GOVERNMENT PROCUREMENT
DRIVING RESPONSIBLE BUSINESS PRACTICES

CREATE.org
Center *for* Responsible Enterprise And Trade

CREATe.org

Center *for* Responsible Enterprise And Trade

The Center for Responsible Enterprise And Trade (CREATe.org) is a non-profit organization dedicated to helping companies and their suppliers and business partners reduce counterfeiting, piracy, trade secret theft and corruption.

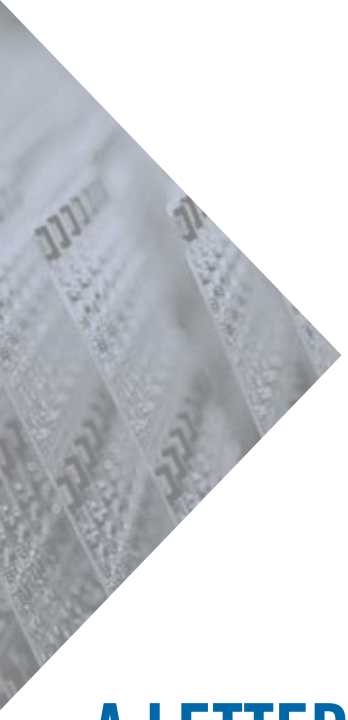
We believe that by improving practices along global supply chains, companies can help drive jobs, growth and innovation – benefiting their own businesses, the global economy, and the communities where they operate. By partnering with governments, non-profits, thank tanks and associations, we hope to amplify the work of each.

To achieve our shared goals, we have developed CREATe Leading Practices for IP Protection and CREATe Leading Practices for Anti-Corruption. Our offering includes practical, scalable and cost-effective online assessments, independent evaluations, training and other resources designed to benchmark and improve processes for safeguarding IP and preventing corruption.

For More Information

Please visit www.CREATe.org, via email at info@create.org or follow us on Twitter @CREATe_org.

TABLE OF CONTENTS



A LETTER FROM CREATe.ORG

Corruption and intellectual property (IP) theft in the form of counterfeits, piracy, and trade secret theft pose significant risks to individuals, companies, governments and societies. Interpol's secretary-general recently noted that while 40 years of terrorism has killed 65,000 people globally, counterfeit medicines killed 200,000 people in China in one year alone. In the EU, an estimated €120 billion is lost to corruption in government procurement, diverting public funds from infrastructure and water projects, health care, education, and other essential services.

Given that governments spend on average 10-15% of GDP on procurement – at an annual rate of approximately U.S. $4 trillion – governments play a critical role in establishing and enforcing the legal regimes to address corruption and IP theft. And increasingly, governments are insisting that their own supply chains be more vigilant in managing these two significant issues by encouraging – and in some instances requiring – specific compliance mechanisms by their own suppliers.

This whitepaper describes how counterfeiting, piracy and corruption can disrupt and taint government procurement. It examines how governments are using procurement rules to require companies to be much more vigilant in managing compliance, particularly with regard to anti-corruption and IP issues. It also outlines the steps government contractors and their suppliers can take to ensure that their practices in these areas are robust, and to remain attractive as responsible vendors to their government customers.

The Center for Responsible Enterprise and Trade (CREATe.org) has produced this whitepaper to bring awareness to these important issues and to provide practical guidance for government contractors and their supply chain and business partners to improve and share leading practices.

To learn more about CREATe or get involved in our efforts, please visit www.CREATe.org.

Pamela S. Passman
President and Chief Executive Officer
Center for Responsible Enterprise and Trade (CREATe.org)

EXECUTIVE SUMMARY

GOVERNMENTS INCREASINGLY are using their purchasing power to insist that government contractors improve their business practices and clean up their supply chains. Given some startling recent examples of bribes infecting public tenders and counterfeits turning up in parts delivered to governments—at times posing significant risks to national security or human safety—government purchasers are particularly focused on anti-corruption and intellectual property (IP) compliance.

This paper describes how counterfeiting and corruption can contaminate government procurement, and the steps governments are taking to address these problems and to encourage responsible, ethical business practices among their own contractors and in the procurement supply chain. It examines how governments are using procurement rules to require companies to be much more vigilant in managing compliance, particularly with regard to anti-corruption and IP issues. It also outlines the steps government contractors and their suppliers can take to ensure that their practices in these areas are robust, and will enable them to remain attractive as responsible vendors to their government customers.

Government procurement is a major force in the global economy. Governments spend on average 10-15% of GDP on procurement (and even more in some developing countries), amounting to a global annual tab of roughly $4 trillion.

I. INTRODUCTION

GOVERNMENT PROCUREMENT is a major force in the global economy. Governments spend on average 10-15% of GDP on procurement (and even more in some developing countries),[1] amounting to a global annual tab of roughly $4 trillion.[2] Aside from employee salaries and social services, procurement represents the largest share of expenditures across all levels of government.[3] The U.S. Government, the world's single largest purchaser, also has the world's largest procurement budget:[4] it spent more than $537 billion in FY 2011 on goods and services.[5] Governments are the largest purchasers of goods and services in many countries.

