THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

International Procurement

STEVEN D. TIBBETS, MARTIN G. MASSE, KRISTINA DAHMANN,
AND BRENDA C. SWICK*

This article reviews international law developments in the field of international procurement in 2013.

I. Security and Origin Issues in Government Procurement of Commercial Software: Ships Passing in the Night or Looming Collision?

The issue of cybersecurity has been a hot topic in U.S. policy in recent years. Noteworthy developments related to cybersecurity occurred in 2013, and more are likely to occur in coming years. One of the primary concerns cybersecurity measures seek to address is the threat posed by malicious code hidden in software that is introduced into sensitive environments, such as those related to the military or critical infrastructure. Methods of combatting this threat include both testing and vetting processes and improving knowledge regarding the origin of software and the identities of actors who may have had access to software at some point in development processes—processes that often cross national borders.

While public policy is being enhanced to promote cybersecurity, particularly with respect to software purchased by government agencies, the software development industry is becoming increasingly globalized, which makes complete knowledge of, and control over, software development processes difficult to achieve. In addition, public policy increasingly favors the government procurement of commercial software and commercial "cloud" services that leverage software products with regard to which the government has little visibility or control. Software companies must leverage global supply chains in order to obtain the labor they need at costs that allow them to compete, particularly with regard to commercial software. Thus, there is a tension between cybersecurity and the globaliza-

* Steven D. Tibbets of Steese, Evans & Frankel, P.C. and Martin G. Masse of McMillan, LLP were the editors of the International Procurement Committee's Year in Review for 2013. Steven Tibbets authored Section I on "Security and Origin Issues in Government Procurement of Commercial Software: Ships Passing in the Night or Looming Collision?" Kristina Dahmann authored Section II on "Recent Developments in Chilean Procurement Law." Brenda C. Swick, Co-chair of the Public Procurement Group at the firm McCarthy Tétrault, LLP authored Section III on "Significant Developments in Canadian Public Procurement Law." The views of the authors are not attributable to their law firms, companies, or government agencies. The article covers developments during 2013.

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

tion trend in software development. Legal developments during 2013 suggest that this tension is far from being resolved. Companies seeking to comply with cybersecurity requirements while still producing software that allows them to stay competitive face unprecedented challenges.

This section summarizes legal authorities applicable to the development of software purchased by the U.S. Government, describes legal developments that occurred in 2013, and offers thoughts regarding additional developments likely to occur in the coming months and years.

A. U.S. Federal Policy Favors Commercial Software and "Cloud Solutions," Which Tends to Reduce Customer Control and Visibility with Respect to Software Development

Broadly speaking, the term "cloud computing" refers to the practice of using a network of remote servers hosted on the Internet, rather than a local server or a personal computer, to store, manage, and process data. The Executive Branch of the U.S. Government has embraced a "cloud first" strategy that favors shifting as much information technology to cloud formats as possible.[1] The amount of information technology the U.S. Government is likely to shift to cloud formats is substantial. According to a 2011 report by the U.S. Chief Information Officer, "[a]n estimated $20 billion of the Federal Government's $80 billion in [information technology (IT)] spending is a potential target for migration to cloud computing solutions."[2]

A shift to cloud computing blurs the lines between the portions of an IT system a customer owns and controls and the portions a vendor owns and controls. As one commenter on cloud solutions has noted,

> [a]s Asian networking moves into the era of 'everything cloud' and Big Data becomes more prevalent, the distinction between the data center resources an enterprise owns and those that it accesses on-demand, will gradually blur – creating the data center without walls. A performance-on-demand approach to allocation of networking resources will offer the best [return on investment] combined with the business critical performance most enterprises need.[3]

Thus, the policy preference for the government to use "cloud" IT solutions will tend to erode the amount of control over, and visibility with respect to, the software development process as government agencies exploit existing commercial products and vendor-hosted applications. Moreover, the "international dimension" of cloud computing introduces security challenges that government policies must evolve to address.[4]

This is not to say that cloud solutions are *per se* unsecure. They often incorporate security features, such as access limitations or processes for "cleansing" applications of

1. Vivek Kundra, Federal Cloud Computing Strategy 2 (2011), *available at* https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

2. *Id.* at 1.

