, and determine ways to work together.

4. Digital Currencies

Digital currency is simply a digital representation of value that functions as a secure, fast and inexpensive online cashless payment system and is firmly entrenched in both domestic and international e-commerce. Digital currencies are an alternative to traditional payment methods which rely heavily on formal banking institutions and financial intermediaries. Digital currencies bypass these intermediaries and associated industry players often fail to register and/or comply with established financial reporting requirements.

Transnational Criminal Organizations appear to be expanding their use of digital currencies as part of their efforts to launder illicit proceeds. Digital currencies have become a preferred laundering tool due to the ability of these organizations to move unlimited amounts of illicit proceeds globally via instantaneous, secure and pseudo-anonymous transactions priced at a fraction of the cost seen in traditional laundering methods.

To address the myriad threats posed by the illicit use of digital currencies, ICE/HSI will continue to employ a multi-pronged enforcement strategy focused on policy, training, procurement of investigative resources and dedicated outreach efforts to our federal, state, local, international and private partners under the Illicit Digital Economy Program.

Moving Forward

1. Sustained Outreach

The most promising strategy for ICE/HSI to pursue in combating crimes proliferating in the various online markets is to engage with industries, trade associations and Non-Governmental Organizations (NGO) that represent industry or collective groups within the sector that are stakeholders in legitimate e-commerce. This engagement also needs to be directed to industry and industry groups on all levels of the marketing, sales, shipping and payment platforms and should include collaboration on trainings to improve law enforcement efforts, deconfliction and robust outreach. ICE/HSI-sponsored symposiums or the development of public service announcements, for law enforcement, industry and the public, and other media are recommended opportunities to promote joint e-commerce and cybercrime efforts.

Not only will ICE/HSI engage industry and industry groups, but we must continue to be faithful and persistent in the communication. ICE/HSI programs will sustain the collaborations over time in order to build industry's trust and confidence in ICE/HSI as a law enforcement agency that will act when called upon.

As ICE/HSI engages industry, we will also continue outreach and training efforts with our domestic and foreign law enforcement partners, and recognize the important role our Attaché Offices have in this effort. ICE/HSI Attaché's must continue engagement at diplomatic and executive levels as many foreign countries with significant trade connections to the United States have either limited, or no existing IPR legislation, or the legislation contains significant vulnerabilities that can be often exploited by transnational criminal organizations engaged in illicit IPR activities. These efforts should be taken on across several U.S. government agencies to present a united front with foreign governments in the interest of the United States' national security and economic integrity. The e-commerce environment has a global reach, therefore training and communication among law enforcement must match the worldwide scope.

2. Policy and Legal Reform that Reflect Emerging Technology

As e-commerce marketplaces expand and new technology emerges, ICE/HSI will adapt policy in a timely manner to provide investigators the most recent and effective tools to combat cyber criminals utilizing both legitimate and illicit forms of e-commerce. ICE/HSI will also continue to work with lawmakers in a continuing effort to adapt and reform existing laws, as well as work with legislators to enact new legislation that provide e-commerce and law enforcement with the legal framework to collaborate and share information for the purposes of criminal enforcement.

Metrics to Evaluate Success

Reported enforcement statistics are standard metrics used by ICE/HSI to demonstrate its successes. These statistics are vital to measuring the enforcement effectiveness of investigations of e-commerce vendors, and illicit e-commerce websites and administrators. However, it is important that HSI also measure its success in collaborating with legitimate e-commerce entities, and actions taken as a result of this collaboration.

Collaboration with all affected industries involved in the e-commerce chain is paramount for success in not only investigating violations, but also in preventing criminal organizations from setting up businesses, shipping and transferring their illicit proceeds. This outreach and education is an easily tracked metric which already occurs in many ICE/HSI programs such as Operation Joint Venture (IPR Center), Cornerstone Outreach Program (Financial) and others. ICE/HSI will document these outreach and education events, including the number and attendance of training and outreach events, and the positive outcomes that result. An example of positive outcome would include when a business alters its public policies in an effort to stop the sale and distribution of counterfeit and dangerous goods as a direct result of dialogue and the effective exchange of information and the investigative findings of all collaborating parties.

Another metric to be tracked is the number of actionable leads disseminated by law enforcement and industry. Actionable leads can result in joint investigations, enforcement on violative websites and social media profiles, and civil or criminal litigation in a state or federal court.

In Conclusion

The ICE/HSI mission of criminal investigation and enforcement of all applicable laws will be enhanced through partnership with domestic and foreign law enforcement as well as a committed collaboration with industry partners and the public. Building and fostering these relationships will strengthen the ability of ICE/HSI to successfully investigate and prosecute violations of law facilitated by individuals and transnational criminal organizations that exploit e-commerce in all of its forms.

Works Cited

(2005). *Congressional Record Volume 151-Part 19.* Washington, DC: U.S. Government Priniting Office.

GAO. (2010). *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods.* Washington, D.C.: GAO.

(2016). *ICE Strategic Plan.* Washington, D.C.: ICE.

IPEC. (2016). *2016 IPEC Joint Strategic Plan.* Washington D.C.

OECD/EUIPO. (2016). *Trade in Counterfiet and Pirated Goods; Mapping the Economic Impact.* Paris: OECD Publishing.

(2014). *QHSR.* Washington, D.C.: DHS.

US Department of Commerce. (2010). *DEFENSE INDUSTRIAL BASE ASSESSMENT:.* Washington, D.C.