Although people often associate sales to governments with big multinationals, public procurement touches companies both large and small across the economy. In 2010, for instance, small businesses received almost $100 billion in U.S. Government contract awards.[6] And large government contractors often use hundreds or even thousands of subcontractors of all sizes and across many markets. For example, Lockheed Martin, one of the world's biggest government contractors, reportedly uses more than 40,000 suppliers.[7]

Given the sheer size of global government spending, government procurement practices inevitably influence the broader market. Recognizing this, governments often seek to leverage their vast purchasing power to drive improvements in industry practice more broadly by requiring suppliers to adhere to responsible business practices. Sometimes these requirements are tied to broader societal goals and priorities such as rules designed to advance worker rights[8] or protect the environment.[9] In other cases, they both advance the government's own interests as a purchaser (and policy maker) and help drive broader change in responsible corporate practices. One recent notable example of this trend involves the growing number of procurement requirements designed to reduce corruption and eradicate counterfeit parts from government contracting and supply chains.

While these requirements affect direct government contractors in the first instance, some apply, either legally or practically, to the millions of subcontractors and suppliers that support them. In the United States, for instance, the Federal Acquisition Regulation (FAR) governing federal procurements contains hundreds of contract clauses implementing federal statutes and regulations. Those laws and regulations, as well as the FAR clauses themselves, require the prime contractor to incorporate—or "flow down"—certain clauses into subcontracts related to the prime contracts. Other flow-down clauses are not mandatory, but prime contractors nevertheless often flow them down to subcontractors in order to protect their interests.

As a result, government procurement rules targeting corruption and IP compliance increasingly require urgent attention not only from government contractors themselves, but also from millions of supply chain companies across the economy.

Companies involved in government contracting, either directly or indirectly, are thus well advised to implement robust IP compliance and anti-corruption programs and to work with their suppliers and subcontractors to ensure they adopt such programs as well. Initial evidence suggests that doing so is good for business and in fact more economical in the long run. Indeed, many of today's best-run businesses already are taking steps to enhance supply chain management—a particularly crucial task in the modern global economy, where a single company's supply chain often includes thousands of suppliers and other business partners, some of which may be located in markets where corruption, IP theft, or other illegal practices are commonplace.[10]

Interpol's secretary-general recently noted that while 40 years of terrorism has killed 65,000 people globally, counterfeit medicines killed 200,000 people in China in one year alone.

II. HOW CORRUPTION AND IP THEFT AFFECT GOVERNMENT PROCUREMENT

AS CREATE.ORG has explored in a previous whitepaper, counterfeit products and parts in a company's supply chain can cause major health and safety problems, irreparably damage a company's reputation, and expose it to major financial liability and risk. These risks may be even greater when the buyer is the government. The reasons include the public nature of the purchase and any follow-on consumption; the relatively larger scale of most public purchases; and the sensitive areas in which the supply often takes place, such as defense and health, with higher stakes and graver consequences.

Governments' growing concerns about IP and anti-corruption compliance in their supply chains are exemplified by recent U.S. Administration and Congressional investigations into the problem of counterfeit parts supplied to the U.S. Department of Defense (DoD). In the words of the U.S. Senate Armed Services Committee, the DoD was facing a "flood of counterfeits" in its supply chain. "Looking at just part of the supply chain over a two-year period from 2009 to 2010, the investigation uncovered approximately 1,800 cases of suspect counterfeit electronic parts. The total number of individual suspect parts involved in those cases exceeded one million."[11]

The examples of counterfeits found in the U.S. Senate Armed Services Committee and U.S. General Accounting Office investigations into defense procurement alone included fake airplane parts, communications and computer systems, protective equipment, GPS systems and even seat belts.[12] These findings led to legislation requiring the DoD to tighten requirements for defense contractors to address counterfeits.[13] An ongoing review is likely to result in further supplier and supply-chain compliance measures for U.S. government suppliers more broadly.

Corruption and IP theft infect government procurement contracts in every region of the world and across a wide range of products and services. A small sampling of recent headlines helps convey the scope and breadth of these problems:

RECENT INCIDENCES OF CORRUPTION

- In April 2012, three contractors pled guilty to conspiracy to commit bribery in a scheme involving U.S. Naval officers in North Island, California. In exchange for bribes of more than U.S.$1 million in checks, gift cards, electronics, and other products, Naval employees allowed the contractors to circumvent the bidding process and avoid competition for contracts worth millions of dollars. The Naval employees also signed off on items that were never delivered and made payment for fictitious work orders.[14]

- The EU Commissioner for Home Affairs, Cecilia Malmstrom, recently stated that an estimated €120 billion is lost to corruption in government procurement each year throughout the 27 EU Member States.[15] The anti-corruption group Transparency International has drawn a linkage between this corruption and the European region's ongoing fiscal crisis.[16]
- In February 2010, BAE Systems, one of the world's largest defense contractors, paid penalties of approximately U.S.$450 million to the U.S. Department of Justice and the UK Serious Fraud Office to resolve corruption claims and charges that it had conspired to make false statements to law enforcers about its anti-corruption undertakings. The BAE activities at issue included arms sales in Eastern Europe, the Middle East, and Africa.[17]
- In 2007, Baker Hughes Inc., a Texas-based provider of oil field products and services, agreed to pay more than U.S.$33 million to settle bribery charges in connection with energy contracts in Kazakhstan, Indonesia, Nigeria, and Angola, including charges that the company paid U.S.$5.2 million to two agents knowing that some or all of the money was intended to bribe government officials in Kazakhstan.[18]