3. Karl Horne, *Redefining the Network with an Open, Software-Defined Architecture*, InformationWeek (Nov. 13, 2013), http://www.informationweek.in/informationweek/perspective/286144/redefining-network-software-defined-architecture.

4. *See* Kundra, *supra* note 1, at 30.

government data when they are removed from a platform the government is using.[5] In fact, the field-tested nature of cloud solutions and the ability to switch providers relatively quickly in the event of security problems have been touted as a security benefit that government-developed IT platforms do not provide.[6] The point is that, despite these features, cloud solutions present a greater risk that threats were introduced during the development process than government-developed and government-managed software products.

B. Cybersecurity Developments in 2013

There were several U.S. Government public policy developments related to cybersecurity in 2013. On February 12, 2013, President Obama issued an Executive Order directing the National Institute for Standards and Technology (NIST) to develop a "Cybersecurity Framework" that provides, among other things, a "prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[7] Subsequently, on October 22, 2013, NIST released its preliminary Cybersecurity Framework to meet the Executive Order's requirements.[8] The Framework provides guidelines for federal government agencies, state and local government agencies, and private parties responsible for managing critical infrastructure to develop cybersecurity systems. It does not provide specific cybersecurity actions that government agencies or other parties must take—the closest the Framework comes to providing specific guidance regarding software development is listing "Supply Chain Risk Management" as an "[area] for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations."[9] The Framework acknowledges the lack of any clear standards or best practices for minimizing cybersecurity risks in the software supply chain: "[s]upply chain risk management, particularly in terms of product and service integrity, is an emerging discipline characterized by diverse perspectives, disparate bodies of knowledge, and fragmented standards and best practices."[10] Beyond that, several bills related to cybersecurity were introduced in the U.S. Congress in 2013, but, as of the writing of this article, none have been enacted into law. As one commenter opined as recently as 2008, "[u]ntil federal and state governments provide definitive guidance, U.S. companies will be on their own in convincing government customers that their [overseas]-developed software is secure."[11]

---

5. *Id.* at 20, 22.

6. *Id.* at 27.

7. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013). The Executive Order addresses a number of cybersecurity issues and measures that have already received a great deal of media attention, such as the possibility of a requirement that private firms must share information about cyber attacks with the government and other private firms. This article focuses only on cybersecurity as it relates to the software-development supply chain.

8. Nat'l Inst. Standards Tech., Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework (2013) *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

9. *Id.* at 36.

10. *Id.* at 39.

11. David A. Kessler, *Protection and Protectionism: The Practicalities of Offshore Software Development in Government Procurement*, 38 Pub. Cont. L. J. 1, 44 (2008).

C. U.S. Government Procurement Country-of-Origin Requirements Do Not Promote Control over the Software Development Process

U.S. Government procurement laws and regulations require agencies to entertain offers for products manufactured abroad. Agencies must further establish that any geographic limitation they impose is necessary to fulfill *bona fide* security needs.[12] These legal rules are somewhat at odds with the cybersecurity goal of achieving greater control over cross-border software development processes.

Broadly speaking, a statute called the Buy American Act (BAA) and implementing U.S. procurement regulations provide that agencies may procure items manufactured only in the United States, but there are a number of exceptions.[13] Procurements of certain information technology items and procurements over certain dollar thresholds may include items manufactured in countries with which the United States has free trade agreements.[14] These are referred to as "designated countries" in the Trade Agreements Act (TAA) and implementing regulations.[15] A number of software development hotbeds, including China and India, are not designated countries.[16]

Business software is often made up of pre-existing software and new code developed to tailor the pre-existing software for a new purpose. Thus, the software the government buys often has been developed in a multi-step process, or a series of multi-step processes, over time and in a variety of locations. Generally, where an item is manufactured in a process involving multiple actions carried out in different countries, the item's "country of origin" is the last place that component materials or subassemblies were "substantially transformed" into an item with a new name, character, or use.

The concept of substantial transformation applies to software. In terms of guidance regarding how it applies to software, there is only one non-binding advisory ruling about software developed through actions in different geographic locations.[17] The country of origin was the country where the "software build" occurred—described in the decision as "the process of methodically converting the source code files into standalone lines, routines and subroutines of software object code that can be run by a computer." The country of origin was the country where a roadmap for the next release of the product was prepared, a graphical user interface was developed, a specification and architecture was developed and written, source code was programmed, testing and validation occurred, or software was burned onto media.[18] To summarize, even where a contract imposes country-of-origin limitations, software may be developed through processes that occur in numerous countries, both "designated" and not. This, in theory, exposes the software to

12. *See* Technosource Info. Sys., LLC, et al., B-405296, 2011 CPD ¶ 220 (Comp. Gen. Oct. 17, 2011) (rejecting agency's attempt to impose geographic limitations on where data centers could be located because agency failed to provide a justification for imposing the limitation and Trade Agreements Act clause in solicitation did not apply to the location of data centers).

13. 48 C.F.R. § 25.001(a) (2013).

14. *Id.* §§ 25.001(b), 25.103(e).

15. *Id.* §§ 25.003, 25.403-25.408.

16. *Id.* §§ 25.003, 25.403-25.408.

17. Letter from Monica R. Brenner, Chief of Valuation & Special Programs Branch, U.S. Customs and Border Prot., to Fernard A. Lavallee, DHL Piper LLP (June 8, 2012) *available at* http://www.dlapiper.com/files/upload/Talend-US-Customs-and-Border-Protection-decision.pdf.

18. *Id.*

greater security threats than if the country of origin were more restricted. Agencies certainly may impose geographic limitations above and beyond the requirements of the BAA or TAA for security purposes, but agencies must have a well-documented and reasonable rationale for the specific limitations they impose in order to withstand a legal challenge.[19]

D. A Great Deal of Commercial Software Is Developed in Places That Are Perceived as Posing Cybersecurity Threats

Commenters have noted that the software industry relies heavily, and increasingly, on relatively inexpensive labor located in Asia. "[T]he seemingly perpetual difficulty faced by U.S. software companies has been to find a sufficient number of skilled computer programmers at a reasonable cost . . . . Over the past decade [1998 to 2008], many U.S. software companies turned their search for programming talent to the rapidly expanding and educated populaces of countries such as India."[20]

At the same time, U.S. Government agencies investigating IT security have identified the development of software in foreign countries as a security threat. According to a 2012 Government Accountability Office report, officials at national-security-related departments of the U.S. Government, including the Department of Energy, the Department of Homeland Security, the Department of Justice, and the Department of Defense, reported that their agencies "have not determined or tracked the extent to which their telecommunications networks contain foreign-developed equipment, software, or services."[21] An earlier GAO report from 2004 noted a trend that the U.S. Department of Defense was increasingly reliant on commercial-off-the-shelf software and on suppliers that were using offshore locations and foreign companies for software development.[22] Likewise, in 2005, a Department of Defense software task force found that the globalization of software development has benefitted the department in the form of lower development costs and increased quality.[23] Thus, the trend of U.S. Government agencies using software developed overseas, and related security risks, is likely to continue and increase.

E. Conclusion

To review, 2013 saw the release of a cybersecurity Executive Order and a subsequent implementing and authoritative "Framework" prepared by NIST. As of this writing, cybersecurity legislation is pending, and it is expected that companies reliant on information technology generally, and government contractors providing information technology items specifically, will face new cybersecurity rules that affect the structure and management of software development supply chains. At the same time, the market trends that

19. *See* Technosource, *supra* note 12.

20. Kessler, *supra* note 11, at 3–4.

21. U.S. Gov't Accountability Office, IT Supply Chain: National Security-Related Agencies Need to Better Address Risks 1 (2012), *available at* http://www.gao.gov/assets/590/589568.pdf.

22. *See* Kessler, *supra* note 11, at 31–32 (discussing U.S. Gov't Accountability Office, Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks 2 (2004), *available at* http://www.gao.gov/new.items/d04678.pdf).

23. *See* Kessler, *supra* note 11, at 34 (discussing Def. Science Bd., Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software (2007), *available at* http://www.acq.osd.mil/dsb/reports/ADA486949.pdf).

encourage companies to develop software overseas and encourage government agencies to exploit "cloud" solutions will continue unabated. Rather than clarifying the situation, developments in 2013 tend to underline just how far we seem to be from resolving the tension between globalization trends and security concerns. It remains to be seen whether legal rules will develop to resolve the tension or whether the software and information technology industries will be left to muddle through. In the meantime, expect U.S. Government customers to address issues of software origin and security on an ad hoc, contract-by-contract basis.