COUNTERFEIT PARTS AND IP THEFT IN THE GOVERNMENT SUPPLY CHAIN

- In 2008, a U.S. military engineer estimated that as many as 15% of all spare and replacement microchips purchased by the DoD were counterfeit. As a result, "we are having field failures regularly within our weapon systems—and in almost every weapon system."[19] Suspect counterfeits range from seatbelt clasps to sophisticated GPS components used in radar systems and microprocessors used in F-15 fighter jet control systems.[20] One recent case involved "fake" Kevlar body armor.[21]
- In June 2013, the Kenya Medical Association (KMA) stated that the surge in counterfeit medicines in Kenya—which according to some estimates account for 30% of drugs sold in the country—was putting significant strains on Kenya's public healthcare system. "We are spending millions in correcting resistance to diseases such as malaria and tuberculosis because patients unknowingly take the [counterfeit] drugs, which have less or no medicinal value to cure them," stated KMA Chairman Elly Nyaim.[22]
- In January 2012, the U.S. Air Force suspended Hong Dark Electronic Trade Company of China and various of its subsidiaries from further government contracting after an investigation revealed that Hong Dark sold more than 80,000 suspect counterfeit electronic parts to DoD contractors and that many of these parts ultimately were installed on military aircraft. The investigation further revealed that Hong Dark's U.S. customer, which sold the parts to U.S. prime contractors, discovered the counterfeit nature of the parts as early as 2009 but failed to disclose this fact, which adversely impacted the government's ability to take effective remedial action.[23]
- Interpol's secretary-general recently noted that while 40 years of terrorism has killed 65,000 people globally, counterfeit medicines killed 200,000 people in China in one year alone. China has been pinpointed as the primary manufacturing source of counterfeit drugs being smuggled into the UK, but the drugs can change hands up to 30 times before reaching a British chemist.[24]
- According to U.S. Customs and Border Protection, counterfeit hardware components have led to network shutdowns in critical government systems, including the failure of a government agency's weather communication system.[25]
- In September 2012, Chinese national Sixing Liu, aka "Steve Liu," a former employee of the Space and Navigation Division of L-3 Communications, was convicted of stealing trade secrets relating to sensitive U.S. military technologies and exporting them to China. The trade secrets allegedly detailed the performance and design of military guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles.[26]
- In November 2010, a Florida woman pleaded guilty to helping her former employer, VisionTech, sell counterfeit computer chips that were ultimately purchased and used by the U.S. military. Prosecutors claimed that VisionTech would import counterfeit chips from Hong Kong and China, then "scuff up labels to make it impossible to tell if the devices in the box matched the code on the labels and use 'large erasers' to polish up the integrated circuits when they arrived in shoddy condition."[27] The fake chips were sold to several key defense contractors and were often destined for use in sensitive military products and programs.
- In July 2013, the U.S. Department of Justice announced the criminal indictment of a Massachusetts man for allegedly selling counterfeit semiconductors for use on nuclear submarines.[28] The indictment charges that from February 2007 through April 2012, the defendant, through two companies he owned and operated, purchased counterfeit semiconductors from sources in Hong Kong and China and sold them to customers throughout the United States, including companies believed by the defendant to be defense contractors supplying parts for nuclear submarines. In announcing the indictment, the Government noted that "[t]he introduction of defective equipment into the military supply chain can result in product failure, property damage and even serious bodily injury, including death. Some of these counterfeit devices can also be preprogrammed with malicious code and enable computer network intrusion."[29]

Governments across the globe increasingly are prescribing specific requirements and sanctions in their procurement rules to guard against these abuses and to promote responsible business practices.

III. EFFORTS BY GOVERNMENTS

IN RESPONSE to the challenges posed by corruption and IP theft in contractor supply chains, and to the specific cases of corruption and counterfeit parts described above, governments across the globe increasingly are prescribing specific requirements and sanctions in their procurement rules to guard against these abuses and to promote responsible business practices. Sanctions may include debarment from future government contracting and criminal penalties (including prison sentences for company officers or employees in egregious cases). In many cases, these obligations extend to subcontractors and others in the supply chain.

The importance of legal and regulatory compliance in U.S. government procurement may best be illustrated by the federal government's crackdown on contractors during Operation Ill Wind, a three-year investigation launched in 1986 by the U.S. Federal Bureau of Investigation into corruption by U.S. government and military officials and defense contractors.[30] Several government officials were convicted of various crimes, including an Assistant Secretary of the Navy, a Deputy Assistant Secretary of the Navy, and a Deputy Assistant Secretary of the Air Force. Dozens of private citizens also were convicted, including several major defense contractors, some smaller defense contractors, employees, and consultants.[31] The scandal led the U.S. Congress to pass the 1988 Procurement Integrity Act, which regulates the pay that procurement officials can receive from contractors during the first year after they leave government and forbids them to provide bid and proposal information to their new employers.

Since then, the U.S. Administration has remained active in tightening IP and ethics compliance requirements for

government contractors and their suppliers. The Federal Acquisition Regulation (FAR), which sets out the ground rules for contracting with the U.S. Government, was recently amended to strengthen the rules on business ethics and compliance. The rules now require government contractors (with some limitations) to have a written code of business ethics and conduct, promote a culture of compliance within their organizations, train employees, implement effective internal controls, conduct periodic reviews, and establish internal reporting mechanisms. Critically, the rules also require prime contractors to flow down this clause to subcontractors in many situations.[32] Contractors must have a compliance program in place within 30 days of being awarded a government contract and provide training on the program within 90 days.