II. Recent Developments in Chilean Procurement Law

A. Introduction

In 2003, the Chilean government adopted its current procurement system, Chilecompra, after a lengthy approval process.[24] The Chilean government modeled the Chilecompra after the Spanish procurement system, and the Chilecompra mirrors many components of the current U.S. procurement system.[25] Originally enacted for several principal reasons, today's Chilean procurement system accomplishes these original goals and continues to expand, save money, provide transparency, and develop as it plans to adapt its bid protest and contract dispute procedures.

The original aims of the Chilecompra include efficiency, cost saving, openness and transparency, and commitment to outside investment. The Chilecompra is an e-procurement system located entirely on-line.[26] The Internet portal saves the Chilean government money each year because the government can more easily acquire the lowest cost bidders. The system enables long-term relationships in which framework agreements are established that eliminate the need for the bid process entirely.[27] The Chilecompra's implementation demonstrated the Chilean government's commitment to both domestic and international investment. This aim is further fulfilled through the European Union-Chile Association Agreement, which provides a free trade area in goods, services, and government procurement.[28]

The current system's operations fulfill and continue these original goals as demonstrated by continued growth of contractor enrollment and continuously increasing the aggregate sum of contracts signed each year.

B. The System: In General

The procurement system is formally called *Dirección de Compras y Contratación Públicas*, while nevertheless maintaining the shorter name of its predecessor, Chilecompras.[29] The *Ministerio de Hacienda de Chile*, the Chilean Finance Ministry, is responsible for adminis-

24. *See generally* Catherine Weller et al., Sustainable Public Procurement: Where do we stand in Chile? (International Institute for Sustainable Development, 2008) [hereinafter Weller et al.].
25. *Id.*
26. *See ChileCompra*, Dirección ChileCompra, http://www.chilecompra.cl (last visited Jan. 19, 2014).
27. *Id.*
28. *See* The International Comparative Legal Guide to: Public Procurement 2012, Global Legal Group, 2 (Dec. 2011) [hereinafter Comparative Legal Guide].
29. *Id.*

tering the Chilecompra. The public procurement system is governed by *Ley de Compras Públicas*, Procurement Law No. 19,886 under Decree No. 250 made by the Finance Ministry in 2003. Additionally, the precursors Law No. 18,75 and Law No. 18,695 mandate that all government contracts require a public bidding process.[30] The entire system and forms involved are still written entirely in Spanish.[31] The Chilean procurement system regulates all forms of government procurement over a minimum threshold amount, which is lower for municipalities.[32]

C. The System: How It Works

Interested contractors must be registered on the Chilecompra's database system before the contractor may place a bid. Registration includes providing information that the company is solvent, legally exists according to its host country's laws, possesses required characteristics for the bidding process, and is compatible to bid in the procurement system's public market, *Mercado Publican*. This registration process is free.

There are three types of procurements: public tender, private tender, and direct contracts. Public tender is the standard public bidding process that allows all interested contractors to submit their bids as to why the government should award their company the contract. Private tender is a form of procurement in which a defined group of eligible contractors may place bids. Direct contracting occurs only when the government shows specific evidence for the need to target one contractor. Private tender and direct contracting occurs only in limited circumstances such as when no interested party exists for a public tender, the contract or the remainder of a pre-terminated contract is for below the required public tender threshold amount, a public emergency, a single source exists for the subject matter of the contract, foreign personnel contracts, or confidential subject matter.[33]

D. The System: Chilecompra Express

A registered contractor has the ability to be included on a list of priority government contractors called Chilecompra Express. These contractors have entered framework agreements with the Chilean Finance Ministry.[34] Once a company has entered a framework agreement, government agencies may enter into a contract with one of these priority contractors without undergoing the public tender process. These framework agreements are limited to services most frequently used by government agencies or to common high-volume transactions.[35]

---

30. *Id.*

31. *See generally Mecado Publico*, ChileCompra, www.mercadopublico.cl (last visited Jan. 9, 2014).

32. Comparative Legal Guide, *supra* note 28.

33. *Id.*

34. Weller et al., *supra* note 24; *see also ChileCompra Express*, Dirección ChileCompra, www.chilecompra.cl/index.php?option=com_content&view=article&id=88&Itemid=147 (last visited Jan. 19, 2014).

35. Weller et al., *supra* note 24.

E. The System: Dispute Resolution for Bid Protests

The procurement statutes dictate contractors eligible to contest an award. Once a contract is signed, an eligible company may apply directly to the government agency for relief and also may directly appeal to the Public Procurement Court. In addition, the Comptroller General of the Republic, the Chilean equivalent of the U.S. Inspector General, may intervene if the need arises.[36]

F. Recent Developments

The Chilean government awards an overwhelming number of contracts to small and micro businesses as defined by the Chilean government. In the first half of 2013, small and micro businesses received 91 percent of the awarded contracts. Chile defines "small business" as a company worth between 2,400 and 25,000 UF and "micro business" as a company worth less than 2,400 UF.[37] *Unidades Tributarias* or *Fiscalizadoras* (UF) is a standardized measurement used to establish something's value; its monetary value equivalent fluctuates daily. As of November 2013, Chile's Internal Revenue Service, *Servicio de Impuestos Internos*, listed the value of one UF as 23,190.54 pesos, roughly equal to U.S. $44. A small business's worth is between U.S. $10,000 and U.S. $1 million, and a micro business's worth is less than U.S. $10,000.[38]

Chile's e-procurement system has grown stronger and more popular. The increase in aggregate dollar amounts of contracts demonstrates the development of the process over the past decade.[39] The number of enrolled providers has more than tripled in the past ten years from 33,451 companies to 116,819 companies in 2013. In 2012, 850 government agencies contracted with 112,636 suppliers for U.S. $9.12 trillion, whereas in 2003, the government and supplier contracts totaled only U.S. $106.7.[40] The current system protects contractors through its stringent requirement of public tenders and transparent procedures. In addition, the system requires deadlines for notices and minimum posting time periods to show available contract opportunities. Regulations require the Chilean government to publicly post general evaluations when a contract's terms are fulfilled. Upcoming developments include a transformation of the review process. The current court includes a specialized three-judge panel available to hear actions alleging illegal or arbitrary government behavior. The future review process aims to be shorter and more expeditious.

In conclusion, Chile's e-procurement system demonstrates the successful and continued achievement of its original aims and future aspirations to strengthen its efficiency and transparency as it celebrates its ten-year anniversary.

---

36. Comparative Legal Guide, *supra* note 28.

37. *Dirección ChileCompra–10 años moderizando al Estado, Desarollado por Área de Comunicaciones y Marketing*, Dirección ChileCompra, www.chilecompra.cl (last visited March 30, 2014) [hereinafter *Dirección ChileCompra*].

38. *U. F. 2013*, Servicio de Impuestos Internos (2013), http://www.sii.cl/pagina/valores/uf/uf2013.htm.

39. *Dirección ChileCompra*, *supra* note 37.

40. *Más de 112 mil proveedores hicieron negocios a través de ChileCompra el 2012*, Boletin ChileCompra Informa, http://www.chilecompra.cl/index.php?option=com_content&view=article&id=1371:mas-de-112-mil-proveedores-hicieron-negocios-a-traves-de-chilecompra-el-2012&catid=301&Itemid=1048 (last visited Jan. 19, 2014).

III. Significant Developments in Canadian Public Procurement Law

The following is a review of some of the more significant public procurement developments in 2013.

A. Canada-EU Comprehensive Free Trade Agreement

Canada and the European Union have recently signed the Canada-EU Comprehensive Economic Trade Agreement (CETA),[41] which will greatly increase the ability of EU companies to sell to provincial, municipal, and federal governments in Canada and for Canadian companies to sell to the EU governments. Significant legislative and regulatory changes to federal and provincial procurement legislation will be required to implement the Agreement.

Federal government contracting is subject to international disciplines under the North American Free Trade Agreement and the World Trade Organization Agreement on Procurement. But allowing access by European companies to lucrative provincial and municipal procurement markets is a game-changer. Up until now, the provinces and municipalities have not been subject to widespread international disciplines governing their procurement process and contract awards. "Though some provincial government entities are subject to the procurement disciplines in the Canada U.S. Agreement on Government Procurement vis-à-vis U.S. suppliers, municipalities have never been subject to permanent international trade disciplines in public procurement."