The threat of debarment from government contracting likewise can incentivize government contractors to strengthen internal compliance and extend compliance oversight to subcontractors. For instance, U.S. law permits debarment officials to terminate or defer debarment proceedings "in consideration of the contractor's agreement to change its business processes, create or improve its ethics program and take other remedial actions to mitigate the risk that the misconduct will recur. Such is frequently reduced to writing in an 'Administrative Agreement, requiring outside, independent oversight by a monitor or ombudsman who reports to the debarring official."[33] U.S. debarment officials also often consider the existence and strength of a company's internal controls in determining whether to bring debarment proceedings against a contractor in the first instance.[34]

Other specific examples demonstrate this trend of governments to tighten up legal liability, management systems requirements, and ongoing review of compliance by contractors and their suppliers:

ANTI-CORRUPTION EFFORTS

- The FAR ethics rules discussed above require contractors to disclose certain violations of criminal law in connection with the award or performance of a government contract or subcontract[35]—which could require contractors to disclose corruption (or even IP theft) in their supply chains to the extent these relate to their fulfillment of a contract.
- The EU Public Procurement Directive, 2004/18/EC, requires Member States to adopt laws that exclude from participation in government procurement any bidder that has been convicted of corruption or fraud and permits them to exclude bidders for "grave professional misconduct."[36] The Directive also allows contracting authorities to impose specific contract performance conditions on successful bidders, in particular with regard to social and environmental issues.[37] Similar provisions exist in the EU Defence Procurement Directive, 2009/81/EC.[38]
- Scotland recently launched a Best Practices initiative through its Procurement Information Hub that provides spending and supplier data for many government contractors. The Best Practice Indicators include core evaluation factors, such as procuring goods and services in a lawful and ethical manner, as well as a requirement for the delivery of quality products and services. This is believed to be the first public sector spending analysis of this level anywhere in Europe.[39]
- Mexico recently passed a law prohibiting acts or omissions aimed at achieving an "unlawful advantage" in procurements with the Mexican federal government.[40] The law applies not only to contractors, but also to suppliers and subcontractors.[41] Corporations can be fined up to $10 million for violations.[42]
- The World Bank's guidelines on procurement using Bank funds require suppliers, contractors, and subcontractors to "observe the highest standard of ethics during the procurement and execution of Bank-financed contracts."[43] It also imposes a range of penalties if a recipient is found to have engaged in "corrupt, fraudulent, collusive, coercive, or obstructive practices" in connection with the procurement—terms that the guidelines define broadly to potentially cover a range of illegal or unethical practices.[44] In many cases, a key condition for firms found to have violated this requirement is to establish an internal integrity compliance program; the Bank recently published guidelines to help companies develop such programs, which include obligations to seek compliance commitments from suppliers and other business partners as well.[45]
- The "Integrity Pact" developed by Transparency International, a leading anti-corruption NGO, is an innovative tool whereby contract bidders jointly agree not to engage in various corrupt or collusive practices.[46] Because the Pacts apply to all potential bidders, "[c]ompanies can refrain from bribing in the knowledge that their competitors are bound by the same rules."[47] Since their inception in the 1990s, Integrity Pacts have been used in more than 15 countries, including Argentina, Colombia, Ecuador, Germany, Indonesia, Mexico, Pakistan, and Paraguay.[48] Governments have seen savings of 30% to 75% as a result of using the Pacts.[49]

REQUIRING IP COMPLIANCE

- Executive Order ("EO") 13103, signed by former U.S. President Clinton on September 30, 1998, imposes obligations on federal contractors to ensure that they are not violating IP rights in software. Specifically, Section 1(c) of the EO provides that "Contractors and recipients of Federal financial assistance . . . should have appropriate systems and controls in place to ensure that Federal funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws."[50] The Obama Administration has committed to reviewing the steps federal agencies have taken to implement EO 13103.[51] Similarly, under California procurement

law, a state contractor must "certify that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Contract for the acquisition, operation or maintenance of computer software in violation of copyright laws."[52]