CETA has generally greatly expanded opportunities for companies from each party to bid on the other's government contracts. The European Union has provided Canada with access equivalent to what it provides amongst its member States within the EU's internal market. The European Union has excluded ports and airports, broadcasting, the postal sector, and shipbuilding and maintenance from the scope of CETA. By contrast, it has provided more comprehensive coverage than Canada in the areas of energy, cultural industries, and public transit. The European Union has also agreed to provide for pre-contractual remedies to Canadian suppliers for the first ten years of CETA. This provision allows Canadian suppliers to stop the award of a contract prior to its being signed. But if the Canadian provinces and territories do not reciprocate in their procurement procedures, this benefit will disappear.

Canada has also agreed to a significant liberalization of its procurement regime. During the CETA negotiation, there were significant concerns expressed by certain non-governmental organizations that CETA would eliminate the ability of Canadian municipalities to favor local suppliers. Though it is true that CETA represents the most favorable market treatment Canada has offered a free-trade partner to date, there are still significant protections.

There will be thresholds set on all procurements below which CETA will not apply. This includes a threshold of $315,000 for procurement by municipalities, academia, school boards, and hospitals. Further, Quebec and Ontario will be allowed to retain a 25 percent Canadian value requirement for procurement of public-transit vehicles. Canada has also excluded a wide range of procurement activities from the application of CETA.

41. *See Comprehensive Economic and Trade Agreement*, Canada-European Union http://www.actionplan.gc.ca/en/content/ceta-aecg/canada-eu-trade-agreement (last visited Jan. 19, 2014).

These include health care, set-asides for Aboriginal businesses, certain regional development exclusions, the cultural industries in Quebec, shipbuilding and repair, certain sensitive goods procured by security-mandated entities, and ports and airports. Utilities and crown corporations are, however, subject to the procurement obligations of CETA.

CETA mandates that Canada create a single point of electronic access for procurement within five years of CETA's entering into force. This should create efficiencies for any company seeking to bid on government services.

But CETA does not completely strip all protections from municipalities and provinces for local procurement, particularly when the procurement is supplied by a small business. The CETA rules on procurement will apply only to contracts above a certain value, roughly equivalent to the thresholds established by the WTO Agreement on Government Procurement. For 2012 to 2013, this threshold was 200,000 Special Drawing Rights (SDRs)—approximately $315,500 for goods and services. For contracts for procurement by utilities, that number was 400,000 SDRs ($631,000). Finally, for construction services, the threshold for applicability was 5 million SDRs ($7.8 million).

These thresholds are *much* higher than those set out in the Agreement on Internal Trade (the document that applies to all government procurements in Canada) and, for contracts other than construction-services contracts, are also higher than current Canadian federal government commitments in NAFTA.

B. Proposed Amendments to the Defence Production Act and Controlled Goods Program

On November 20, 2013, Public Works and Government Services Canada (PWGSC) launched consultations on proposed amendments to the Defence Production Act (DPA)[42] that will have a significant impact on Canadian companies in the defence, aerospace, security, and satellite sectors. Companies that are subject to the DPA and its Controlled Goods Regulations[43] are subject to significant registration, screening, and security obligations in their dealings with controlled goods and technology within Canada. The proposed amendments will significantly change the scope of products and technology subject to the Controlled Goods Program (CGP), including by removing approximately 52 percent of the current entries covered by the DPA Schedule.

It was strongly recommended that companies dealing with defence, aerospace, security, and satellite goods and technology carefully review the proposals to ensure that they understood the changes and, if necessary, addressed any concerns through submissions to PWGSC. The deadline for submissions was December 20, 2013.

1. *Background: Canada's Controlled Goods Program*

Canada's CGP was established in 2001 to address U.S. concerns over Canada's treatment of defence and other related goods and technologies subject to control under the U.S. International Traffic in Arms Regulations (ITAR). The CGP was intended to harmonize defence trade controls, practices, and enforcement between Canada and the

42. R.S.C., 1985, c. D-1.
43. SOR/2001-32.

United States and, inter alia, to allow for the transfer of various ITAR-controlled items from the United States to Canada without a license.