- Section 1603 of the National Defense Authorization Act of 2013 requires the Secretary of Defense to develop a national strategy for reducing, to the maximum extent practicable, the presence of counterfeit parts in the supply chain. In furtherance of this objective, Section 807 of the Act promotes the use of unique identification technologies to track assets in the possession of contractors or deployed in the Armed Forces.
- The U.S. DoD recently proposed rules that would require contractors to establish and maintain a counterfeit electronic part avoidance and detection system, which would include training, inspection and testing of electronic parts, and mechanisms to enable the traceability of parts to suppliers.[53] The purpose of these rules would be to shift the burden of detecting and avoiding the use of counterfeit electronic parts in DoD procurements to contractors. To help achieve this objective, the rule would prohibit contractors from claiming reimbursement for the cost of replacing counterfeit electronic parts or related corrective action cost. In anticipation of this rule, contractors have begun demanding additional contractual protections against counterfeit parts and negotiating the issue of shared liability with their suppliers.[54]
- In December 2011, the European Commission published a proposal to revise the EU Public Procurement Directive that, in addition to reaffirming that government contracts should not be awarded to companies that have been found guilty of corruption or fraud, also would authorize contracting authorities to exclude bidders for violations of competition rules or intellectual property rights.[55]
- Mexico regularly conducts audits of government agencies to identify unlicensed software use and publicly discloses the results. The government has begun cracking down on non-compliant companies through audits, fines, and referrals to tax authorities.[56] Specifically, in 2010 the Mexican government published the Administrative Manual of General Application in the Field of Information Technology and Communications (MAAGTIC), making implementation of the stated rules governing ICT mandatory for all federal agencies[57]. After investing 2 years instituting MAAGTIC requirements within their own agency, the Secretaria de Economia (Mexican Ministry of Economy) went a step further by becoming the first governmental agency to become Verafirm Certified, an ISO 19770-1 software asset management standards-based certification administered by BSAI The Software Alliance. The then Secretary of Economy Bruno Ferrari explained that the decision to adopt best practices for software asset management reflects the Mexican government's respect for intellectual property and noted that the government must lead by example in assuring no piracy is occurring.[58]

In light of this growing web of government procurement rules on corruption and IP theft,[59] companies increasingly face the need to adapt their business practices and processes, particularly with their supply chain, to maintain their ability to bid on government contracts. In addition to ensuring legal compliance and minimizing risk, effective management of IP and anti-corruption practices also can help companies operate more effectively and successfully.

Governments and industry have a shared interest in promoting broader adoption of such practices. First, virtually all government procurement rules on corruption and IP theft target practices that, if left unaddressed, can undermine a company's ability to build employee trust and loyalty, and can also divert employee focus away from their core tasks of succeeding on company merits. Second, the failure to root out corruption, fraud, or theft can quickly lead to a broader culture of non-compliance within a company, affecting even core areas that can imperil the company's financial foundations. Third, many of these practices can open a company to substantial monetary liabilities to shareholders or customers, and even criminal liability.

Industry response to the 2008 U.S. FAR ethics and compliance rules, summarized above, supports this view. As requested by Congress, the Government Accountability Office conducted a survey in 2009 to determine, among other things, how large DoD contractors perceived the new rules.[60] While some initially expressed concern that these rules would impose too many costs and burdens on contractors, the survey revealed that these contractors and others actually saw important benefits to the new rules. These included:

- Codifying good business practice for all contractors;
- Contributing to a company culture emphasizing business integrity;
- Providing standards that helped create a level playing field;
- Building employee trust and confidence;
- Reducing contractor liability and risk.[61]

Moreover, studies have shown that a robust compliance program can actually increase a company's bottom line.[62] Indeed, a consortium of five of the world's leading accountancy associations recently endorsed a model framework that recognizes the importance of robust internal compliance controls, including measures to ensure respect for IP rights in technology.[63] Conversely, companies that fail to implement compliance programs may be subject to liability under the U.S. Foreign Corrupt Practices Act, False Claims Act and other laws.[64] For example, a hospice company was required to pay $6.1 million for submitting false claims which arose, in part, from an inadequate compliance program.[65]

The European Commission published a proposal to revise the EU Public Procurement Directive that, in addition to reaffirming that government contracts should not be awarded to companies that have been found guilty of corruption or fraud, also would authorize contracting authorities to exclude bidders for violations of competition rules or intellectual property rights.

BEST PRACTICES:

- Promote transparency in supply chains.
- Encourage greater supply chain accountability.
- Foster cooperation and information sharing.
- Develop “risk maps” to identify high-risk activities by suppliers.
- Encourage close cooperation on responsible supply chain practices.

IV. BEST PRACTICES TO FOSTER COMPLIANCE

AS THE PRIOR SECTIONS illustrate, governments are increasingly assertive in requiring government contractors to eliminate fraud, corruption, and IP theft from their operations and their supply chains. Given the sheer magnitude of government spending and the potential reach of these requirements deep into procurement supply chains, companies across the economy have much to lose if they fail to adopt adequate safeguards and compliance programs that help root out corruption, fraud, and IP theft and also promote a culture of integrity and legal compliance.

While any specific proposals in this area necessarily must be tailored to the size, scope, and nature of the company and its business, the recommendations below can help provide a useful framework for companies to proactively address these issues before they cause problems—and to help government procurement officials adopt consistent, pragmatic rules in this area that do not impose undue burdens or costs on industry. Adherence to these best practices will also help companies comply with many of the key procurement compliance requirements described above, and to improve their management systems and compliance more generally.

- Promote transparency in supply chains. Transparency is a cornerstone principle of nearly all government procurement regimes because it helps eliminate opportunities for parties to engage in corruption and theft. As the OECD notes, "corruption thrives on secrecy."[66] Companies should strive for greater transparency in their supply chains while also demanding greater transparency from suppliers about their own practices. To this end, contractors should press suppliers to adopt robust internal controls on fighting corruption and respect for IP rights and should work with and monitor key suppliers to ensure that these controls are followed in practice.
- Encourage greater supply chain accountability. Meaningful change is unlikely to occur unless suppliers are held accountable for their actions. Companies should include contractual commitments that impose the same ethics and compliance responsibilities on suppliers that apply to the companies themselves. Contractors should strictly prohibit suppliers from supplying counterfeit parts or engaging in any form of IP theft or corruption. Contractors should also consider adopting "hotlines" for anonymous reporting of problems with suppliers, and should insist on the ability to conduct third-party audits of relevant supplier practices.
- Foster cooperation and information sharing. Meaningful transparency is difficult to achieve when each party is working in isolation and fails to share relevant information. Governments should encourage contractors and their suppliers to share information–both with relevant government agencies and with other industry participants–on problematic suppliers, risk signals, and other relevant data that can help all parties identify potential problems and take appropriate mitigation steps. To avoid claims of illegal collusion, contractors should consider sharing such information through third parties that can provide independent assessments, verify information, and serve as a trusted repository of data.
- Develop "risk maps" to identify high-risk activities by suppliers. The risk that suppliers might be engaging in corrupt practices, IP theft, or other illegal practices is likely to vary significantly depending on the nature and scope of the contract at issue, the types of IP used by suppliers, and other factors. Specific risk criteria may also include changes in key management, extensive use of subcontractors, deterioration in a supplier's finances, or a history of non-compliance. Companies should work internally and collaboratively (with third-party providers, trade associations, and others) to develop "risk maps" that identify the highest-risk suppliers and activities, which can then form the basis for developing targeted and cost-effective mitigation strategies.
- Encourage close cooperation on responsible supply chain practices. This recommendation builds upon the sixth recommendation in the OECD's Principles for Integrity in Government Procurement[67] by recognizing that contractors and suppliers play a vital role in helping maintain integrity in procurement–and that voluntary industry action is preferable to inflexible rules. As the OECD notes, "suppliers should . . . be encouraged to take voluntary steps to reinforce integrity in their relationship with the government. These include codes of conduct, integrity training programmes for employees, corporate procedures to report fraud, . . . [and] certification and audits by a third independent party."[68]

Government efforts to drive improvements in responsible supply chain practices through procurement requirements should signal to all companies the importance of eradicating corruption, fraud, and IP theft in supply chains, particularly if those companies want to do business with government or with other government contractors. Through cooperation with industry and a commitment to act first and foremost through voluntary best practices, governments and their private-sector suppliers have the potential to achieve meaningful benefits for themselves and for society more broadly.

ENDNOTES

[1] See Organization for Economic Cooperation and Development (OECD), Principles for Integrity in Public Procurement 9 (2009), at http://www.oecd.org/gov/ethics/48994520.pdf; see also Transparency & Accountability Initiative, Opening Government: A guide to best practice in transparency, accountability and civic engagement across the public sector (2011), at http://www.transparency-initiative.org/wp-content/uploads/2011/09/Opening-Government.pdf.

[2] See OECD, supra n. i, at 9.

[3] See Paul R. Schapper, Corruption and Technology in Public Procurement 6, World Bank (Apr. 2007), at http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/CorruptionversusTechnologyinPublicProcurement.pdf.

[4] Gerald H. Lander, Valerie J. Kimball, and Kimberly A. Martyn, Government Procurement Fraud: Could SOX Be Used to Hold Contractors Accountable?, The CPA Journal Online (Feb. 2008), at http://www.nysscpa.org/cpajournal/2008/208/infocus/p16.htm (last visited January 10, 2013).

[5] See Government Accountability Office, Government Contracting: Federal Efforts to Assist Small Minority Owned Businesses (Sept. 2012), at http://www.gao.gov/assets/650/648985.pdf.

[6] Jeanne Sahadi, Cutting Washington Could Hit Main Street, CNN Money (July 23, 2012), at http://money.cnn.com/2012/07/23/news/economy/federal-spending/index.htm.

[7] Id.

[8] For example, Sections 1701 through 1708 of the 2013 National Defense Authorization Act authorize the U.S. Government to punish government contractors or subcontractors that engage in certain activities related to labor violations or sex trafficking. See 22 U.S.C. §§ 1101, 1351, 2313, 7103, 7104. In California, state government contractors must certify compliance with the state's Sweatfree Code of Conduct and ensure that their subcontractors comply in writing with the Code, under penalty of perjury. Cal. Pub. Cont. Code § 6108(g).

[9] In October 2009, President Obama signed Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance, which requires federal agencies to set and meet specific sustainability related targets. GSA and EPA lead a working group to identify ways to make the U.S. Government's supply chain more sustainable and have launched multiple initiatives to that effect. See, e.g., General Services Administration, Greening The Supply Chain, at http://www.gsa.gov/portal/content/285653.

[10] For example, a 2012 study commissioned by the Business Software Alliance found that 68% of software in emerging markets was pirated, compared to 24% in developed nations. See Business Software Alliance, Shadow Market: 2011 BSA Global Software Piracy Study 9 (May 2012), at http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf; see also The Conference Board, Safeguarding Intellectual Property and Addressing Corruption in the Global Supply Chain (Dec. 2012), at http://www.conference-board.org/publications/publicationdetail.cfm?publicationid=2379. A survey by McAfee rated China, Pakistan, and Russia as countries posing the greatest threat to IP infringements. See McAfee, Unsecured Economies: Protecting Vital Information (2009), at http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

[11] Comm. on Armed Serv's, U.S. Senate, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain i-ii, S. Rep. No. 112-167 (2012), at http://www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf.