More recently, in response to human rights, employment, and privacy concerns, the United States implemented changes to the ITAR that permit transfers of ITAR-controlled items to certain dual and third-country nationals within Canada. In conjunction with those changes, Canadian authorities have implemented an Enhanced Security Strategy that significantly tightened many of the requirements under the CGP, including extensive screening of individuals in Canada who are to have access to CGP-controlled items.[44]

2. *The Canadian and U.S. Defence Control Regimes*

The Canadian CGP was designed to work hand-in-hand with the U.S. ITAR regime so that, generally speaking, goods and technology controlled for ITAR purposes would also be subject to domestic controls in Canada under the CGP.

Some Canadian companies have found the requirements to be overly burdensome and have encountered problems specifically in the intersection of the Canadian and U.S. regimes. This has included instances in which items that were no longer controlled under the U.S. ITAR regime are still be controlled under the Canadian CGP regime (and vice-versa).

3. *Proposed Amendments to the Defence Production Act*

In response to a number of concerns expressed regarding administrative burden and inconsistencies between the Canadian and U.S. regimes, PWGSC has proposed significant amendments to the DPA Schedule that identifies the goods and technology subject to the CGP.

A key proposal involves the identification of two streams of goods and technology in the new Schedule. Stream 1 will be all ITAR-controlled goods and technology imported from the United States, and Stream 2 will be all other items with strategic significance or national security implications regardless of their country of origin. For Stream I, the Schedule will make direct reference to the U.S. Munitions List (USML) that identifies all ITAR-controlled items. This is intended to ensure that as the United States reforms its export controls and moves items from USML control under the U.S. State Department to dual-use control under the U.S. Commerce Department, the Canadian CGP regime will reflect those changes (subject, of course, to any items that Canada may otherwise control for CGP purposes under Stream 2).

In PWGSC's Consultation Paper, there is a long list of items to be removed from CGP control that are currently referred to in the DPA Schedule and set out in Group 2 (Munitions List), Item 5504 (Strategic Goods and Technology), and Group 6 (Missile Technology Control Regime) of Canada's Export Control List (ECL).

It is important to note that none of the proposed changes will impact Canadian controls on the export or transfer of ECL goods or technology from Canada.

44. *See generally* Final U.S. ITAR Rule on Dual and Third-Country Nationals Raises New Challenges for Canadian Business, *available at* http://www.mccarthy.ca/article_detail.aspx?id=5422.

4. *Timeline for Next Steps*

PWGSC accepted submissions on the proposed changes until December 20, 2013. After taking into account responses received, PWGSC will issue a Consultation Report in January of 2014 and then publish a notice of the changes in the Canada Gazette–Part 1 between May and June of 2014. Publication in the Canada Gazette–Part 2 will occur between October and November of 2014. It is presently anticipated that the amended DPA Schedule will come into force in November of 2014.

Companies should be closely reviewing the proposals to determine whether there are any positive or negative impacts to their operations as well as whether any additional items should be removed from CGP control. Monitoring two streams of controlled items for CGP purposes and a different set of items for export control purposes may also create complications for some organizations.

C. Amendments to Canada's Foreign Anticorruption Legislation

On June 19, 2013, Bill S-14: The Fighting Foreign Corruption Act, received Royal Assent, thereby bringing into force the most significant changes to Canada's anti-corruption legislation, the Corruption of Foreign Public Officials Act (CFPOA),[45] since its inception. The amendments significantly increase the scope of the CFPOA's prohibitions and enhance the ability of Canadian authorities to prosecute and penalize offenders.

Canadian companies should now be carefully reviewing their anti-bribery policies and procedures to ensure they are in full compliance with these new laws. Further, those companies whose policies currently allow for facilitation payments should now be taking steps to eliminate those practices, as the government has served notice that the existing exception for such payments will be repealed.

1. *The Key Changes*

There are six key changes to Canada's anti-bribery regime. In brief, they are as follows:

- the exception for facilitation payments is now subject to elimination by an order of the federal Cabinet; the government has put Canadian companies on notice that the exception for payments made to expedite or secure the performance of acts of a routine nature will be eliminated at a future date, allowing time for companies to adjust their policies and being cognizant of the competitive disadvantage this may create vis-à-vis other countries (such as the United States) that continue to allow their companies to make such payments;
- there are new prohibitions against engaging in a wide range of activities regarding books and records when undertaken for the purposes of bribing a foreign public official or disguising such bribery;
- the jurisdiction of the CFPOA is significantly expanded from a territorial to a nationality basis; regardless of where the alleged bribery has occurred, the CFPOA now applies to all Canadian companies and citizens as well as permanent residents present in Canada after they commit the offense;

45. S.C. 1998, c. 34.

- the maximum term of imprisonment for individual offenders has been increased from five to fourteen years; in addition to sending a signal regarding the seriousness with which the government views CFPOA violations, this eliminates the availability of discharges and conditional sentences;
- the definition of business activity subject to the CFPOA has been expanded with the removal of the "for profit" requirement; and
- the Royal Canadian Mounted Police (RCMP) has been accorded exclusive authority to lay charges for CFPOA and related offenses.

These changes should be viewed in the wider context of recent policy initiatives and increased anticorruption enforcement in Canada. This past year saw new and vigorous enforcement of the CFPOA by the RCMP and Crown prosecutors. The widely publicized guilty pleas of Niko Resources Ltd. in June of 2011 and Griffiths Energy International in January of 2013, along with ongoing RCMP investigations into the activities of a number of other Canadian companies, serve as stark warnings of the costs of noncompliance.

D. Aerospace Review Report

The Canadian Federal Government announced that, in December 2013, it will begin its implementation of the recently completed report "Beyond the Horizon: Canada's Interest and Future in Aerospace,"[46] conducted by a review committee led by the Honourable David Emerson.[47]

The report recommendations include:

- making aerospace a priority in Canada's Science and Technology Strategy to ensure a more cohesive approach to the development and delivery of aerospace programs;
- improving the prioritization of technology investments and creating large-scale technology demonstration capacity to boost Canadian competitiveness and domestic capabilities to meet the growing demand for more efficient aircraft and space-related technologies;
- streamlining programs including the Strategic Aerospace and Defence Initiative and transforming it into a risk-sharing instrument to foster Canada's full aerospace and research and development potential;
- fully leveraging procurement tools such as Canada's federal offset program and the Industrial Regional Benefits Program to bolster industry capabilities through intellectual property and technology transfer;
- introducing a more efficient export control and defence certification regime; and
- stabilizing Canadian Space Agency funding to enable it to better serve Canada's public and industrial priorities.

46. *See* Aerospace Review, Beyond the Horizon: Canada's Interests and Future in Aerospace (2012), *available at* http://aerospacereview.ca/eic/site/060.nsf/vwapj/Aerospace-e-online.pdf/$file/Aerospace-e-online.pdf.

47. *See Industry Minister James Moore to Address Aerospace Innovation Forum*, Gov't of Can. (Nov. 29, 2013), http://news.gc.ca/web/article-eng.do?nid=797409.

1. *Case Law Developments*

Envoy Relocation Services Inc. v. Canada (Attorney General)[48] concerned a tender by the federal government. The trial judge awarded $29 million to the unsuccessful bidder due to the court's findings that the tender had been conducted unfairly.

The dispute arose from a 2004 Request for Proposal (RFP) by the Canadian government. The RFP was for a relocation service for personnel employed in the Canadian armed services, government services, and RCMP. An earlier RFP had been undertaken in 2002. One element in both RFPs was a service called Property Management Services (PMS). Under PMS, the winning bidder was required to arrange and pay for various services to the individuals being moved, such as realty services, legal services, and similar services. The incumbent provider, which had won the 2002 RFP, knew that PMS services were used hardly at all by any of the transferred individuals. In the 2004 RFP, the incumbent provider, again, knew that few individuals used PMS, so it included zero cost for this service in its bid. The other bidders were told to include a specified level of projected users of PMS and did so. By doing so, their bids were about $45 million more than they would otherwise have been if they had bid zero as a ceiling for PMS, as the incumbent had done. The trial judge found that, because of the unfairness with which the Crown had conducted the RFP, the Crown had breached the contract that applied to the bidding process and Envoy Relocation Services was entitled to about $29 million in damages.

The trial judge held that "in the tendering context, the measure of damages is loss of profits" of the plaintiff whose bid ought to have been accepted. The court also held that the duty of good faith is not temporal in nature—the duty extends backward in time to the drafting of the terms of the request for proposals. It found that a biased bid-preparation process would lead to biased outcomes, thus violating the duty of good faith owed to compliant bidders in the present.

48. Envoy Relocation Services Inc. v. Canada *(Attorney General)*, 2013 ONSC 2034.