[12] See, e.g., U.S. General Accounting Office, Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts (Mar. 2010), at http://www.gao.gov/products/GAO-10-389.

[13] National Defense Authorization Act for Fiscal Year 2012, Pub. L. 112-81, Sec. 848 (enacted Dec. 31, 2011), at http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf.

[14] Inspector General, U.S. Department of Defense, Semiannual Report to the Congress 43-55 (Sept. 2012), at http://www.dodig.mil/sar/SAR_OCT_2012_web.pdf.

[15] See Nikolaj Nielsen, €120 billion lost to corruption in EU each year, EUObserver.com (Mar. 6, 2013), at http://euobserver.com/justice/119300.

[16] Id.

[17] See Steven A. Tyrrell, DoJ Prosecution of BAE Heralds Continued Aggressive FCPA Enforcement Environment (Feb. 8, 2010), at http://www.weil.com/news/pubdetail.aspx?pub=9725.

[18] U.S. Securities and Exchange Commission, SEC Charges Baker Hughes With Foreign Bribery and With Violating 2001 Commission Cease-and-Desist Order (Apr. 26, 2007), at http://www.sec.gov/litigation/litreleases/2007/lr20094.htm.

[19] Brian Grow et al., Dangerous Fakes, Business Week (Oct. 1, 2008), at http://www.businessweek.com/stories/2008-10-01/dangerous-fakes.

[20] Id. at 24-26.

[21] 157 Cong. Rec. S4183 (daily ed. June 29, 2011) (statement of Sen. Whitehouse), at http://www.whitehouse.senate.gov/news/release/whitehouse-counterfeits-pose-danger-to-our-troops.

[22] Rajab Ramah, Kenya: Counterfeit Drugs Pose Public Health Threat in Kenya, allAfrica.com (June 13, 2013), at http://allafrica.com/stories/201306140050.html.

[23] See Department of the Air Force, Memorandum in Support of the Suspensions of Hong Dark Electronic Trade Company et al. (Jan. 13, 2012), available at http://stevezeva.homestead.com/Suspension_Memo.pdf.

[24] Mark Townsend, Health Fears Grow as Fake Drugs Flood into Britain, The Guardian (Jan. 3, 2009), at http://www.guardian.co.uk/business/2009/jan/04/fake-pharmaceuticals-drugs-china-nhs.

[25] See Peter Hlavnicka, Debunking Common Myths About Counterfeits, BusinessWeek (Mar. 1, 2010), at http://www.businessweek.com/stories/2010-03-01/debunking-common-myths-about-counterfeitsbusinessweek-business-news-stock-market-and-financial-advice. .

[26] U.S. IP Enforcement Coordinator, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (Feb. 2013), Annex B-2, at http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[27] Robert McMillan, Woman helped sell fake chips to US military, PC World (Nov. 23, 2010), at http://www.pcworld.idg.com.au/article/369021/woman_helped_sell_fake_chips_us_military/.

[28] U.S. Department of Justice, Massachusetts Man Charged with Selling Counterfeit Semiconductors Intended for Use on Nuclear Submarines (July 15, 2013), at http://www.justice.gov/opa/pr/2013/July/13-crm-790.html.

[29] Id.

[30] See, e.g., Irwin Ross, Inside the Biggest Pentagon Scam, CNN Money (Jan. 11, 1993), at http://money.cnn.com/magazines/fortune/fortune_archive/1993/01/11/77357/index.htm.

[31] Id.

[32] 73 Fed. Reg. 67064; FAR Case 2007-006, Contractor Business Ethics Compliance Program and Disclosure Requirements (Nov. 12, 2008).

[33] Steven A. Shaw, Deputy General Counsel, U.S. Department of the Air Force, Government Tools to Encourage Ethical Conduct of their Contractors 2 (Feb. 27, 2009), at http://www.safgc.hq.af.mil/shared/media/document/AFD-110314-025.pdf.

[34] Id. at 3.

[35] FAR Parts 3, 9, 42, 52.

[36] OJ L 134, 30.4.2004, p. 114, recital 43 and art. 45, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:134:0114:0240:EN:PDF.

[37] Id., recital 33 and art. 26.

[38] OJ L 134, 30.4.2009, p. 1 (recital 41 and arts. 20-21, 39), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:216:0076:0136:EN:PDF.

[39] The Scottish Government, Best Practice Indicators for Public Procurement in Scotland: Guidance (2008), at http://www.scotland.gov.uk/Resource/Doc/225104/0060921.pdf.

[40] Mónica Schiaffino & Rogelio Alanis Robles, Mexico's New Federal Anti-Corruption in Public Contracts Law, Littler (June 13, 2012), at http://www.littler.com/publication-press/publication/mexicos-new-federal-anti-corruption-public-contracts-law.

[41] Victoria Prussen Spears, Companies Doing Business in Mexico Should Focus on New Anti-Corruption Law, 4 Financial Fraud Law Report 701 (Sept. 2012), at http://meyerowitzcommunications.com/writings-victoria-spears_2_1516943952.pdf.

[42] Id.

[43] See World Bank, Guidelines: Procurement of Goods, Works, and Non-Consulting Services Under IBRD Loan and IDA Credits & Grants by World Bank Borrowers 6 (Jan. 2011), at http://siteresources.worldbank.org/INTPROCUREMENT/Resources/278019-1308067833011/Procurement_GLs_English_Final_Jan2011.pdf.

[44] Id. at 7; see also id. (defining "fraudulent practice" as "any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation").

[45] See World Bank, Debarment with Conditional Release & Integrity Compliance, at http://siteresources.worldbank.org/INTDOII/Resources/Integrity_Compliance_Guidelines.pdf.

[46] See Transparency International, The Integrity Pact: A Powerful Tool for Clean Bidding (2009), at http://www.transparency.hu/uploads/docs/integrity_pact.pdf.

[47] Id.

[48] Id. at 6.

[49] Id.

[50] Exec. Order No. 13,103, 3 C.F.R. 221-223 (1999), reprinted in 40 U.S.C. § 11101 note (2011). The EO further provides that, "[i]f agencies become aware that contractors or recipients are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determine that such actions of the contractors or recipients may affect the integrity of the agency's contracting and Federal financial assistance processes, agencies shall take such measures . . . as the agency head deems appropriate and consistent with the requirements of law." Id.

[51] See IPEC, 2013 Joint Strategic Action Plan On Intellectual Property Enforcement 14 (June 2013), at http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

[52] See California Department of General Services, General Provisions—Information Technology §39(e), at http://www.documents.dgs.ca.gov/pd/modellang/GPIT060810.pdf; General Provisions for Non-IT Commodities §36(f), at http://www.documents.dgs.ca.gov/pd/modellang/GPnonIT0407.pdf.

[53] DoD, Proposed Rule: Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012–D055), 78 Fed. Reg. 28780 (May 16, 2013), at http://www.gpo.gov/fdsys/pkg/FR-2013-05-16/pdf/2013-11400.pdf.

[54] Nicole Blake Johnson, Feds, Industry Split Over Counterfeit Parts Strategy, Federal Times (Nov. 26, 2012), at http://www.federaltimes.com/article/20121126/DEPARTMENTS01/311260007/Feds-industry-split-over-counterfeit-parts-strategy.

[55] European Commission, Proposal of 20 December 2011 for a Directive of the European Parliament and of the Council on Public Procurement, COM(2011) 896 final, recitals 34 and 55, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0896:FIN:EN:PDF.

[56] See Jodie Kelley, Mexico's Impressive IP Leadership, TechPost (Aug. 8, 2011), at http://blog.bsa.org/2011/08/08/mexicos-impressive-ip-leadership/.

[57] http://www.maagtic.com/2010/08/que-es-maagtic.html

[58] http://techpost.bsa.org/2012/11/30/mexicos-foresight/

[59] Government efforts to rid procurement supply chains of corruption and IP theft are fully consistent with applicable international trade rules. For instance, the WTO's Agreement on Government Procurement (GPA), the leading international instrument in this area, seeks to advance the goals of non-discrimination and transparency in procurement. See, e.g., WTO, Overview of the Agreement on Government Procurement, at http://wto.org/english/tratop_e/gproc_e/gpa_overview_e.htm. While a key goal of transparency is to deter discrimination, it also helps uncover and eradicate corruption. As one NGO has explained, "Transparency in government procurement helps reduce corruption by permitting public oversight of the use of public funds. It increases the likelihood that public institutions will function fairly, openly and efficiently . . ." Transparency & Accountability Initiative, supra n. i, at 67. GPA parties also have consistently interpreted the agreement to allow measures designed to fight corruption and protect property rights, so long as these measures do not discriminate against foreign products, services, or suppliers. The reason for this is clear: corruption and theft by contractors or in their supply chains distort competition by giving an advantage to suppliers that succeed by virtue of illegal practices and deception rather than based on the merits of their offerings.

[60] See U.S. Government Accountability Office, Defense Contracting Integrity: Opportunities Exist to Improve DOD's Oversight of Contractor Ethics Programs, GAO-09-591 (Sept. 2009), at http://www.gao.gov/new.items/d09591.pdf.

[61] Id. at 10.

[62] Tiffany McDowell, Deloitte's Three Ways to Instill Ethical Guidelines: How Promoting and Enforcing Ethical Policies Can Have a Positive Impact on The Bottom Line, 5 Strategic HR Review 16–19 (2006).

[63] See Committee of Sponsoring Organizations of the Treadway Commission, Internal Control – Integrated Framework: Framework and Appendices 100 (May 2013) (endorsing compliance methodology designed to provide "appropriate controls over changes to technology, . . [including] verifying the entity's legal right to use the technology in the manner in which it is being employed").

[64] Clay Hagedorn & Chadd Tierney, Polsinelli Shughart PC, Designing and Implementing an Ethical Compliance Program: A Primer, Aspatore (2011), at http://www.polsinelli.com/files/Publication/33fd94bc-638f-4c6b-8327-5a8d734e7c4b/Presentation/PublicationAttachment/65558704-3cd1-4487-8a4b-5af1378f4f99/Government%20Contracting%20Chapter.pdf.

[65] U.S. Department of Justice, Hospice Care of Kansas and Texas-based Parent Company to Pay $6.1 Million to Resolve Allegations of False Claims (June 21, 2012), at http://www.justice.gov/opa/pr/2012/June/12-civ-768.html.

[66] See OECD, supra n. i, at 10.

[67] Id.

[68] Id. at 12.

CREATe.org
Center *for* Responsible Enterprise And Trade